

**IMPLEMENTING THE 21ST CENTURY
CURES ACT: MAKING ELECTRONIC
HEALTH INFORMATION AVAILABLE
TO PATIENTS AND PROVIDERS**

**HEARING
OF THE
COMMITTEE ON HEALTH, EDUCATION,
LABOR, AND PENSIONS
UNITED STATES SENATE
ONE HUNDRED SIXTEENTH CONGRESS**

FIRST SESSION

ON

EXAMINING IMPLEMENTING THE 21ST CENTURY CURES ACT, FOCUSING
ON MAKING ELECTRONIC HEALTH INFORMATION AVAILABLE TO PA-
TIENTS AND PROVIDERS

MARCH 26, 2019

Printed for the use of the Committee on Health, Education, Labor, and Pensions



Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

41-393 PDF

WASHINGTON : 2021

COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS

LAMAR ALEXANDER, Tennessee, *Chairman*

| | |
|-------------------------------|--|
| MICHAEL B. ENZI, Wyoming | PATTY MURRAY, Washington |
| RICHARD BURR, North Carolina | BERNARD SANDERS (I), Vermont |
| JOHNNY ISAKSON, Georgia | ROBERT P. CASEY, JR., Pennsylvania |
| RAND PAUL, Kentucky | TAMMY BALDWIN, Wisconsin |
| SUSAN M. COLLINS, Maine | CHRISTOPHER S. MURPHY, Connecticut |
| BILL CASSIDY, M.D., Louisiana | ELIZABETH WARREN, Massachusetts |
| PAT ROBERTS, Kansas | TIM KAINE, Virginia |
| LISA MURKOWSKI, Alaska | MARGARET WOOD HASSAN, New Hampshire |
| TIM SCOTT, South Carolina | TINA SMITH, Minnesota |
| MITT ROMNEY, Utah | DOUG JONES, Alabama |
| MIKE BRAUN, Indiana | JACKY ROSEN, Nevada |

DAVID P. CLEARY, *Republican Staff Director*

LINDSEY WARD SEIDMAN, *Republican Deputy Staff Director*

EVAN SCHATZ, *Minority Staff Director*

JOHN RIGHTER, *Minority Deputy Staff Director*

C O N T E N T S

STATEMENTS

TUESDAY, MARCH 26, 2019

Page

COMMITTEE MEMBERS

| | |
|--|---|
| Alexander, Hon. Lamar, Chairman, Committee on Health, Education, Labor, and Pensions, Opening statement | 1 |
| Murray, Hon. Patty, Ranking Member, a U.S. Senator from the State of Washington, Opening statement | 3 |

WITNESSES

| | |
|--|----|
| Moscovitch, Ben, M.A., Project Director, Health Information Technology, The Pew Charitable Trusts, Washington, DC | 6 |
| Prepared statement | 7 |
| Summary statement | 15 |
| Savage, Lucia, C., J.D., Chief Privacy and Regulatory Officer, Omada Health, Inc., San Francisco, CA | 16 |
| Prepared statement | 17 |
| Summary statement | 29 |
| Rehm, Christopher, R., M.D., Chief Medical Informatics Officer, LifePoint Health, Brentwood, TN | 29 |
| Prepared statement | 31 |
| Summary statement | 34 |
| Grealy, Mary, J.D., President, Health Leadership Council, Washington, DC | 36 |
| Prepared statement | 37 |

ADDITIONAL MATERIAL

| | |
|--|----|
| Supplemental remarks of Lucia C. Savage, J.D. | |
| Digital Health Data and Information Sharing: a New Frontier for Healthcare Competition | 54 |
| ONC's Proposed Rule On Information Blocking: The Potential To Accel- erate Innovation In Health Care | 83 |
| Comments of Omada Health, Inc. to U.S. Department of Health and Human Services Office for Civil Rights in Response to Request for Information, Docket # 0945AA00 | 86 |
| Supplemental remarks of Mary Grealy, J.D. | |
| HLC BPC Report on Advancing Interoperability, Information Sharing, and Data Access | 98 |

IMPLEMENTING THE 21ST CENTURY CURES ACT: MAKING ELECTRONIC HEALTH INFORMATION AVAILABLE TO PATIENTS AND PROVIDERS

Tuesday, March 26, 2019

U.S. SENATE
COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m., in room SD-430, Dirksen Senate Office Building, Hon. Lamar Alexander, Chairman of the Committee, presiding.

Present: Senators Alexander [presiding], Cassidy, Romney, Braun, Murray, Baldwin, Kaine, Jones, Hassan, Rosen, and Casey.

OPENING STATEMENT OF SENATOR ALEXANDER

The CHAIRMAN. The Senate Committee on Health, Education, Labor, and Pensions will please come to order. Senator Murray and I will each have an opening statement, then we will introduce the witnesses. After the witnesses' testimony, Senators will each have about five minutes of questions.

Reid Blackwelder is a family physician with three clinics in the tri-cities area of East Tennessee. A few years ago, he talked with the New York Times about his electronic health records that were supposed to make his life easier saying, "we have electronic health records at our clinic but the hospital, which I can see from my window, has a separate system from a different vendor. The two do not communicate. When I admit patients to the hospital, I have to print out my notes and send a copy to the hospital so they can be incorporated into the hospital's electronic records." Dr. Blackwelder could pay for his patients' hospital records to be electronically sent from his system to the hospital system, but it would cost him \$26,400 every month or \$316,800 a year. So, for Dr. Blackwelder and many other doctors, record keeping is now more expensive and burdensome as a result of electronic health care records.

In 1991, the National Academy of Medicine released a report urging the prompt development and implementation of what were then called computer-based patient records. We forget that was well before the internet was in common usage in the United States. The report said, these systems have a unique potential to improve the care of both individual patients and reduce waste through continuous quality improvement. Electronic health records, as they came to be called, got a boost in 2009 when the Federal Government, in a bipartisan effort, began the Meaningful Use Program,

spending over \$36 billion in grants to incentivize doctors and hospitals to use these systems. As was the prediction in the 1991 report, the hope was that electronic records would improve patient care and reduce unnecessary healthcare spending. This is important to this Committee because at our hearing last summer Dr. Brent James from the National Academies testified that up to 50 percent of what we spend on health care is unnecessary. So, there is bipartisan focus, both in the Congress and the administration, on reducing health care costs.

One way to reduce what we spend on administrative tasks and on necessary care, is by having electronic health records that talk to one another, which we call interoperability. But in 2015, six years after the Meaningful Use Program started, as this Committee worked on the 21st Century Cures Act, we realized that in many cases electronic health records added to administrative burden and increased unnecessary health care spending. A major reason for that is the records are not interoperable. One barrier to interoperability is called information blocking, which is when some obstacle is in the way of a patient's information being sent from one doctor to another. So, in 2015, this Committee held six bipartisan hearings, formed a working group to find ways to fix the interoperability of electronic health records. These hearings led to a bipartisan group of HELP Committee Members working together to include a provision in the 21st Century Cures Act, to stop information blocking and encourage interoperability.

Today's hearing is about two rules that the Department of Health and Human Services proposed to implement this provision in the 21st Century Cures Act. The two rules are complicated, but I would like to highlight a few ways they lay out a path toward interoperability. One, the rules define information blocking so we know what we mean when we are talking about it. So, it is more precisely clear what we mean when one system, hospital, doctor, vendor, or insurer is purposely not sharing information with another.

Second, the rules require that by January 1, 2020, for the first time insurers must share a patient's health care data with the patient so their health information follows them as they see different doctors. Third, all electronic health records must adopt the same standards for data elements, known as application programming interface or API, two years after these rules are completed. And fourth, hospitals are required to send electronic notifications to a patient's doctors immediately when that patient is admitted to, discharged from, or transferred from the hospital. According to the Department of Health and Human Services, these new rules should give more than 125 million patients easier access to their own records in electronic format. This should be a huge relief to any of us who have spent hours tracking down paper copies of our records and carting them back and forth to different doctors' offices. The rules will reduce administrative burden on doctors so they can spend more time with patients.

A recent study from Kaiser found that emergency room doctors in order use electronic health record systems make up to 4,000 mouse clicks per shift. If electronic health records data was truly interoperable, it would greatly reduce how many clicks doctors

have to make. According to the Department of Health and Human Services, spending less time on these administrative tasks will improve efficiency and save about \$3.3 billion a year. And because doctors can see patients full medical history, they can avoid ordering unnecessary tests and procedures. I also want to be aware, and I know this Committee does, of unintended consequences from these two rules. Are we moving too fast?

In 2015, I urged the Obama administration to slow down the Meaningful Use Program, which they did not do, and looking back, the results would have been better if they had. Are the standards for data elements too rigid? Is the door still open for bad actors to game the system and continue to information block? And how can we ensure patient privacy as patients gain more access and control over their personal health information, and how do we help them keep it secure? I want to ensure these rules will make the problem of information blocking better not worse.

I look forward to any specific suggestions to improve the rules from those who use electronic health record systems. Electronic health records that work can give patients better outcomes and better experiences at a lower cost.

Senator Murray.

OPENING STATEMENT OF SENATOR MURRAY

Senator MURRAY. Thank you very much, Mr. Chairman.

Back in 2008, just one in 20 hospitals used electronic health records. A decade later, we have made enough progress to flip that number entirely. Today, just one in 20 hospitals have not adopted electronic health records. And over the past decade, we have seen how better information about a patient's health care does make a big difference. In national news, electronic health records played an important role in understanding how the water in Flint, Michigan was putting families in danger. And while they do not always make headlines, electronic health records also make a difference by helping care providers identify health problems sooner so patients can get preventive care to stay healthy, avoid duplicated tests or medication errors, and identify treatments that might be counter-productive based on a patient's medical history or current prescriptions.

The HITECH Act we passed in 2009 was a big part of accomplishing the progress we have seen so far, but we have to continue building on that progress to ensure health information technology lives up to its full potential. And we have to continue oversight, following up the work we did in 2015 after the Office of the National Coordinator for Health Information Technology put out a report detailing some of the challenges ahead. The report made clear information blocking was a serious problem throughout the health care system. While high tech required certified electronic health record products to meet technical standards intended to make good information more accessible for care providers, the ONC report found substantial evidence some organizations were intentionally setting up barriers between their systems and other systems, like exorbitant fees whenever someone sent, received, or even searched for a patient's information, contracts that restricted people's ability to access and share their own health information, and systems built

in ways that made sharing information needlessly complicated. Maybe they missed the day in kindergarten about sharing, because putting something where only you can reach or charging excessive fees for it is absolutely not how it should be done. And it is absolutely not acceptable when it comes to people's health.

We cannot afford to have bad actors who prioritize their bottom line over patients' best interest, and block information hospitals, providers, and patients need to be able to share that with one another. We also cannot expect health IT systems to get better when some vendors include gag clauses that prevent care providers from speaking out about the problems, or issues, or errors they encounter. It should be easy for providers shopping for electronic record systems to learn about potential issues. It should be easy for medical professionals to hear about a problem with a system they use, and it should be easy for anyone to speak out when they see something that would jeopardize people's health. When systems cannot speak with each other and people cannot speak up about the problems they see, it is patients who do get hurt. Like the man in California who suffered brain damage after his diagnosis was delayed because a hospital software could not properly interface with a lab software, or the woman in Vermont who died of a brain aneurysm that might have been caught if a software problem had not stopped the order for a test that she needed. When we talk about making sure we have a strong health IT system, we are not just talking about technology and innovation. Families' lives depend on making sure we get this right, which is why I was glad we were able to take steps to address these issues in the 21st Century Cures Act.

I look forward to hearing from our witnesses about their perspective on ONC's proposed rule to implement the Cures' provisions. In that bill, we moved to end information blocking, and make clear when patients and their care providers need information, they should not be stopped by unnecessary, unreasonable barriers. And we tasked ONC with clarifying what sort of concerns, like privacy, and safety, and security, would be grounds for reasonable exceptions. We also took steps to help ONC strengthen its certification program beyond technical criteria for electronic health records, so they can make sure that if vendors want to get the Government seal of approval, then they cannot engage in information blocking or use gag clauses.

The new conditions also call for open application programming interfaces, or APIs, another step that will help make sure systems developed by different vendors and used by different doctors are able to speak to each other, and that patients have an easier time getting access to their medical records. I am glad ONC is moving to put these common sense steps into action. I am interested in making sure this gets done right. I look forward to hearing from our witnesses about their perspective on ONC's approach, and about the steps the Centers for Medicare and Medicaid Services is taking to make claims data more accessible and prompt care providers to be better about sharing information. Of course, as we continue to proof our health IT system, we need to make sure that health information is being provided in a way that works for patients as well.

During our 2015 hearings, I shared the story of woman who had been seeking the results of her pregnancy test, but instead of a clear answer, her electronic health record simply reported her hormone levels—not helpful. We need to do better for her and for other patients who have gone looking for information they can use only to find massive binders, unreadable PDFs, and stacks of CDs. Engagement and usability have to be part of this discussion. And last but not most certainly not least, we need to talk about security, privacy, and data stewardship. That means prioritizing the development of technology and best practices that can help prepare for the constantly evolving cyber security threats of the 21st century.

It also means having a national conversation about what is required for all parties to be good stewards of the data people entrust them with, and that conversation is only going to become more important as tech companies and others introduce new products like mobile applications that empower people with their health care data but are not covered by existing HIPAA protections. Patients should be able to expect tech companies are going to use their most sensitive information responsibly and give them the tools they need to be able to control how and when their information is disclosed. Our objective should be to make sure tech companies are putting patients in the driver's seat, not the other way around. It is clear we have come a long way when it comes to strengthening our Nation's health information infrastructure, but it is also clear there are a lot of challenges ahead.

I look forward today to hearing from all of our witnesses. Thank you for being here. We want to hear about how data and technology can actually empower patients and care providers, and I hope we can continue our bipartisan work on this important issue, Mr. Chairman.

Thank you.

The CHAIRMAN. Thank you Senator Murray and thank you for your leadership on this. I think all Members of the Committee would agree that the 21st Century Cures Act is one of the most important pieces of legislation we have had a chance to work on. Senator McConnell, Majority Leader, said it was the most important bill in the Congress in which it passed, and it was a bipartisan piece of legislation.

I have noticed that we can do three things in the Committee, it seems to me. One, we can call attention to something, which we are doing today and which we did with our five hearings on electronic health care records. Two, we can pass a law, which we did with 21st Century Cures. And three, we can make sure the law works, which is what this hearing is about—it is about oversight. And we welcome our witnesses.

The first one, Mr. Ben Moscovitch is the Project Director of Health Information Technology at the Pew Charitable Trust. He leads research on the challenges of achieving interoperability and highlights possible solutions.

Next, we will hear from Ms. Lucia Savage. She is the Chief Privacy and Regulatory Officer at Omada Health. Omada is a digital behavioral health company that aims to address health issues including type 2 diabetes, heart disease, and obesity. She focuses on

advancing health care using technology and maintaining the security of patients' health information.

The third witness, Dr. Christopher Rehm, is Chief Medical Information Officer of LifePoint Health in Brentwood, Tennessee. It is a hospital system with 89 locations in 30 States. He works both with physicians and patients to apply technology solutions to health care needs.

Finally, we will hear from Ms. Mary Grealy, President of the Healthcare Leadership Council, which is comprised of health care executives from leading organizations and companies in the health care industry, health plans, hospitals, health product distributors, pharmacies, and academic medical centers.

Welcome to each of our witnesses. Thank you for making time for us today. If you will summarize your remarks in about five minutes, we will then have questions. Why don't we begin, Mr. Moscovitch with you.

**STATEMENT OF BEN MOSCOVITCH, M.A., PROJECT DIRECTOR,
HEALTH INFORMATION TECHNOLOGY, THE PEW CHARITABLE TRUSTS, WASHINGTON, DC**

Mr. MOSCOVITCH. Chairman Alexander, Ranking Member Murray, Members of the Committee, thank you for holding this hearing and for the opportunity to present testimony. If one were to read recent news articles, it would be reasonable to think that our healthcare system is less efficient and less safe because of the transition from paper to electronic records.

The truth is EHRs have revolutionized modern medicine by giving clinicians better tools to document patients' needs, safely prescribe medications, and administer care. But, as Congress recognized in the 21st Century Cures Act, gaps remain. They keep EHRs from reaching their full potential. Oversight from this Committee can help fill those gaps. My testimony will focus on three aspects of the recently proposed regulations to implement Cures that could one, enable easier use of health data, two, promote better matching of patient records, and three, improve safety and reduce clinician burden.

First, interoperability requires patients and clinicians to be able to effectively access and extract information from EHRs. To address that, Congress directed ONC to develop new criteria for EHRs, which help different systems communicate. These are called APIs or Application Programming Interfaces. APIs are the foundation of the modern internet. They allow travel websites to aggregate airline fares, personal financial applications to pull data from an individual's accounts, and countless other everyday uses. For APIs to be effectively used, different systems need to exchange data in the same way. To accomplish this, ONC identified the use of a standard called FHIR for data exchange and provided guidance on how to consistently implement it for better interoperability. As ONC finalizes the rule, Congress should ensure that the agency maintains its commitment to these standard APIs.

Interoperability also requires health organizations to know that they are communicating about the same person. This is often referred to as patient matching. When data are exchanged, records may not be matched up to half the time. Pew has identified con-

crete steps that Congress should encourage ONC to take, including ones recently highlighted in a GAO report required by Cures. We found that better standardization of data can improve match rates. For example, Pew funded research at Indiana University revealed that use of the U.S. Postal Service standard for address would increase match rates by approximately 3 percent, a significant improvement. One technology developer told us this would help their system match an additional tens of thousands of records per day. To improve matching, ONC should specify use of the postal service standard for address and include other routinely collected elements like email address, which is already in half of records but not used for matching. In Cures, Congress also recognized that EHR usability must be improved. Usability refers to system design, as well as how they are customized and used. Poor usability can contribute to clinician burden and contribute to medical errors.

Pew collaborated with MedStar Health to examine the contribution of EHR usability to medication safety events, such as dosing errors in three pediatric health care facilities. The research found that EHR usability contributed to more than a third of the 9,000 events examined. This Committee can encourage ONC to make patient safety a priority in implementing Cures. Congress charged ONC with developing new criteria for EHRs used in pediatric care. While ONC rightly identified 10 priorities for pediatric care, such as the dosing of drugs based on weight, the agency should better focus on safety and usability. For example, ONC should clarify that developers seeking certification for pediatric functions involve pediatricians and pediatric nurses to test the system.

Congress also required ONC to establish an EHR reporting program. The agency should embed safety in the usability aspects of this program, as recommended by clinicians, technology professionals, and others. In conclusion, the bipartisan passage of Cures launched a new era for digital health by providing patients and clinicians with better access to data and reducing medical errors. As the administration continues its implementation, this Committee can ensure that Congress's goals are met by supporting secure, standard API access to a wide range of health data, encouraging ONC to address patient matching through better standards, and pressing ONC to focus on patient safety throughout the implementation of Cures.

Thank you for holding this hearing, and I look forward to answering your questions.

[The prepared statement of Mr. Moscovitch follows:]

PREPARED STATEMENT OF BEN MOSCOVITCH

Chairman Alexander, Ranking Member Murray, Members of the Committee, thank you for holding this hearing and for the opportunity to present testimony.

My name is Ben Moscovitch; I serve as the Project Director of Health Information Technology at The Pew Charitable Trusts (Pew), a nonprofit, nonpartisan research and policy organization. Our health information technology project focuses on improving the safety of electronic health record (EHR) systems, and enhancing the exchange of information so that health care providers and patients have the data they need to make informed decisions.

EHRs have revolutionized how clinicians deliver care by equipping them with better tools to document patients' health status, safely prescribe medications, and otherwise order health care interventions. And, these tools have the potential to make

it easier for patients and clinicians to have more complete and robust data to coordinate care across health care settings.

Seeking to build on the improvements spurred on by the digitization of paper records, Congress recognized that gaps remain in realizing the full potential of EHRs to give patients their data, make clinical care more efficient, and enhance patient safety. The 21st Century Cures Act (Cures), passed in 2016, marked an important step toward remedying these deficiencies by addressing barriers to both the effective exchange of health data, known as interoperability, and the usability of these systems.

Congress, through Cures, set a positive vision for the future of EHRs—a vision where patient data are securely accessible to patients and clinicians wherever and whenever they need them. Access to health data would help advance the coordination of care for patients who see multiple physicians. This coordination would help patients live longer and better lives, and reduce costs associated with duplicate laboratory and other services. And, this vision would have EHRs serve as a critical, helpful tool that clinicians can seamlessly use to administer higher quality care. In this vision, EHRs are indispensable, yet almost invisible to patients because the systems are easily and efficiently used, and only interject in care to offer essential support services to help clinicians provide safer, higher quality care.

Earlier this month, the Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare & Medicaid Services (CMS) issued proposed rules to begin implementing that vision captured in Cures. The regulations aim to ease the exchange of health data when patients want to access their information or have it transmitted to their health care providers, and otherwise focus on barriers to the use of these systems to improve patient care.

My testimony will focus on three key aspects of the proposed rules from ONC and CMS published earlier this month that address Congress’ desire to improve the interoperability of health data and effective use of EHRs. Specifically, I will discuss:

- provisions enabling easier extraction and use of health data from EHRs via application programming interfaces (APIs), which enable different technologies to communicate;
- needed enhancements to better match patient records across the different health care providers where individuals seek care; and
- necessary improvements to the usability of EHR systems to address design and implementation factors that can both introduce burdens on clinicians and contribute to medical errors.

Enhanced Interoperability via Application Programming Interfaces

For patients to obtain their records or health care providers to exchange information, they first need the ability to effectively extract data from EHRs. To address that challenge, Congress required ONC to develop new criteria for EHRs to make “all data elements” available via APIs, which are software tools that allow systems to request and deliver information to other systems. APIs are the foundation to the modern internet; they allow travel websites to aggregate fares from different airlines, personal financial applications to pull data from an individual’s accounts, and countless other everyday uses.¹

Currently, EHRs often do not support the robust use of APIs for data exchange, or if they do, those APIs can be implemented in proprietary ways that inhibit the use of the data by clinicians and patients. The Cures provision on APIs—colloquially referred to as “open APIs”—would let other technologies more readily access data within the system in a secure manner. The term “open” does not suggest that health data can be freely accessed by any user. Instead, “open” refers to the fact that these APIs would be easier to use, such as that the business and technical documentation would be publicly available.

By including this provision in Cures, Congress recognized that APIs reflect the future of data exchange in health care. They can enable patients to access their health records, hospitals to better exchange data with other organizations, and health care facilities to build and implement new decision support tools on top of their EHRs.

¹ The Pew Charitable Trusts, “Electronic Tools Can Strengthen Health Care Data Access, Sharing” (2018), <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2018/09/electronic-tools-can-strengthen-health-care-data-access-sharing>.

In the recently proposed regulations, ONC implements this API provision, making several critical decisions on the standards to use for data and what information EHRs must be able to release.

ONC Advances Standard, Secure APIs

For third-party technologies—like smartphone applications that patients use to download their records or clinical decision support tools that sync with EHRs—to utilize APIs to access data, the developers of these tools must know how to request and access the information. When EHRs use different standards for APIs, each third-party technology must change its systems to reflect every variation.

Recognizing this challenge, ONC sought to minimize the variability across systems by requiring the use of standards for APIs. Achieving standardization across APIs necessitates consistency both for how information can be accessed and how the data elements are represented. ONC accomplishes that goal by requiring use of the Fast Healthcare Interoperability Resources (FHIR) standard, which technology developers are increasingly adopting, for how to exchange information.

However, FHIR permits the depiction of data elements in different ways and considers the inclusion of some data as optional, which could inhibit interoperability. To reduce this variability, ONC proposes to require the use of an implementation guide developed by the Argonaut Project—a collaboration among technology developers and health care providers—that provides constraints on how to implement FHIR.

This combination of the FHIR standard and the Argonaut Project implementation guidelines will reduce the barriers to API use, so that patients and clinicians are better able to access data contained in EHRs. As ONC finalizes the rule, Congress should ensure that the agency maintains its commitment to standardized APIs—both through the use of FHIR and refined implementation guidelines.

ONC Expands Data Elements Made Available

To fully take advantage of APIs as a tool to improve interoperability and patient access to electronic health data, Congress required that they provide access to “all data elements” within an EHR system. In ONC’s proposed rule, the agency provides guidance on what information constitutes “all data elements” that systems would be required to make available.

In prior regulations, ONC has required EHRs to have APIs that make certain information—referred to as the Common Clinical Data Set (CCDS)—available for patient access, such as through a smartphone application. The CCDS contains some critical information, including medications, laboratory tests ordered, and problem lists, but lacks other data, such as physicians’ notes. ONC has proposed expanding and adjusting the CCDS to meet the statutory requirement of making “all data elements” available. This expanded data set would be renamed the U.S. Core Data for Interoperability (USCDI), and would include additional key information. ONC’s proposed additions include:

- *Different types of clinical notes.* These clinical notes include free text entered by clinicians and other data about laboratory and imaging observations, treatment plans, and other aspects of care. In clinical notes, clinicians describe the nuances of care and patients’ medical conditions. The addition of notes to the USCDI can give patients and other clinicians critical information that may not be captured effectively in structured fields or medical codes.
- *Provenance.* Provenance indicates the author, the author’s organization, and a time stamp for data elements in the EHR. The inclusion of provenance would allow patients and clinicians to understand the origin of the data, such as whether a medication was entered by a primary care physician or at a hospital. The time stamp will allow applications to chart or sort information, such as by listing patients’ medications starting with the most recent. The addition of provenance to the USCDI would provide much needed context for the data.
- *Patients’ addresses and phone numbers.* The availability of addresses and phone numbers will better enable systems to link patient records across systems, and is described in more depth below.
- *Pediatric vital signs.* The inclusion of pediatric vital signs would enable more precise care for children by allowing different applications to model

the growth of a patient according to biologic reference ranges, and prescribe the proper dosing of drugs based on weight and age.

ONC has also requested comments on whether to expand the “medication allergies” list to also encompass reactions for other substances, such as food. By expanding this capability, clinical decision support tools could, for example, alert clinicians when patients are allergic to substances from which medications are made, such as eggs or pigs, and could improve patient safety.

Electronic Health Information Export Could be Enhanced

ONC’s implementation of the API provision from Cures supports API-based access to some—but not all—data contained in EHRs. In parallel, the ONC proposed rule also includes provisions that would facilitate the extraction of a broader group of data—referred to as electronic health information (EHI)—from health information technology systems. The EHI provision in the proposed rule would require EHR systems to support the export of all their patient data, and potentially information from other data bases connected to it. The EHI export function must support the export of an individual patient’s data as well as information on all patients in the system to allow health care providers to switch EHR systems if they so choose.

Unlike the API provisions in the proposed rule, ONC does not propose to require that technologies make this information available via any specific standards or format. Indeed, no such standard exists to describe all possible data elements across all EHRs. Instead, ONC indicates that the information should be extracted and remain computable wherever possible. Eventually, ONC states, it expects that health technologies would increasingly enable the extraction of EHI via APIs.

As noted above, Cures required ONC to issue new criteria for EHRs to make “all data elements” available via APIs. However, ONC has proposed API requirements that would only expose a subset of data—the USCDI—via APIs. To address the gap between what Congress required in Cures and ONC’s current proposal for APIs, Congress should encourage ONC to expeditiously make all EHI available via APIs wherever possible.² However, unlike the USCDI data, much of EHI data may not have widely adopted standards or be easily exchanged via FHIR. Therefore, ONC should require EHR vendors to support an API-based export capability for all data elements (i.e., information beyond the USCDI), even without requiring any particular standard for EHI that is not part of the USCDI. Eventually, as standards are more widely adopted for different data elements that are made available via the EHI provision, ONC should expand the USCDI to encompass more of this information.

Timeline for Health Care Provider Adoption

Historically, ONC releases regulations for a new edition of certification criteria for EHRs and separately CMS issues rules for health care providers to adopt technologies that meet those requirements.

However, as currently written, ONC’s regulations would require technologies certified to the 2015 version of the criteria to upgrade to meet provisions in the new regulations within approximately 2 years of when they are finalized by the agency. By the end of that 2-year period, health care providers that have not upgraded their systems to include functions—such as for APIs and EHI—required by the new regulations would no longer be using certified products and could fall out of compliance with CMS requirements.

In effect, ONC has created a system that would require several steps to occur in approximately 2 years: the development of new functions by EHR vendors; the testing and certification of those functions; implementation of changes at health care facilities; customization and configuration of the technology by health care providers; the testing of systems to ensure that they function properly within a facility and do not introduce inadvertent patient safety risks; and the training of staff.

Given all the steps that need to occur during that time period, Congress should ensure that these systems, once implemented, are sufficiently tested—including for safety—by health care providers. Additionally, ONC should work with CMS to ensure that the timeline the agency finalizes in the regulations is not subsequently delayed. This assurance would provide certainty to both EHR developers and health care providers on government’s expectations on when these provisions take effect.

² Josh Mandel, “Cures Envisions APIs for ‘All data’; ONC Proposes ‘a Limited Set’” (2019), <https://github.com/jmandel/interop-2019-nprms/blob/master/ehi-export.md>.

CMS Regulations Advance API Use for Patient Access to Claims

In parallel to ONC's regulations, the CMS proposed rule also advances the use of standard, FHIR-based APIs for patients to gain access to their information held by health plans. This would allow patients to—for example—download claims data on their phones, giving them a holistic understanding of the services and treatments that they have received from different health care providers. Equipping patients with their claims data builds on previous efforts from CMS to leverage this information, including by providing increased access to the data by researchers working to identify ways to improve care quality and reduce costs.³

Claims are especially useful because, unlike other information sources, they contain data for nearly every encounter an individual has with the health care system. Claims are standardized for providers and payers, resulting in easier aggregation of information across the health care system. As CMS states in this proposed rule, “[w]hereas EHR data is frequently locked in closed, disparate health systems, care and treatment information in the form of claims and encounter data is comprehensively combined in a patient’s claims and billing history.”

CMS’ efforts to give patients access to their claims data and provide researchers with this information, while laudable, omits one critical element particularly important for the Medicare population. Currently, claims only indicate that a procedure was performed—for example, a total knee replacement—but not the brand and model of implant used. In parallel, the unique device identifier system developed by the Food and Drug Administration (FDA) provides each medical device with a code corresponding to its brand and model. Adding the device identifier to claims can fill the gap, and provide patients, clinicians, and researchers with additional information on products used to sustain life and support care.⁴

Incorporating device identifiers in claims can also generate significant savings. The Department of Health and Human Services Office of the Inspector General (OIG) found that the failures of just seven types of cardiac implants cost Medicare \$1.5 billion to treat affected patients, and an additional \$140 million directly to beneficiaries in out-of-pocket costs.⁵ These findings led the OIG to support the addition of device identifiers to claims. The White House’s fiscal 2020 budget request for FDA also listed strong support for the addition of device identifiers to claims.⁶ For CMS to effectively equip patients with their data—including from claims—and provide researchers with information to evaluate care, the agency should ensure that claims contain critical information on the products used.

Given broad support across the health care industry and CMS’ recognition of the importance of access to claims data, Congress should ensure that device identifiers are incorporated into claims.

Ineffective Patient Matching Also Inhibits Widespread Interoperability

To achieve interoperable exchange of medical data, health organizations must also know that they are communicating about the same person. Presently, up to half of the information exchanges made by health care organizations may fail to accurately match records for the same patient. Both ONC and CMS included requests for information (RFIs) on patient matching in their proposed rules.

To accurately match records held at different health care facilities, organizations typically compare patients’ names, dates of birth, and other demographic data to determine if records refer to the same individual. Health care facilities use algorithms to conduct these matches, and also employ staff to manually review records—which is both costly and time consuming. This process, referred to as patient matching, often fails to accurately link records because of typos entered into the system; simi-

³ Centers for Medicare & Medicaid Services, “CMS Administrator Verma Unveils New Strategy to Fuel Data-driven Patient Care, Transparency,” Apr. 26, 2018, <https://www.cms.gov/newsroom/press-releases/cms-administrator-verma-unveils-new-strategy-fuel-data-driven-patient-care-transparency>.

⁴ The Pew Charitable Trusts, “Unique Device Identifiers Improve Safety and Quality” (2016), <https://www.pewtrusts.org/en/research-and-analysis/fact-sheets/2016/07/unique-device-identifiers-improve-safety-and-quality>.

⁵ Department of Health and Human Services Office of Inspector General, “Shortcomings of Device Claims Data Complicate and Potentially Increase Medicare Cost for Recalled and Prematurely Failed Devices” (2018), <https://oig.hhs.gov/oas/reports/region1/11500504.pdf>.

⁶ Food and Drug Administration, “FDA Fiscal Year 2020 Justification of Estimates for Appropriations Committees” (2019), <https://www.fda.gov/downloads/AboutFDA/ReportsManualsForms/Reports/BudgetReports/UCM633738.pdf>.

larities in names, birth dates or addresses among different patients; changing information, such as when individuals move or get married; and many other reasons.⁷

While some private sector technologies—such as referential matching, wherein third-party data are used to support matches—show promise, market forces have been unable to solve the patient matching problem for decades. In fact, patient matching requires collaboration between unaffiliated organizations, even competitors, that lack incentive to agree to a set of standards or develop systems that seamlessly exchange information.

Recognizing that effective patient matching is necessary to achieve interoperability, a provision in Cures championed by several Members of this Committee required the Government Accountability Office (GAO) to evaluate steps that ONC and the private sector have taken to address this challenge.⁸ The GAO report highlights a solution that many organizations—including a contractor to ONC—have proposed: consistent use of standards for demographic data.⁹

In parallel, Pew conducted 2 years of research—including interviews with health care providers, focus groups with patients, and contracted studies—to examine different ways to address matching challenges. The Pew research—summarized in a report released in October 2018—examined four main opportunities: the standardization of data; the use of unique identifiers or biometrics (such as facial recognition or fingerprint scans); a smartphone-based, patient-led solution; and referential matching.

ONC Should Advance Standardization to Improve Match Rates

While no single solution will completely solve the patient matching problem, our research identified concrete steps ONC can take to make meaningful progress to address this challenge.

First, ONC should require the use of standards for certain demographic data elements. In Pew-funded research published earlier this month, researchers at Indiana University studied whether the standardization of different data elements improves patient matching rates.¹⁰ Indiana University researchers attempted to match records in four data bases, standardized the data in those data bases, and then retried matching the records to determine whether that standardization yielded better results.

The research revealed that the standardization of address to the standard employed by the U.S. Postal Service (USPS), which details the preferred abbreviations for street suffixes and states, for example, would improve match rates by approximately 3 percent. One technology developer indicated that this would help their system match an additional tens of thousands of records per day. Separately, standardizing last name—while showing limited utility on its own—would further improve match rates if done in addition to address standardization.

ONC already proposes in the new recent regulations to embed address in the USCDI, but further improvements in match rates could be realized if the agency simply updates this provision to require use of the USPS standard when matching records. Software that automatically converts addresses to the USPS standard after they are input into the system is available in the commercial market; it is the reason many websites, for example, automatically make format changes to your address at the time you place an online order. Use of this standard would not necessarily require workflow changes at the point of patient registration, and would meaningfully help better link records using the general processes that providers already employ.

Second, the use of additional data elements could also improve match rates. For example, research published in 2017 showed that email addresses are already being

⁷ The Pew Charitable Trusts, “Enhanced Patient Matching Is Critical to Achieving Full Promise of Digital Health Records” (2018), <https://www.pewtrusts.org/en/research-and-analysis/reports/2018/10/02/enhanced-patient-matching-critical-to-achieving-full-promise-of-digital-health-records>.

⁸ Government Accountability Office, “Approaches and Challenges to Electronically Matching Patients’ Records across Providers” (2019), <https://www.gao.gov/products/GAO-19-197>.

⁹ Genevieve Morris et al., “Patient Identification and Matching Final Report” (2014), https://www.healthit.gov/sites/default/files/patient_identification_matching_final_report.pdf.

¹⁰ Shaun J Grannis et al., “Evaluating the Effect of Data Standardization and Validation on Patient Matching Accuracy,” *Journal of the American Medical Informatics Association* (2019), <https://doi.org/10.1093/jamia/ocy191>.

captured in more than half of patient records.¹¹ However, email address is not typically used for matching despite its widespread availability. ONC could improve match rates by identifying and including in the USCDI readily available data elements—potentially email address, mother's maiden name, or insurance policy identification number—that health information technologies should use for matching.

Given the effect of low match rates on patient safety and health care spending, as well as the failure of the market to address this challenge, Congress should work with ONC to ensure that the agency is requiring use of better standards for address and enabling the utilization of additional data elements for matching.

ONC Should Leverage Key Cures Provisions to Improve Usability and Safety

Along with barriers to the interoperable exchange of data among health care providers and to patients, Congress also recognized in Cures that subpar EHR usability hampers the ability of these systems to meet their full potential in delivering more efficient and safer care.

Usability refers to the layout and design of systems, and how their customization, configuration, and implementation affects their use by clinicians. Usability-related safety problems can emerge due to confusing interfaces, the need to develop workarounds to complete tasks, an overabundance of unnecessary alerts, and many other issues given the central role that EHRs increasingly have in helping clinicians order procedures, review health information, and obtain decision support.

Poor usability has two major consequences. First, ineffective usability can contribute to clinician burden and burnout, which can make them more susceptible to making errors.¹² Second, poor usability can contribute directly to patient harm through errors that occur when clinicians interact with the EHR. Pew collaborated with MedStar Health's National Center for Human Factors in Healthcare to examine the contribution of EHR usability to medication safety events in three health care organizations that treat pediatric patients. The research, published in *Health Affairs* last year, revealed that EHR usability contributed to 3,243 of 9,000 safety events examined.¹³ Of those usability-related events, more than 80 percent involved an inappropriate drug dose, and 609 of the usability-related events reached patients. In one case, a transplant patient missed days-worth of medication that would help prevent organ rejection. In another case, the blood transfusion for a newborn in critical condition was delayed due to the inability to create a record. These findings, including other research conducted by MedStar Health, found a clear link between the usability of EHRs and patient safety.¹⁴

ONC has an opportunity to improve system usability and patient safety under the existing authority provided to the agency by Congress as part of Cures. Congress has required that ONC create voluntary certification criteria for EHRs used in the care of children and develop a new EHR reporting program that could be used to identify and address usability issues. Patient safety could be greatly improved if ONC makes it a priority during their implementation of these provisions.

Pediatric EHR Certification Program Should Include Patient Safety

The health care needs of children and adults differ substantially; for example, pediatric patients often receive medication dosage amounts based on their weight. Given differences such as this, Congress included provisions in Cures for ONC to develop and adopt new voluntary criteria for EHRs used in the care of children.

In the proposed rule, ONC identified 10 clinical priorities for pediatrics, including weight-based dosing, use of biometric norms for growth charts, as well as age- and weight-specific dose range checking. The 10 clinical priorities selected by ONC right-

¹¹ Adam Culbertson et al., "The Building Blocks of Interoperability: A Multisite Analysis of Patient Demographic Attributes Available for Matching," *Applied Clinical Informatics* 8, no. 2 (2017): 322–336, <https://doi.org/10.4338/ACI-2016-11-RA-0196>.

¹² Louise H. Hall et al., "Healthcare Staff Well-being, Burnout, and Patient Safety: A Systematic Review," *PLOS One*, July 8, 2016: <https://doi.org/10.1371/journal.pone.0159015>; and Maria Panagioti et al., "Association Between Physician Burnout and Patient Safety, Professionalism, and Patient Satisfaction: A Systematic Review and Meta-analysis," *JAMA Internal Medicine* 2018;178(10):1317–1331. doi:10.1001/jamainternmed.2018.3713.

¹³ Raj M. Ratwani et al., "Identifying Electronic Health Record Usability and Safety Challenges in Pediatric Settings," *Health Affairs* vol. 37, no. 11: Patient Safety (2018): <https://doi.org/10.1377/hlthaff.2018.0699>.

¹⁴ Jessica L. Howe et al., "Electronic Health Record Usability Issues and Potential Contribution to Patient Harm," *Journal of the American Medical Association* 319, no. 12 (2018): 1276–78, <http://dx.doi.org/10.1001/jama.2018.1171>.

ly recognize many of the key clinical priorities for pediatric patients, including factors that research has shown contribute to patient safety problems. However, ONC should build on the provisions in its regulations to further improve the usability and safety of EHRs. Specifically, ONC could take concrete steps to tailor the certification program to pediatric care and improve patient safety:

- *Involve pediatric end users.* ONC currently requires EHR developers to involve at least 10 end users of the system in testing the system for certification. However, research suggests that some health information technology developers do not use appropriate end users to test their systems.¹⁵ ONC should clarify that any EHR developer seeking certification for pediatric functionalities should test the system using pediatric-focused clinicians, such as pediatricians and pediatric nurses. ONC could indicate, for example, that at least five of the 10 end-users participating in testing have pediatric expertise to obtain this certification.
- *Use pediatric-focused scenarios.* EHR developers currently use different testing scenarios—which mimic real clinic events and workflows—to demonstrate the functionality of their systems. To obtain certification for pediatric functionality, ONC should clarify that some of the testing scenarios must focus on situations involving children as patients.
- *Utilize mock pediatric data.* EHR developers use data on mock patients to demonstrate that their technologies meet ONC's certification program. ONC supplies some test data for those assessments. For a pediatric-focused certification, ONC should supply test data for mock pediatric patients and clarify that the test data used must involve mock data of children.

As ONC revises its approach to the voluntary certification program for EHRs used in the care of children, Congress should work with the agency to prioritize patient safety and system usability by ensuring that these common-sense approaches are incorporated.

Usability Criteria in EHR Reporting Program Should Include Safety

Through Cures, Congress also requires ONC to develop a reporting program to examine several different functions of EHRs, including system interoperability, security, usability and user-centered design. Findings obtained via this EHR Reporting Program, as envisioned by Congress, would be publicly available on ONC's website.

Late last year, ONC began implementing this provision. The agency selected a contractor to administer the program, and issued an RFI to obtain input on what data to collect on the use and functions of EHRs.¹⁶ While the recent regulations do not implement this provision from Cures, ONC is expected to issue associated rule-making in the future.

In response to the RFI, organizations representing clinicians, health technology professionals, and hospitals—among others—urged ONC to incorporate safety in the usability aspects of the program, though importantly not as a separate category.¹⁷ Pew provided recommendations to ONC on how to collect some of this information, and is collaborating with MedStar Health to identify additional opportunities for embedding safety into the usability aspects of the EHR Reporting Program.

Congress has provided ONC a prime opportunity to improve the usability—and consequently, safety—of EHRs. As ONC implements this program, this Committee should work with ONC to ensure that the usability aspects of the EHR Reporting Program focus on the facets of usability that contribute to unintended patient harm.

Conclusion

The bipartisan passage of Cures launched a new era for improving EHR interoperability and patient safety. As CMS and ONC continue their implementation of

¹⁵ Raj M. Ratwani et al., “Electronic Health Record Vendor Adherence to Usability Certification Requirements and Testing Standards,” *Journal of the American Medical Association* 314, no. 10 (2015): 1070–71, <http://dx.doi.org/10.1001/jama.2015.8372>.

¹⁶ Office of the National Coordinator for Health Information Technology, “Request for Information Regarding the 21st Century Cures Act Electronic Health Record Reporting Program,” *Federal Register*, Aug. 17, 2018, <https://www.regulations.gov/document?D=HHS-ONC-2018-0022-0001>.

¹⁷ Ben Moscovitch, “Medical Groups Urge Federal Government to Strengthen Health IT Usability, Safety,” Dec. 11, 2018, <https://www.pewtrusts.org/en/research-and-analysis/articles/2018/12/11/medical-groups-urge-federal-government-to-strengthen-health-it-usability-safety>.

Cures and other policies related to health information technology, this Committee can play an important role in the coming months by ensuring that these agencies carry out the goals expressed by Congress. Specifically, this Committee can conduct oversight in several key areas:

- Support ONC's efforts to require secure, standard API access to a wide range of health data, including clinical notes;
- Address the gap between Congress' requirements in the 21st Century Cures Act and ONC's current proposal to advance the release of more data—including all EHI—via APIs;
- Advance the addition of device identifiers to claims;
- Encourage ONC to address patient matching through the use of the USPS standard for address and the incorporation of additional demographic data elements in the USCDI;
- Press ONC to focus on addressing the risks to patient safety as part of the voluntary criteria for EHRs used in the care of children; and
- Urge ONC to embed safety in the usability aspects of the EHR Reporting Program.

By taking these steps in the coming months, Congress can provide patients and clinicians with better access to health data, reduce medical errors associated with the use of EHRs, and continue to ensure that the potential of the 21st Century Cures Act is fully realized on behalf of patients and clinicians across the country.

Thank you for holding this hearing today, and for your bipartisan commitment to improving the interoperability, usability and safety of electronic health records. I look forward to answering any questions you may have.

[SUMMARY STATEMENT OF BEN MOSCOVITCH]

Electronic health records (EHRs) have revolutionized how clinicians deliver care by equipping them with better tools to document patients' health status, safely prescribe medications, and otherwise order health care interventions. And, these tools have the potential to make it easier for patients and clinicians to have more complete and robust data to coordinate care across health settings.

Seeking to build on the improvements spurred on by the digitization of paper records, Congress recognized that gaps remain in realizing the full potential of EHRs to give patients their data, make care more efficient, and enhance patient safety. The 21st Century Cures Act (Cures) marked an important step toward addressing these gaps by optimizing the use of these technologies and addressing barriers to both the effective exchange of health data, known as interoperability, and the usability of these systems.

My testimony will focus on three key aspects of the recently proposed rules from the Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare & Medicaid Services (CMS) published earlier this month that address Congress' vision to improve the interoperability of health data and effective use of EHRs. Specifically, I will focus on:

- provisions enabling easier extraction and use of health data from EHRs via application programming interfaces (APIs), which enable different technologies to communicate;
- needed enhancements to better match patient records across different health care providers; and
- necessary improvements to the usability of EHR systems to address design and implementation factors that can both introduce burdens on clinicians and contribute to medical errors.

As CMS and ONC continue their implementation of Cures, this Committee has an opportunity to ensure that these agencies carry out the goals expressed by Congress. Specifically, this Committee can conduct oversight in several key areas:

- support ONC's efforts to require secure, standard API access to a wide range of health data;
- advance the addition of device identifiers to claims;
- encourage ONC to address patient matching through the use of the better standards for address and exchange of additional demographic data elements;

- press ONC to focus on addressing the risks to patient safety as part of the voluntary criteria for EHRs used in the care of children; and
- urge ONC to embed safety in the usability aspects of the EHR Reporting Program established by Cures.

By taking these steps in the coming months, Congress can provide patients and clinicians with better access to health data, reduce medical errors associated with the use of EHRs, and continue to ensure that the potential of the 21st Century Cures Act is fully realized for patients and clinicians across the country.

The CHAIRMAN. Thank you, Mr. Moscovitch.
Ms. Savage, welcome.

STATEMENT OF LUCIA C. SAVAGE, J.D., CHIEF PRIVACY AND REGULATORY OFFICER, OMADA HEALTH, INC., SAN FRANCISCO, CA

Ms. SAVAGE. Chairman Alexander, Ranking Member Murray, and the entire Committee, thank you for the opportunity to speak with you today.

From October 2014 through January 2017, I served as Chief Privacy Officer at ONC. I was the senior advisor for efforts to enable patients to get their health information through apps, and I provided technical assistance as you were drafting 21st Century Cures. After leaving ONC, I joined Omada Health, a late-stage, privately held healthcare company that focuses on chronic disease prevention and management, as well as supporting people with anxiety and depression. We utilize a secure digital communications platform to connect individuals to professional health coaches—no robots here. In the process, our participants share their health information just like they would with any other provider. We analyze that information in real time using proprietary data science and we feed actionable insights back to the individual and his or her health coach in real time on a secure app. The result is health care services that scale quickly and leverage those individual insights at the population health level.

One of my duties at Omada is to oversee its operations as a health care service provider and covered entity under HIPAA. In other words, we are just like a doctor's office under Federal law. That means that for our business, all of the HIPAA privacy, security, and breach notification rules apply. ONC proposes some bold reforms that could significantly impact the way facts are shared and that should foster innovation. Among the most impactful things they propose is that information blocking rules apply to business-to-business transactions. This is a logical and necessary next step to achieving the vision of an innovative healthcare system where health facts can flow appropriately and securely to benefit patients.

Included in my supplemental remarks is an article published yesterday by the American Bar Association Antitrust Law Journal where professors Martin Gaynor, Julia Adler-Milstein, and I examine the anti-competitive effects of B2B health information exchange absent ONC's rule. There are, however, three areas where ONC could push its vision more aggressively or the agency may want to consider unintended consequences of its rulemaking.

First, the ONC rule does strike a good balance on privacy and security. It has appropriate exceptions for privacy promises made

to individuals, for state or Federal laws, for securing one's own system, for system maintenance, and for safety. However, the rule proposes ongoing deference to organizational policies that might be at odds with democratically developed privacy laws that support interoperability. I encourage ONC to consider a transition or sunset period, during which institutions have time to adapt to app-enabled health information exchange, and to eliminate organizational policies that block appropriate flow of health facts.

Second, 21st Century Cures applies the prohibition against information blocking to developers of health information technology. However, the ONC proposal applies that only to a subset or certified health information technology, primarily certified EHRs. This limitation leaves out many types of health information technology where individuals' health facts are collected. For example, the proposed rule does not reach to health information technology in the emerging world of connected devices or software as a medical device, and it seems to omit any non-certified EHR, such as a lab or pharmacy electronic record system that is not certified.

Third, ONC proposes to allow technology developers to license interoperability elements. Licenses must not be so expensive or so restricted as to interfere with or stifle innovation, or create barriers to new entrance. As ONC finalizes the concept of interoperability elements it is critical that it clarify that the health facts within that software are never to be licensed. Omada made this point in our recent proposal response to the RFI from the Office for Civil Rights, and I have included those comments in my supplemental materials.

Finally, I applaud CMS's efforts to ensure that people have the same app-enabled access to their health facts from health plans as they do from providers. CMS expects that common consumer tools like laptops, smartphones, and apps will be used throughout the healthcare system. In the health care startup world, we use these common consumer tools every day to connect with and deliver valuable health care services to individuals.

We are excited to have the barriers to interoperability fall, and we look forward to a time when the barriers fall for us to be paid for efficacious health care services with these common consumer tools.

Thanks again for the opportunity to testify and I look forward to answering your questions.

[The prepared statement of Ms. Savage follows:]

PREPARED STATEMENT OF LUCIA C. SAVAGE

U.S. Senate Committee on Health, Education, Labor, and Pensions
Implementing the 21st Century Cures Act: Making Electronic Health Information Available to Patients and Providers
March 26, 2019

Testimony for Lucia C. Savage, JD

Chairman Alexander, Ranking Member Murray and the entire Committee: Thank You for the opportunity to submit these detailed written comments. Part 1 includes the remarks I made as testimony before the Committee. Part 2 adds some important details on how Omada operates as a health care service provider under HIPAA and how ONC's proposal will in many ways help us grow. It also provides some additional detail on the areas where we think ONC could do better.

Part 1:

From October 2014 through January 2017, I served as the Chief Privacy Officer at the Office of the National Coordinator for Health Information Technology. I was the senior privacy advisor for efforts to enable patients to get copies of their health information through apps, and I provided technical assistance as 21st Century Cures was being drafted.

After leaving ONC, I joined Omada Health, a late-stage, privately-held health company focused on chronic disease prevention and management, as well as supporting those dealing with anxiety and depression. We utilize a secure digital communications platform to connect individuals to professional coaches. In the process, our participants share their health information, just as they would with any healthcare provider. We analyze that data in real-time using proprietary data science techniques, and feed actionable insights back to the participant and his or her coach. The result is health care services that adapt in real time to the needs of individual participants, while maintaining the ability to scale quickly and leverage those individual insights at a population health level. One of my duties is to oversee Omada's operations as a healthcare service provider and HIPAA-covered entity, legally just like a doctor's

office under federal law. This means that all of the HIPAA Privacy, Security, and Breach Notification rules apply to us.

ONC proposes bold reforms that could significantly impact the way personal health facts are shared and that should foster innovation. Among the most impactful is that information blocking rules apply to health information technology operating in a business-to-business environment. This is a logical, and necessary next step in achieving the vision of an innovative healthcare system where health facts can flow appropriately and securely to benefit patients. Included in my supplemental materials is an article published yesterday in the American Bar Association's Antitrust Law Journal, where Professors Martin Gaynor, Julie Adler-Milstein and I examine the anti-competitive aspects of the B2B health information exchange absent ONC's rule.

However, there are three issue areas where either ONC could push this vision more aggressively, or where the agency may want to consider unintended consequences from its rulemaking.

First, while the ONC rule strikes a good balance on privacy and security, with appropriate exceptions for privacy promises made to individuals, state or other federal law, securing one's own system, system maintenance, and safety, the rule proposes ongoing deference to organizational policies that might be at odds with democratically-developed privacy laws that support interoperability. I encourage ONC to consider a transition or sunset period, during which institutions have time to adapt to app-enabled authorized sharing of health facts, and to eliminate organizational policies that block the free flow of health information.

Second, the 21st Century Cures Act applies the prohibition against information blocking to developers of "health information technology" as defined in HITECH Section 13101(5). The ONC proposal, however, applies only to a subset of this category, certified electronic health records developers. This limitation leaves out many types of health information technology where individuals' health facts are collected. For example, the proposed rule does

not reach to health information technology in the emerging world of connected devices or Software as a Medical Device, and seems to omit any non-certified EHR, such as a lab or pharmacy electronic records system that is not certified.

Third, ONC proposes to allow technology developers to license "interoperability elements." Licenses must not be so expensive or restrictive as to stifle innovation or create barriers to entry. As ONC finalizes the concept of interoperability elements, it is critical that it clarify that health facts themselves are never to be licensed. Omada made this point in our recent response to the RFI from the Office of Civil Rights; I have also included that comment letter in my supplementary materials.

Finally, I applaud CMS' efforts to ensure that people have the same app-enabled access to their health facts from plans as from providers. CMS "expects" that "common consumer tools" like laptops, smartphones and apps will be used throughout the healthcare system (84 Fed. Reg. 7628 (March 4, 2019)). In the healthcare start up world, we use these "common consumer tools" every day to connect with, and deliver valuable health care services to, individuals. We are excited to have barriers to interoperability fall and we look forward to the time when barriers fall to being paid for efficacious health care services deployed with common consumer tools.

Thank you again for the opportunity to testify. I look forward to answering your questions.

Part 2:

A: Omada Is a Provider and Covered Entity under HIPAA

Despite our digital communications and data science platform, Omada is and operates as a health care service provider under federal law, and thus as a covered entity under HIPAA. Additional detail is set forth below.

HIPAA applies to three types of “providers” (45 CFR 160.103): acute inpatient hospitals, professionals, and “any other entity that supplies health care services and bills electronically for them. The regulation states:

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business [Emphasis added].

Omada falls into that third category, and has operated as a provider and covered entity since its founding in 2011.

As a provider and covered entity, we are legally just like a doctor’s office or hospital. This means that when we collect, use, or disclose an individual’s health information, we do so under HIPAA’s exacting standards. Further, because of how seriously we take our participant’s privacy, and as our Terms of Use, Privacy Policy and HIPAA Notice of Privacy Practices make clear, we do not sell data from our participants, even in a de-identified form. So, we are quite distinct from an array of social media and retail apps. The same is not true for an app purchased from an app store that is not offering a reimbursable health care service. In some ways, it is good that as a nation we are having a debate about these ad-tech based apps and privacy at the same time that we are bringing the automation of apps to traditional healthcare. This is because the debate itself raises consumer awareness and that awareness makes sure they are choosing health care modalities that are right for them.

For us, HIPAA's approach to privacy, health fact sharing, and interoperability have enabled us to build a business based on delivering demonstrable health outcomes -- then charging our customers based on those outcomes. Put simply, if we don't deliver improved care, better outcomes, and value to our customers, our business does not work.

For example, for our flagship Diabetes Prevention Program (DPP) healthcare service, the Centers for Disease Control (which oversees recognition standards for DPP) identifies weight loss as the core clinical indicator of success. In our DPP, after paying an initial account set up fee, Omada is paid for its services only if it can prove weight loss. Our outcomes-based model for this program therefore depends on our ability to use the health information we collect from our participants to measure outcomes. It also depends on our ability to share those outcomes, sometimes in an identifiable way, with the organization paying for our health care service, such as a health plan, a clinic, or a self-insured employer. We detailed some examples of our information sharing practices in our response to OCR's recent Request for Information. I have attached that response to this detailed statement.

Given our business model, we already exchange health information regularly where we are legally permitted to do so and it is appropriate, even in a B2B transaction; for example, reporting book-of-business results back to a large health plan via a custom, secure reporting feed or even an API we develop. We believe ONC's push into B2B transactions will facilitate more, and easier, less expensive, secure transactions with a wider variety of business partners, allowing Omada to grow in new ways.

In the past, we declined to be an authorized app within the app store of various certified EHR vendors because we concluded that the price tag was too high and the information terms were too constrained. For example, as a health care provider in our own right, if we acquire a health fact like a blood sugar test result from another provider, we cannot be in a position where we cannot use that fact in our outcomes-based model, or cannot disclose that health fact to other providers or to the individual without paying more fees. We think that ONC's proposal will

go a long way towards solving this particular problem, so long as the EHR developer's ability to license "interoperability elements" prohibits attempts to license health facts.

B: Health Facts vs. "Interoperability Elements": As a health care service provider who develops our own software to deliver our services, we handle PHI in ways quite different from traditional healthcare. For example, our intake questionnaire and clinical screener is filled out 100% online, not through a clipboard in a waiting room. This means, however, that from a software engineering and health care services perspective, we have a keen sense of what in our entire database is a meaningful health fact (a person's weight for example) and is not meaningful because it is a piece of metadata (the log file of the scale manufacturer showing it sent the scale weight to us for example). And, we could share just health facts with a person or another business (such as raw data in a spreadsheet sent securely) or we could share those health facts in a more meaningful, structured way.

At Omada, we think ONC means for the "interoperability elements" to be like the meta data or the external structure to the health facts in the examples above. We are all-in on interoperable health facts. And we hope that other health information technology developers of all kinds would be too. But, because ONC's rule imposes few limits on the scope of a license to "interoperability elements," and does not state that health facts are not licensable, we worry that technology developers will license an "interoperability element" only when it is in their self-interest to do so, not for the good of the patient. Worse, a health information technology developer might only license "interoperability elements" in anti-competitive ways. In fact, in writing the accompanying article for the American Bar Association Antitrust Law Journal, my co-authors and I discuss how under Supreme Court precedent, health facts occur in nature and therefore cannot become a single entity's intellectual property.

We also have talked to other health start-ups of various sizes and they share our concern that the proposal to license "interoperability elements" is potentially the exception that undermines the overall goal of interoperability.

C: What Health Information Technology Does ONC's Proposal Cover? In my oral testimony, I described the fact that ONC's proposal does not cover all health information technology. I would like to elaborate.

21st Century Cures amended prior definitions of the Health Information Technology for Clinical Health Act (HITECH) by adding a definition of "interoperability" that applies without exception to all "health information technology," also as defined in HITECH. HITECH section 3000(1) has one definition of "certified electronic health records technology" and a separate and distinct definition of "health information technology" (Id.). "Health Information Technology is

"(5) . . . hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information."

Cures applies its definition of "interoperability" and its concomitant prohibition against information blocking to "health information technology", not just to certified EHRs. Cures states:

"(10) INTEROPERABILITY.—The term 'interoperability', with respect to health information technology, means such health information technology that—
 "(A) enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user;
 "(B) allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and
 "(C) does not constitute information blocking as defined in section 3022(a)."
 [Emphasis Added. P. Cures section 4003(a)(2)(10), P. Law 114-255 (December 163, 2016), codified at 42 USC 300jj-52.

Cures then goes on to state that information blocking is prohibited:

(B)(i) if conducted by a health information technology developer, exchange, or network, such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information; [Id. section (3022(a)(1)(B)(1). [Id. creating section 3022 of the Public Health Service Act. Emphasis added]

Cures then charges ONC with developing rules about what does not constitute information blocking, and that charge is not limited to ONC's traditional regulatory authority over certified EHRs. Rather, that charge states:

“(3) RULEMAKING.—The Secretary, through rulemaking, shall identify reasonable and necessary activities that do not constitute information blocking for purposes of paragraph (1).

And it is paragraph (1)(B)(i) that applies the term information blocking to “health information technology.”

Based on the above provisions, Omada believes that Congress in Cures authorized rules against information blocking that reach beyond certified EHR developers. In contrast, ONC’s rule, as proposed, applies only to certified EHR developers, on whom is imposed the certification obligation of developing the open-specification read-only APIs, using the Fast Health Interoperability Resource (FHIR) standard (see generally 84 Fed. Reg. 7465-7508, March 4, 2019). As a result of comparing Cures to ONC’s rule, we concluded that many collectors and custodians of digital health facts are not prohibited from information blocking. Two potential examples follow:

Example 1: A pathologist uses a proprietary health information technology system developed for her by a third party to store lab data. That health information technology system is not certified. The developer is not required to make a standards-based API available for the pathologist’s information sharing needs.

Example 2: A manufacturer sells a leg brace that contains a radio frequency chip and a gyroscope, to measure mobility and gait after a joint replacement. That manufacturer’s proprietary health information technology system that is not certified. Even if the manufacturer bills Medicare for monitoring services and therefore is a HIPAA covered entity, that proprietary health information technology system is not required to make the health facts it contains available to individuals, their physicians or their other providers in a standards-based, interoperable manner.

We recognize that ONC or the Office of Inspector General might not have the robust authorities over health information technology developers that already exist over certified EHR

developers. But we see this as an enforcement authority problem to be solved next, not as a reason NOT to extend the prohibition against information blocking to all developers of health information technology. If we truly want interoperable health facts to flow where the individual needs them to manage their care using common consumer technologies (84 Fed. Reg. 7628, March 4, 2019), then information blocking of health facts must be prohibited everywhere.

D: Privacy Policies vs. Privacy Laws: In my testimony, I expressed concern with ONC's proposal to allow organizational policies enacted transparently before ONC's rule took effect, to continue to be enforced without constituting information blocking. See proposed 45 CFR 170.202(b). There are many organizational policies which are necessary for appropriate privacy practices, and in fact HIPAA requires that covered entities have written policies. We have many at Omada. But all organizational policies are not created equal, and ONC's rule should not give deference to policies that unnecessarily thwart interoperability. Here are two examples of such policies that should not be allowed to persist.

Example 1: Although the physician's office offers its patients secure identity credentials to message their doctors through their certified EHR, their organizational policy prohibits individuals from asking for a copy of their own health records using the portal. Rather, if an individual does this, office staff requires that the individual contact by fax or mail a remote health information management office. *Bitter [Release of Information] Irony, Journal of AHIMA* November/December 2017, page 32: http://www.ahimajournal-digital.com/ahimajournal/november_december_2017?pg=33#pg33.

Example 2: A hospital system has a written policy that it will not allow individuals to transmit (or download a copy of) their health facts to any technology service that is not approved by the system's information security office, even though there is no evidence that this type of download threatens the security of the hospitals' systems.

ONC's proposal does require that historic policies meet a facts-and-circumstances test for reasonableness, being carefully tailored, etc. But this refinement fails to account for the

world we have now, where the full efforts of Congress and the Executive Branch are working to ensure consumers can use everyday technology to manage their health, yet faxes remain ubiquitous. In this situation, it would be far better for patients and their everyday technologies if ONC and HHS required providers to sunset old policies by the effective date of the rule, and to replace them with policies that actually meet the prohibition against information blocking, instead of investigating policy by policy the facts and circumstances of each situation, while patients and their caregivers are waiting for their health facts.

D: Which Providers Does ONCs Proposal Cover? Before concluding I want to be clear that, as proposed, ONC's rule would not apply to Omada Health, because ONC proposes that the only providers within the rule's scope are those identified in the Social Security Act, not entities who, like Omada, fall into that third category of "any other" health care service provider. ONC has requested input on this point, and Omada expects to comment that ONC should use the HIPAA definition of health care provider so that providers of healthcare services of all types cannot block the appropriate interoperable flow of health facts to other providers. We recognize this change will sweep Omada and many others into the ambit of the ONC rule, and we are okay with that. As a health care service provider who uses digital health information to provide personalized services to individuals and to prove our value proposition to payers paying for those services, and with a company value of #ParticipantsFirst, we want to make it easy for our participants to get the healthcare that is right for them, even if it means taking health facts we collected and sharing those facts with another provider.

Respectfully submitted,



Lucia C. Savage JD
Chief Privacy and Regulatory Officer
Omada Health, Inc.

Attachments

- A:** Savage, Lucia, et al. *Digital Health Data and Information Sharing: a New Frontier for Healthcare Competition*, 82 ANTITRUST LAW JOURNAL NO. 2 (2019).
- B:** Comments of Omada Health, Inc. to U. S. Department of Health and Human Services Office for Civil Rights in Response to Request for Information, Docket # 0945AA00, submitted February 10, 2019.
- C:** Savage, L., *ONC's Proposed Rule On Information Blocking: The Potential To Accelerate Innovation In Health Care*, Health Affairs Blog, February 15, 2019.

[SUMMARY STATEMENT OF LUCIA SAVAGE]

Lucia C. Savage, JD, is Chief Privacy and Regulatory Officer at Omada Health. From October 2014 to January 2017 she served as Chief Privacy Officer at the Office of the National Coordinator for Health IT (ONC). At ONC, Ms. Savage was the senior privacy advisor on an individual's rights to get their own health data electronically and by app. She also provided technical assistance in drafting the health information technology provisions of Cures.

Her current employer, Omada Health, is a late-stage, privately-held health care company focused on chronic disease prevention and management, as well as supporting those dealing with anxiety and depression. Omada utilizes a secure digital communications platform to connect individuals to professional coaches. In the process, its participants share their health information, just as they would with any healthcare provider. Omada is a health care provider and a covered entity under HIPAA, legally just like a doctor's office. The HIPAA Privacy, Security and Breach Notification rules apply to Omada.

Ms Savage will testify that:

- While the ONC rule strikes a good balance on privacy and security, the rule proposes ongoing deference to organizational policies that might be at odds with privacy laws that support interoperability. Rather than deference, a transition or sunset period might be appropriate for organizational policies.
- The prohibition against information blocking should apply more widely to "health information technology" (a term defined in 21st Century Cures), and not just to certified EHR developers. A more expansive reach will more effectively and quickly assure that individuals can get and use their health facts wherever they are collected in the healthcare system.
- ONC should clarify its proposal on licensing "interoperability elements" to ensure that an individual's *health facts* are never subjected to such licenses, and that the licenses themselves are not so strict or expensive as to inhibit innovation.
- Omada is fully committed to interoperable exchange of health facts, and sees the full implementation of these rules as an opportunity for growth, even if it means that Omada, which is not currently a provider type proposed to be covered by the rule, is in scope for the rule's reach.
- CMS timely proposes to require health plans to make individuals' health facts available from plans on the same conditions as those facts are available from providers. This proposal, if finalized will ensure consumers can continue to use everyday consumer tools, like laptops, smartphones and apps to get care and manage their health.

The CHAIRMAN. Thank you, Ms. Savage.
Dr. Rehm, welcome.

**STATEMENT OF CHRISTOPHER REHM, M.D., CHIEF MEDICAL
INFORMATICS OFFICER, LIFEPOINT HEALTH, BRENTWOOD,
TN**

Dr. REHM. Thank you very much. Chairman Alexander, Ranking Member Murray, and Members of the Senate HELP Committee, thank you for the opportunity to testify before you today.

As Chairman Alexander stated, I am the Chief Medical Informatics Officer at LifePoint Health. And LifePoint Health is a provider organization that provides care in over 89 communities in 30 states across the United States. Our clinical technology environment consists of over 20 distinct inpatient and ambulatory EHRs, and countless vendor partners providing departmental and point solutions. It takes a tremendous amount of effort for our team to build, configure, and tie together these systems so that our medical teams are set up for success to provide safe, efficient, high quality care to every patient we see in the communities that we serve. De-

spite our best efforts, our providers and patients are impacted by the lack of interoperability daily.

The desire to make electronic health information freely available spans the political spectrum and has been a long-standing goal of both patients and medical teams. I am here today as a healthcare provider, someone who has taken care of patients, and supports others who take care of patients. I love my work and my colleagues love their work, but this is hard. The lack of interoperability associated with our medical technology, some of it related to the technology itself, some of it related to the regulations that apply to this technology, make it harder to do our job. Electronic medical records, medical devices, and patient monitors are supposed to help us be better caregivers. Instead these technologies frequently add to the complexity and burden that we feel.

Today, I will touch on some of the causes and offer suggested solutions to lessen the provider burden and move toward the interoperable future that we all desire. First, providers do not build these technologies. We purchase them from vendors. It is commonplace that vendors develop products that do not interoperate. Many vendors release products that meet minimum standards for ONC certified technology. Their contracts do not cover the maintenance for updating them when new regulations come about. It is up to the provider organizations to cover the cost and the burden of implementing these add-ons to cover new regulations.

In addition to being costly, upgrades take time. Where we are often given 6 months to comply with CMS regulations, it can take up to 12 months for a provider organization to review, configure, test, train all of our end users, and deploy numerous vendor technologies, ensuring that we do not break hundreds of existing custom interfaces that are already in place. We applaud the ONC proposal to require health IT vendors demonstrating that their products are usable for patients and providers in a real-world environment. We need our health care technology and software systems to work in real life settings in concert with other vendor technologies if we expect to meet the needs of patients and providers now and in the future.

Second, where the HITECH Act catalyze the new from paper to digital records via provider-based incentives and penalties, unfortunately it did not address or create the underlined infrastructure of interoperability to enable data liquidity across technologies. Provider organizations have been left to bridge the gap with interface engines, workarounds, and manual processes with varying degrees of success and reliability. This lack of infrastructure is troublesome for a number of reasons, from privacy and security challenges to the ability of providers to seamlessly send and receive data. For example, the CMS proposed rule would require hospitals to send electronic notifications when a patient is admitted, discharged, or transferred as part of the conditions of participation.

In order to comply with the condition of participation, providers must clearly understand the requirement and the objective compliance measure. This proposal lacks both of those elements, which is concerning given the tremendous penalties hospitals face for failing to comply with conditions of participation. Instead, I encourage the administration to focus on its current activities to improve inter-

operability, such as continuing to advance the goals of the Trusted Exchange Framework and Common Agreement, known as TEFCA, and vendor accountability for the products that they develop. Another victim of this lack of infrastructure is patient-provider trust that data will be secure and used appropriately. The proposals both envision that unvetted third-party applications will be accessing patient electronic health data via open APIs.

Personally, I like the idea of controlling my own data, but the truth is the vast majority of us, me included, do not read the entire terms of use agreement on every app or website that we enroll in. We believe our data is more private and secure than it actually is. The entrance of non-health care actors into the healthcare market, particularly those that fall outside of HIPAA requirements, necessitates strong principles of trust and security. One approach that supports innovation and provides the needed safeguards to govern personal electronic health data is an industry backed process to independently vet these applications to ensure they meet all relevant security standards, use data appropriately and in line with consumer expectations, and for those applications that offer medical advice, is the advice clinically sound?

In closing, Government policies must allow digital health information to be exchanged in a way that protects and prioritizes the health interests of individuals and the health systems and clinicians who care for them. In this technological age, it is important we all remember that deployment of health information technology, interoperability, data exchange, and security are all in service of delivering the highest quality care. It is not about the technology. It is about the patients, their care, and their outcomes.

Thank you for the opportunity to speak today. I have additional information on these topics in my written testimony I hope you will also consider.

[The prepared statement of Dr. Rehm follows:]

PREPARED STATEMENT OF CHRISTOPHER REHM

Chairman Alexander, Ranking Member Murray, and Members of the Senate HELP Committee, thank you for the opportunity to testify before you today. It is an honor to be invited to participate in today's discussion.

My name is Christopher Rehm. I am a physician and the Chief Medical Informatics Officer at LifePoint Health. LifePoint Health is a provider organization that delivers Acute, Emergency, Post-Acute and Outpatient care for over 85 communities in 30 states. Our clinical technology environment consists of 10 different Inpatient electronic health records (EHRs), greater than 10 Ambulatory EHRs, and countless vendor partners providing departmental, ancillary and point solutions. My team and I work with our hospitals and providers to build, configure and tie together these systems so that our providers are set up for success to provide safe, efficient, high quality care to each and every patient we see in the communities we serve.

The desire to make electronic health information freely available spans the political spectrum and has been a long-standing goal of patients and those who care for them. These proposed rules represent an important step in our journey to achieve the ultimate aims of a truly person-centric health care delivery system. I applaud this Committee and Federal health agencies for recognizing the need to improve existing regulations to keep pace with evolving technologies and innovations. I support the ability of patients to have access to their health information and understand that the future health of our population and the sustainability of our industry depends upon the timely, efficient movement of data.

There are several ways that we can choose to navigate toward this future state. The new Centers for Medicare & Medicaid Services (CMS) and Office of the National Coordinator for Health Information Technology (ONC) rules represent the in-

terpretation of the great work that this Committee did on the 21st Century Cures Act. And we support the general direction of the rules. Having said that, if we do not take time to consider how these new rules may affect certain stakeholders in the health care ecosystem, especially providers and patients, the decisions that we make today may have unintended consequences for years to come.

Cost and Regulatory Burden of Health IT on Providers

I am here today as a health care provider—someone who has taken care of patients and oversees others who take care of patients. I love my work because there is no other place or profession where people are so consistently caring and devoted to alleviating human suffering caused by disease. But many of the forces facing hospitals, doctors, nurses and patients make it really hard to do the job well.

Some of the most stifling forces are those imposed by our technology and the regulatory policies that govern them. Electronic medical records, devices, diagnostics, monitors—these are all things that are supposed to augment our practice, to help us be better caregivers. Instead, our technology only adds to the complexity and burden that we feel. Part of the problem is that there is no underpinning that supports a system-of-systems for technology in the health care industry. No one has established the rules of the road for data exchange, like industries such as banking, aviation, cable, telecom and others did decades ago. Vendors develop products and services that do not interoperate. In order to support some level of communication across systems, the market has created even more products and services—like integration and interface engines—that help to glue together these proprietary technologies. But it is up to the providers to bear the burden and cost of implementing and integrating all of these separate pieces, and it doesn't stop once we have bought them.

Many vendors release products that meet minimum viability standards for ONC certified technology, but their service contracts do not include the cost of maintaining and updating them to remain compliant with new regulations. Coming into compliance with new or updated regulations generally involves upgrading the EHR or device to modify how information is documented, collected and reported.¹ The average-sized community hospital (161 beds) spends nearly \$760,000 annually on information technology investments needed to support compliance with Federal regulations.² These IT changes and associated costs are crushing our industry where margins are already thin.

Additionally, these upgrades take time. Six months is simply not enough time for a provider organization to review, build, configure, test, train and deploy numerous vendor technologies following new releases to be ready to meet the regulatory deadlines for reporting under the CMS programs. IT product design, testing and implementation requires lead time, particularly when it involves a vendor. Time frames for implementation and updates need to be adjusted to reflect what is reasonable and acceptable, for instance, 12 months after a Generally Available release date from a vendor.

We applaud the ONC proposal to require health IT vendors to demonstrate that their products are usable to patients and providers in a real-world environment. Any solution can work in a vacuum. We need our health care technology and software systems to work in real life settings and in concert with many other vendor technologies if we expect them to meet the needs of patients and providers now and in the future.

While the HITECH Act catalyzed the move from paper to digital records via incentives and penalties on health care providers, it did not, unfortunately, address or create an underlying infrastructure of interoperability to enable data liquidity among technologies. Think about this for moment: it is the equivalent of telling people they must buy cars and move those cars from place to place, but there are no roads and no agreed upon design for the roads, let alone the funding to actually pay for the construction. In the case of EHRs, it is the provider organizations who have been left to bridge the gap with everything from integration and interface engines, to workarounds that lead to significant “clicks” for clinicians, to even a combination of electronic and manual processes.

Health care providers are trying hard to persist in their dedication, but the increasing pressure of having to do more with less weighs heavily on these well-meaning people. Atul Gawande's November 2018 article was aptly titled “Why Doctors

¹ Assessing the Regulatory Burden on Health Systems, Hospitals and Post-acute Care Providers. *American Hospital Association*. February 2018.

² Assessing the Regulatory Burden on Health Systems, Hospitals and Post-acute Care Providers. *American Hospital Association*. February 2018.

Hate Their Computers,”³ and a joint Fortune and Kaiser Health News article just last week highlighted and astounding average of 4,000 clicks per shift for an emergency room doctor.⁴ Clinicians need our support, encouragement, and appreciation for the value they bring to patients and to society.

As a health care provider, I support the ability of patients to have access to their health information and the sharing of information across disparate technologies, systems, and providers. The CMS proposed rule would require, as part of the Medicare Conditions of Participation (CoPs), hospitals to send electronic notifications when a patient is admitted, discharged, or transferred. Hospitals would be required to send these notifications to other facilities, providers, or community care providers with an established patient relationship who the hospital has reasonable certainty will receive the notifications. While I support this idea directionally—and look forward to achieving this level of information sharing—this is unfortunately putting the cart before the horse. It sounds like it would be simple to implement, but there are numerous unanswered questions and operational considerations. For example, not all EHRs can generate these messages—and this functionality is not required of vendors under the ONC certification rules. And if a provider is not connected to a health information exchange or similar network, of which the most advanced ones are quite costly, it is an enormous undertaking—in both time and money—to connect to these other providers and facilities individually.

In order to comply with a CoP, providers must clearly understand what it is they must do and how they will be surveyed and judged to determine compliance. This proposal lacks both of those elements, which is concerning given the tremendous penalties hospitals face for failing to comply with CoPs, including termination from the Medicare program. Instead, I encourage the administration to focus on its current activities to improve interoperability, such as continuing to advance the goals of the Trusted Exchange Framework and Common Agreement (TEFCA), as well as its proposals in this rule to further ensure vendors are accountable for the products they develop. The responsibility for interoperability cannot and should not be borne solely by providers, and there are plenty of things that vendors, business associates, plans and other organizations can and should be expected to do and contribute.

Patient Privacy and Security

It is clear that Congress and this administration are committed to solving the issue of interoperability and achieving complete patient access in the U.S. health care system. So far, the administration is relying on third party apps and the private market to solve these problems. The rules state that they wish to “enable patients to access their health information electronically . . . to make the data available through an application programming interface [API] to which third party software applications connect to make the data available to patients.”⁵

Providing unvetted third party applications fairly open access to patient digital health data concerns me as both a clinician and a consumer. I am well-aware of the argument that it is the patient’s prerogative to specify where and to whom their data goes. Personally, I like the idea of controlling my own data. But reality does not always align with our ideas, particularly when it comes to our personal information—whether health-related, financial, or even demographic. The truth is that the vast majority of us, myself included, do not read the entire “terms of use” agreement on every app or website that has some of our personal information, and we often mistakenly believe our data is more private or more secure than it actually is.

While it may be tempting to allow access to personal digital health information for any and all entities who claim to operate under the banner of “promoting care coordination,” we would be wise to take a lesson from the consumer data privacy events of the past few years. Millions of individuals were surprised and angry to learn how Facebook was using and selling their data, while other consumers weren’t even aware that all their financial information is funneled through three to four major credit bureaus, two of which experienced major breaches in the last few years.

Digital data is the currency of the modern technology ecosystem and marketplace. There are fortunes to be made in mining and monetizing your personal digital health data. New rules and processes that govern and protect digital health data

³ Atul Gawande, *Why Doctors Hate Their Computers*, The New Yorker (Nov. 12, 2018), <https://www.newyorker.com/magazine/2018/11/12/why-doctors-hate-their-computers>.

⁴ Erika Fry and Fred Schulte, *Death by a Thousand Clicks: Where Electronic Health Records Went Wrong*, Fortune and Kaiser Health News (Mar. 18, 2019), <http://fortune.com/longform/medical-records/>.

⁵ 84 Fed. Reg. 7610, 7612 (Mar. 4, 2019).

must be sensitive to the reality that not all covered entities, business associates, and third parties are created equal. Particularly with regard to entities that fall outside of the HIPAA requirements, it is imperative that patients, their families, providers, and consumers can trust that these applications—and the data both sent to and received from them—are secure, private, and clinically sound.

The vision for the future is one in which a patient's data flows between her/his care providers, the patient and her/his providers, and between the patient's personal electronic device and the provider.

That vision presupposes that data is vetted, clinically sound and comes from a trusted source. The reality is that neither clinicians nor patients have the ability to validate that it is trusted data.

A Trust-Based Approach

I believe there are ways to support the innovation coming from the external marketplace while providing the needed safeguards to govern personal digital health data. The entrance of non-health care actors into the health care market—particularly those that fall outside of the HIPAA requirements—necessitates strong principles for trust and security. One such idea is an industry-backed trust platform technology architecture, supported by an appropriate governance model.

This is a wide-ranging solution that would encompass all health-related digital information on a single platform architecture. In the meantime, I also encourage a smaller scale solution to address privacy, security, and clinical efficacy of third-party applications, specifically an industry-backed process to independently vet these applications to ensure they are meeting all relevant security standards; are using data appropriately and in line with consumer expectations; and, for those applications that offer medical advice, are clinically sound. Such a process will go a long way toward ensuring trust while removing the burden of this process from consumers and providers.

What Federal Policy Can Do

Policymakers must strike a balance between their desire to make personal digital health information available and the burdens that these requirements place on health systems under proposed timelines. Government policies must allow digital health information to be exchanged in a way that protects and prioritizes the interests of individuals—and the health systems and clinicians who care for them—while allowing the marketplace to innovate and interact in a responsible and controlled way.

In this technological age, it is important we all remember that the deployment of health information technology, interoperability, data exchange, privacy and security are all in service of patients receiving and providers delivering the safest, highest quality care. It is not about the technology; it is about patients, their care, and their outcomes.

[SUMMARY STATEMENT OF CHRISTOPHER REHM]

Chairman Alexander, Ranking Member Murray, and Members of the Senate HELP Committee, thank you for the opportunity to testify before you today.

My name is Christopher Rehm. I am a physician and the Chief Medical Informatics Officer at LifePoint Health. LifePoint Health is a provider organization that delivers Acute, Emergency, Post-Acute and Outpatient care for over 85 communities in 30 states. Our clinical technology environment consists of 10 different Inpatient EHR's, greater than 10 Ambulatory EHR's, and countless vendor partners providing departmental, ancillary and point solutions. My team and I work with our hospitals and providers to build, configure and tie together these systems so that our providers are set up for success to provide safe, efficient, high quality care to each and every patient we see in the communities we serve.

The desire to make electronic health information freely available spans the political spectrum and has been a long-standing goal of both patients and medical teams. I am here today as a health care provider—someone who has taken care of patients and supports others who take care of patients. I love my work—and my colleagues love their work. But sometimes health IT and the regulatory policies that govern them are stifling and make it harder to do our job. Electronic medical records, medical devices, and patient monitors are supposed to help us be better caregivers. Instead, these technologies frequently add to the complexity and burden that we feel.

I will touch on some of these causes today as well as offer suggested solutions to help alleviate a portion of this burden to support providers as we move toward the interoperable future we all desire.

First, providers do not build these technologies; we purchase them from vendors. I have frequently found, however, that vendors develop products and services that do not interoperate. Many vendors release products that meet minimum standards for ONC certified technology, and their contracts do not include the cost of maintaining and updating them to remain compliant with new regulations. It is up to the providers to bear the burden and cost of implementing and integrating these separate pieces.

In addition to being costly, upgrades take time. While we are often given 6 months to comply with CMS regulations, it can take up to 12 months for a provider organization to review, configure, test, train and deploy numerous vendor technologies, ensuring we did not break hundreds of custom interfaces, following new releases.

We applaud the ONC proposal to require health IT vendors to demonstrate that their products are usable for patients and providers in a real-world environment. We need our healthcare technology and software systems to work in real life settings and in concert with many other vendor technologies if we expect to meet the needs of patients and providers now and in the future.

Second, while the HITECH Act catalyzed the move from paper to digital records via provider-based incentives and penalties, it did not, unfortunately, address or create an underlying infrastructure of interoperability to enable data liquidity across technologies. Provider organizations have been left to bridge the gap with interface engines, work arounds and manual processes—with varying degrees of success.

This lack of infrastructure is troublesome for a number of reasons—from privacy and security challenges to the ability of providers across the country to send and receive data. For example, the CMS proposed rule would require hospitals to send electronic notifications when a patient is admitted, discharged, or transferred as part of the Conditions of Participation (CoPs).

In order to comply with a CoP, providers must clearly understand the requirement and the objective compliance measure. This proposal lacks both of those elements, which is concerning given the tremendous penalties hospitals face for failing to comply with CoPs, including termination from the Medicare program. Instead, I encourage the administration to focus on its current activities to improve interoperability, such as continuing to advance the goals of the Trusted Exchange Framework and Common Agreement (TEFCA) and vendor accountability for the products they develop.

Another victim of this lack of infrastructure is patient and provider trust that data will be secure and used appropriately. The proposals envision unvetted third party application access to patient digital health data via open APIs. Personally, I like the idea of controlling my own data. But the truth is that the vast majority of us, me included, do not read the entire “terms of use” agreement on every app or website, and we believe our data is more private or more secure than it actually is.

I believe there are ways to both support the innovation coming from the external marketplace while providing the needed safeguards to govern personal digital health data. The entrance of non-healthcare actors into the healthcare market—particularly those that fall outside of the HIPAA requirements—necessitates strong principles for trust and security. One idea is an industry-backed process to independently vet these applications to ensure they meet all relevant security standards; use data appropriately and in line with consumer expectations; and, for those applications that offer medical advice, are clinically sound.

Government policies must allow digital health information to be exchanged in a way that protects and prioritizes the health interests of individuals—and the health systems and clinicians who care for them—while allowing the marketplace to innovate and interact in a responsible and controlled way.

In this technological age, it is important we all remember that deployment of health information technology, interoperability, data exchange, privacy and security are all in service of delivering the highest quality care. It is not about the technology; it is about the patients, their care and their outcomes.

Thank you for the opportunity to speak to the Committee today. I have additional information on these topics in my written testimony that I hope you will also consider.

The CHAIRMAN. Thank you, Dr. Rehm.
Ms. Greal, welcome.

**STATEMENT OF MARY GREALY, J.D., PRESIDENT,
HEALTHCARE LEADERSHIP COUNCIL, WASHINGTON, DC**

Ms. GREALY. Excuse my laryngitis, please. Chairman Alexander, Ranking Member Murray, and Members of the Senate HELP Committee, thank you for inviting the Healthcare Leadership Council to testify before you today.

HLC is a coalition of Chief Executives from all disciplines within American healthcare. It provides a forum for the Nation's health care leaders to work together toward their vision of a 21st century healthcare system that makes affordable, high-quality care accessible to all Americans. Members of HLC, hospitals, academic health centers, health plans, pharmaceutical companies, medical device manufacturers, laboratories, biotech firms, health product distributors, post-acute care providers, and information technology companies, advocate for measures to increase the quality and efficiency of health care through a patient-centered approach.

The members of HLC are saying that the time is here, the time is now, to achieve full nationwide interoperability of health information and to have secure, seamless access to data for clinicians, patients, and health care consumers. Today, I am pleased to present to you a significant project undertaken by HLC with the Bipartisan Policy Center, two organizations that between us represent many of the major companies that purchase healthcare, pay for healthcare, provide healthcare, and deliver access to the data that drives quality health care.

Despite all the progress we have seen in health care moving into the digital age with more providers utilizing electronic health records and more consumers able to get health information on our smartphones, everyone in this room knows that we still have a long way to go. Today, we do not interact with just one family physician. We as patients interact with primary care doctors, specialists, hospitals, clinical labs, pharmacies, insurers, and more, yet these entities often do not talk to each other electronically. And if we are to reach our goal of a healthcare system that provides high-quality, patient-centered care, interoperability is not simply desirable, it is absolutely necessary.

HLC and the Bipartisan Policy Center set out to determine what needs to be done to achieve nationwide health data interoperability. We engaged the University of California at San Francisco to interview dozens of experts from multiple health care sectors and the Government. What we learned in these interviews led to the recommendations and our call to action that we provided as an attachment in our written testimony. There are a couple of exciting aspects to this project and the proposals that emerged from it that I would like to highlight for the Committee. It is significant that leaders from the private sector across the entire health care continuum have come together and agreed upon mechanisms to accelerate nationwide interoperability. And this is not just a matter of telling Government what it should be doing, but rather these private-sector entities are placing the responsibility among themselves

and upon themselves, pledging action and embracing accountability.

Thus, you see us calling for collaboration between healthcare payers and providers to use payment incentives to drive adoption of baseline interoperability expectations. And a call for providers to work with electronic health record companies and software developers in incorporating these same expectations into their business contracts. We are calling for common standards to be utilized to improve patient matching, and we are calling for the rapid adoption and implementation of open standards-based APIs. These just touch the surface of the recommendations you will see in the report.

We are pleased that the leaders in the public sector stepped forward with the proposed Federal rules we are discussing today on data access and interoperability, and we see a great deal of alignment in these rules with what we are offering in our report. We applaud the efforts of ONC and CMS to eliminate information blocking and ensure the consumers have easy access and ability to share their health information as they wish. These rules represent an important and perhaps ground breaking first step for true nationwide interoperability.

I would note that both proposed rules include changes to how patient health information is used and shared. These rules incorporate new innovative products such as third-party applications that are not currently covered by the HIPAA Privacy Law. We need to ensure a thoughtful approach in how entities currently subject to HIPAA share information with these new entities to ensure the safeguarding of sensitive and valuable personal health information.

Any future legislation or rulemaking that addresses the electronic flow of identifiable health information should engender the same trust as the HIPAA privacy standards have done for the past 20 years. Given the significant impact of these rules, including the strong enforcement, penalties, we are requesting that ONC and CMS grant a 30-day extension of the comment period for the proposed rules.

Thank you for the opportunity to speak to the Committee today, and I look forward to discussing the comments of HLC members and our commitment toward advancing nationwide interoperability.

[The prepared statement of Ms. Grealy follows:]

PREPARED STATEMENT OF MARY GREALY

Chairman Alexander, Ranking Member Murray, and Members of the Senate Health, Education, Labor, and Pensions (HELP) Committee, thank you for the opportunity to testify today.

My name is Mary Grealy, and I am President of the Healthcare Leadership Council (HLC). HLC is a coalition of chief executives representing all disciplines within American healthcare. It is the exclusive forum for the Nation's healthcare leaders to jointly develop policies, plans, and programs to achieve their vision of a 21st century healthcare system that makes affordable high-quality care accessible to all Americans. Members of HLC—hospitals, academic health centers, health plans, pharmaceutical companies, medical device manufacturers, laboratories, biotech firms, health product distributors, post-acute care providers, home care providers, and information technology companies—advocate for measures to increase the quality and efficiency of healthcare through a patient-centered approach. All of these health sectors, and the patients they serve, are affected by and committed to comprehensive access to health data.

The members of HLC are saying that the *time is here*, the *time is now* to achieve *full nationwide interoperability* of health information and to have secure, seamless access to data for clinicians, patients and healthcare consumers.

Today, I'm pleased to present to you the results of a significant project undertaken by HLC with the Bipartisan Policy Center (BPC), two organizations that, between us, represent many of the major companies that purchase healthcare, pay for healthcare, provide healthcare, and deliver access to the data that drives quality healthcare.

For all the progress we've seen in healthcare moving into the digital age—with more providers utilizing electronic health records and more consumers able to get health information on our smartphones—everyone in this room knows we still have a long way to go. Today, we don't just interact with one family doctor. We as patients interact with primary care doctors, specialists, hospitals, clinical labs, pharmacies, insurers, and more. Yet, these entities often don't talk to each other electronically. And if we're to reach our goal of a healthcare system that provides high-value, high-quality, safe, cost-effective, patient-centered care, interoperability is not simply desirable—it's necessary.

HLC and BPC set out to determine what needs to be done to achieve nationwide health data interoperability. We engaged the University of California at San Francisco to interview dozens of experts from multiple healthcare sectors and the government. These interviews gave us an idea of the barriers that stand between the present and our essential future, and how to overcome them, leading to the recommendations we've provided as an attachment to this testimony.

Our goals today and moving forward are clear and unwavering—we intend to bring information seamlessly to the point of care to support care delivery, and we will meet the information needs of patients and consumers to support their health and healthcare. There are a couple of exciting aspects to this project and the proposals that emerged from it that I want to highlight for the Committee.

It's quite significant that leaders from the private sector—across the entire healthcare continuum—have come together not only to say that we must accelerate the movement toward nationwide interoperability, but they have agreed upon mechanisms by which to do it. And this isn't just a matter of telling government what it should be doing, but rather, these private sector entities are placing the responsibility upon themselves—pledging action and embracing accountability.

Thus, you see us calling for collaboration between healthcare payers and providers to use payment incentives to drive adoption of baseline interoperability expectations, and a call for providers to work with electronic health record (EHR) companies and software developers in incorporating those same expectations into their business contracts.

We're calling for common standards to be utilized to improve patient matching, to make certain the right patient is getting the right treatment at the right time, all the time. And we're calling for providers, EHR companies, software developers, payers and other sectors to pursue rapid adoption and implementation of open standards-based APIs. These just touch the surface of the recommendations you will see in the attached report.

But the other aspect of this project that is so encouraging is that we are in alignment with the Federal Government and its goals in this area.

We are pleased that leaders in the public sector stepped forward with proposed Federal rules on data access and interoperability and we see a great deal of agreement in these rules with what we are offering in our report.

We applaud the efforts of the Office of the National Coordinator for Health Information (ONC) and the Centers for Medicare and Medicaid Services (CMS) to eliminate information blocking and ensure that consumers have easy access and the ability to share their health information as they wish. These rules represent an important, and perhaps groundbreaking, step toward true nationwide interoperability.

It should be noted that both proposed rules include changes to how patient health information is used and shared. These rules incorporate new, innovative products, such as third-party applications, that are entering the healthcare market at a rapid pace but are not covered by the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules. We need to ensure a thoughtful approach in how those entities currently covered by HIPAA share information with new entities to ensure the safeguarding of sensitive—and valuable—personal health information. Any future legislation or rulemaking that addresses the electronic flow of identifiable health information should engender the same trust as the HIPAA privacy standards have done for the past 20 years.

Given the significant impact of these proposed rules, including strong enforcement and penalties, we are requesting that ONC and CMS grant, at a minimum, a 30-day extension of the deadline for submitting comments on the proposed rules. An extension would provide more adequate time to conduct a thoughtful analysis of the proposed rules and their impact, and to fully address the multiple requests for comments and information embedded within them.

Thank you for the opportunity to speak to the Committee today. I look forward to discussing the commitment of HLC members toward advancing nationwide interoperability. These commitments are explicitly included in the *HLC BPC Report on Advancing Interoperability, Information Sharing, and Data Access*, which is included as part of my written testimony.

The CHAIRMAN. Thank you, Ms. Grealy, and thanks to each of you. We will now have a round of 5 minute questions.

We will begin with Dr. Cassidy.

Senator CASSIDY. Thank you, Mr. Chairman. I thank you all for being here. Raised several interesting things. Ms. Grealy, I just learned that in my state, the patient does not own her data. Does HLC have a position on whether or not the patient should own her data?

Ms. GREALY. We think it is important that patients do own their data and that they have access to that data. And that really, the providers and those working with that patient health information, really are the stewards of that information.

Senator CASSIDY. Simple answer, yes. Thank you for that. Ms. Savage, you raised a point, I think you did, of the ability for the health plan—again, do I own the data that the health plan has? Or should I own that data?

Ms. SAVAGE. As you mentioned, it is really a matter of state law. So technically within a health plan, you may not own the data, but you certainly have a right to get a copy. That is the state of the law.

Senator CASSIDY. Let me ask, define the data. If the health plan is purchasing data from data brokers, not just about the doctor who saw me for a busted arm, but rather the data from the grocery store as to whether or not I am buying high cholesterol food, should I have the right to that data?

Ms. SAVAGE. You have a right to get any data that the health plan is using to make a medical decision about you.

Senator CASSIDY. Now, define medical decision.

Ms. SAVAGE. Well, it is a little bit ambiguous and so I—

Senator CASSIDY. Oh, that is what I thought.

Ms. SAVAGE. That is right. But I want to definitely distinguish is you do not have a right to get data that is used, for example, to calculate a measure because that is not—

Senator CASSIDY. To calculate a measure—

Ms. SAVAGE. Like a measure. Like a plan, HEDIS measure for how many people referred to a mammogram or something like that.

Senator CASSIDY. Got it.

Ms. SAVAGE. That is not about you. But if they are using that data to decide that you should or should not have a particular treatment or should or should not have a premium increase that is definitely within the data you should be able to get access to.

Senator CASSIDY. Now, you say should, implying that you personally think that we should, but legally do I—legally do I have access to that data?

Ms. SAVAGE. Absolutely, you legally have access to that. The problem is that in caring that out, obviously there is a lot of gaps in how people do that. That issue of individuals getting their own data, I think is a top five complaint at OCR.

Senator CASSIDY. Do we have a need therefore for standardization of how the patient would access her data and what exactly comprises that data so that there is not this variability in response?

Ms. SAVAGE. I think there are some great paths of standardization beginning to take hold. The idea of using an app and a standard API is one, although not all data will be available behind that API in the immediate future. A second is the Association of Health Information Management, AHIMA, is working on a standardized form and they are urging people to adopt it voluntarily so that it can be turned into an online form so people can use it, but it is not enough.

Senator CASSIDY. I think that my colleagues and I would be, and I certainly am interested, if you all have ideas as to how I could know if the health app that I am using does—feeding up to the insurance plan, that I actually have that data as well as that which they purchase from data brokers, which I am told is quite extensive.

Ms. SAVAGE. Right. So that is a couple of different issues, but in my longer testimony I refer to an article that I did with ten or so tips people could just adopt right now that would make it easier for patients and nothing prevents a health insurer from adopting those. I want to separate that for a moment from the broker purchased data because we do not know exactly which health plans are doing that, and second or third from the app you choose to use. All different things.

Senator CASSIDY. I get that. So that is my question for you, Dr. Rehm. So, I recently read of somebody partnering with somebody so that smart watches were on the wrist of the insured. And I thought to myself, now they know how many steps I am taking today and whether or not my gate becomes shuffling and so maybe I have the first onset of Parkinson's disease, right. And should that be protected, the fact that I am basically telling them that I may be at risk for a neurologic disease—by the way I do not have a neurologic disease for the record, that I know of.

[Laughter.]

Dr. REHM. I would characterize that, as soon as that personal health data gets transmitted into the healthcare system that information should be protected so—

Senator CASSIDY. But I do not believe it necessarily currently is, correct?

Dr. REHM. Well, if that, let us say you have an EMR that allows you to add personal health devices to that EMR so that the patient that is wearing that watch or scale, for that instance, feeds my EMR, then that information is entered into the EMR and it is protected, at least in my practice.

Senator CASSIDY. Now you are speaking of the theoretical, but I am pressing on you, do we know that is the case?

Dr. REHM. Only if it answers the EMR. So, I would say we do not know that is the case.

Senator CASSIDY. If it goes to the health plan, and not to the doc, but if it goes to the health plan, is that part of the data that Ms. Savage referred to as being a covered entity—a HIPAA protected set of data or not?

Dr. REHM. I do not know.

Senator CASSIDY. I do not know either. Ms. Savage?

Ms. SAVAGE. Yes, the health plan is a covered entity under HIPAA just like a physician's office.

Senator CASSIDY. But is the app, the information that they are receiving from the app considered part of that covered data?

Ms. SAVAGE. When it flows into the covered entity's custody, it becomes covered by HIPAA. The second thing to remember is, OCR has been very clear, when the app is sponsored by or paid for by the covered entity, the collection by the app is in fact covered by HIPAA. The one place we do not, that OCR does not reach, is to an app that is not paid for or sponsored by a covered entity itself.

Senator CASSIDY. Got it. So, if I just voluntarily give. I am going over. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Cassidy.

Senator MURRAY.

Senator MURRAY. Thank you very much. And Ms. Savage, you talked about the importance balance between protecting patient privacy and making sure patients have access to their data. I think that is what the Senator was going after. Let me ask a little differently. Do patients who share their health care information with third-party apps have their information protected under the patient privacy laws of HIPAA?

Ms. SAVAGE. It is going to go back to who is sponsoring that app. So, in the Omada context, our app is sponsored by us. We are a healthcare provider under HIPAA. All the HIPAA rules apply within the app, however, we do not stop people from taking whatever they want about the health information, just like Senator Cassidy did, and blurting it out in whatever context they want. And so, unless the context in which that blurt is received is also covered by HIPAA, it would not be covered.

That might be a third party app that is not covered, that is covered only by the Federal Trade Commission or State Attorneys General, as opposed to being within kind of the confines of a HIPAA-covered entity and its sponsorship.

Senator MURRAY. Well, what should patients know? What should we all know about how our data can be shared if we use an app that is not covered by HIPAA privacy protections? Can their data be sold or just goes to drug companies or advertisers?

Ms. SAVAGE. Yes. It is a very confusing place for consumers when in 2016 we sent a report up to Congress on this very thing. It is footnoted in ONC's rule, and consumers just—it is too much information for them to understand and it is very confusing for them. I think that they have the ability to rely pretty well on what their doctors do and how the healthcare system works, and those rules are very familiar, but people definitely feel that—think those rules apply when they do not.

Senator MURRAY. Can your data be sold?

Ms. SAVAGE. Outside of HIPAA, yes. Within HIPAA, it cannot be sold in an identifiable way. There is a very specific rule on that.

Senator MURRAY. Like to drug companies? It could be sold to drug companies?

Ms. SAVAGE. Well, if you were, if it was a third party app, without naming names, and any kind of social media app, of course.

Senator MURRAY. Okay. Well, so there is a lot of potential for digital records, but it also comes with risks. I think that is pretty clear.

Ms. SAVAGE. Correct.

Senator MURRAY. Tell us what policy recommendations would you make to better protect patient privacy.

Ms. SAVAGE. It is a very complicated area that I know many Senators and many of your colleagues and also House Members are working on, and what I think is to look at the totality of the fact that the digital life is no longer sliced up into economic sectors and we really need policies to converge.

Whether that is things that look like HIPAA migrating outwards or some uniform policy that everyone can, as a consumer, easily understand, that would be my policy recommendation. And that is not an easy thing to do given our Federalized system but that is where I think the direction needs to go, is how to converge it so that it is the same and the expectations are the same for consumers wherever they go.

Senator MURRAY. Consumers understand it better because it is uniform?

Ms. SAVAGE. Yes.

Senator MURRAY. Okay. Mr. Moscovitch, open APIs are really an essential programming feature that allow programs to share information with each other, and the requirement that electronic health records make them available was a very high priority for this Committee. As you said in your testimony, APIs are the foundation of the modern internet. So, to ensure that the APIs are truly open, the Office of the National Coordinator for Health Information Technology proposes electronic health records developers publish business and technical documentation associated with their APIs. Talk to us about why that requirement is so important.

Mr. MOSCOVITCH. The documentation is much like an instruction manual for how third-party developers can request information and how it is formatted so they can use it. In other industries, that documentation is publicly available to spur innovation. If a technology has an API, for developers to use it they need that instruction manual or that documentation or else they do not know how to request the documentations, whether it is behind a paywall or some other proprietary manner or made public on a website and it still needs to be developed.

Senator MURRAY. Is that going to impose a burden on electronic health-record developers in your opinion?

Mr. MOSCOVITCH. One thing ONC did in the regulations is leverage existing work that is already done through different standards bodies, and which many EHR developers are already implementing. That is through the work, the standards and FHIR work that ONC is doing. So, the industry is already moving in this direction and are already developing documentation based off of FHIR standards.

Senator MURRAY. Okay. And quickly, Ms. Savage and I can go back to you. We want to make sure the Department of Health and Human Services takes the time to implement Cures right away, but if health organizations are hoarding data in order to gain a competitive advantage for themselves, there are real consequences if the Department takes too long to implement these policies. So, what do you think the risks are of delaying the prohibition on information blocking?

Ms. SAVAGE. Well, I cannot do an economic estimation. You have to go to my co-author, Martin Gaynor, on that, but I think that we know that there is lots of savings that have been documented for the little teeny bits of interoperability we have right now and avoided redundant costs. And that will only grow. And then there is the whole consumer frustration piece. In every part of their lives they are quickly and efficiently using the supercomputers in their pocket except in this.

I cannot even estimate the increase in productivity if we all don't have to spend hours and hours and hours chasing down our records and moving them around in the system for ourselves.

Senator MURRAY. Okay. Thank you. Thank you very much, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Murray. And Ms. Savage, your last comment was important to me. This all—listing this testimony sounds very complex, difficult, obtuse, all those things, but we are really talking about a very common everyday experience for most Americans. I mean, as we think about our health care records, we think on the one hand, well, I can make an airline reservation just like that. Two, I can order something over Amazon just like that, and if I want to take my health care records from Vanderbilt to the Mayo Clinic, the best thing for me to do is to go down to the bottom floor of the hospital with a wheelbarrow and put them all in there, and then pack them in a suitcase, and then fly to Minneapolis, and then drive to Rochester, and hand them to the doctor. So that is—even though each of those two institutions do not use those because they are leading the country really in terms of interoperability within their systems.

We are well-meaning here. But I can still remember going to Vanderbilt to find out about electronic health care records and they said, Meaningful Use 1 was helpful, Meaningful Use 2 was Okay, Meaningful Use 3 was terrifying because as we project our good intentions out to the real world of hundreds of thousands of doctors, and thousands of hospitals, and millions of patients, sometimes it does not work like we hope it would. So that is how we got to standards that we are talking about today and how we got to these rules about information blockage.

My question is about the standards. I had this great fear, as we were doing the 21st Century Cures bill, that if we required standards that somebody would write them in Washington and that they would be the wrong standards and they would not imply properly to everybody. We would just create more of an administrative burden and big mess than existed.

If I am remembering it right, what we just said was you have to have standards. We are not going to write them for you. And now the rules are saying but you are going to have to use these

standards written in the private sector so everybody can work together and talk with each other.

My question is, Dr. Rehm, let me ask you, are these the right standards? Are we correct to insist that there be the same standard for everybody, and are we going too fast in asking doctors and hospitals to implement these rules?

Dr. REHM. I will start with the first one. I think we are headed in the right direction with being very prescriptive in the standard, because when the standard is broad and you leave it up to the industry to implement, they will take advantage of the breath of what is allowed in the standard, which then leaves the provider organization trying to do all the manual work in between because it is not interoperable.

I do think being as prescriptive and precise in the standard and requiring people to develop to that standard will accelerate interoperability. And the second part of your question as it relates to going too fast, I think you just have to keep in mind that the provider side is always months behind when the technology is developed to cover us—

The CHAIRMAN. What I am meaning by that is on Meaningful Use 3, it was my strong feeling that if we could kind of slow the train down a year or two, that we would get where everybody wanted to go more effectively than if we insisted on pushing it. Well there were two different views on that and maybe it was the train was going too fast to slow down, but I want to make sure that these new rules are implemented at a pace that gets us where we want to go but does not do it so rapidly that it makes it more difficult to get where we want to go.

Dr. REHM. Right now there is 24 months for the technology organizations to come alongside the final rule and implement whatever is in the final rule. I think that you got to add time to the end of that for the provider organizations to be able to react to whatever it is they release, because we will have to understand and work with whatever technology is released at the end of those 24 months, and the provider side will need time.

The CHAIRMAN. Ms. Grealy, I have a little less than a minute. What about the standard, should we require standards? Are these the right standards, and is the time that the administration is allocating for implementing the standards appropriate?

Ms. GREALY. I think there is a need for standards. I think your concern, and it is a concern that we share, is making sure that we are still allowing for innovation within those standards. We do not want to stifle the innovation and improvement, electronic records and the exchange of information. I think we will hear from everyone that they probably will want a bit more time. We are at the outset asking for a longer time to analyze and comment on these rules—

The CHAIRMAN. Well, before you stop, does the proposal allow for innovation? I mean I have always imagined that these problems would be solved not by anyone here writing them, but by somebody showing up with a, Delta Airlines reservation system and then everybody is, oh, that is the way to do it, and they use it. Or maybe it was American, I do not remember who it was but that is the way it happened.

Ms. GREALLY. But I think standards like open APIs—I think there is just broad, deep agreement that is the way we should go, and the FHIR standard. So, there is a need for standards. I do not think we view these as stifling innovation at this point. We never want to be micromanaged, again, because that would stifle the innovation, but I think you are hearing—everyone is committed to interoperability and we do need some rules of the road that we can all understand and implement.

The CHAIRMAN. Thank you.

Senator Baldwin.

Senator BALDWIN. Thank you, Mr. Chairman. Thank you to our witnesses. I hail from Wisconsin and we have a long history of playing a major role in technological transformation. My colleagues, many have heard about successful health IT innovations from Gundersen Health System and La Crosse from Marshfield Clinic, and of course Epic Systems in Verona, Wisconsin, which exchanges nearly 4 million records a day.

However, our system has not yet achieved the ultimate goal of being fully interoperable, which is why I was proud to play a role on this Committee in crafting the 21st Century Cures Act. The proposed rules released by the administration to advance implementation of the 21st Century Cures Act are critical steps to achieving interoperability and improving patient access to health data. Several provisions would allow patients to become more engaged with their own care by requiring electronic health-record systems to make patient data available to be exported and available through third-party apps, as we have been discussing.

We need to do more to empower patients, however I am concerned that the proposal may expose new vulnerabilities for patient confidentiality. Dr. Rehm, these proposals to expand patient data sharing through third-party applications potentially lead to breaches in patient privacy and security, and how can we best balance patient access while preserving the confidentiality of the physician-patient relationship in our fast, developing digital era?

Dr. REHM. Right. So, as I put in the written testimony and in the oral testimony, I do think that there is risk with third-party applications that do not necessarily—HIPAA does not apply to them all, potentially, in this scenario of what the open API—a third party app can be developed, can be directed toward consumers and there is nobody vetting or currently there is no organization that would be vetting just the technology infrastructure security of that application.

At LifePoint, we have a technology review board that looks at applications that some of our member hospitals want to bring into the fold, and it is frequent that when we do a deep dive into that technology, we find a cybersecurity risk and so we do not bring that technology into our technology stack.

We need to do something to protect the patients because if they are drawn to a consumer-driven app, they use it, they use the open API to pull their health information into that application, who is it that is making sure that company is putting the proper safeguards to keep that data secure? So, I think it is a risk.

Senator BALDWIN. Thank you. Mr. Moscovitch, you noted that the proposal requires electronic health record systems to ensure

that all of their patient data and electronic health information can be exported to patients, which could include other information from vendors' data bases.

I have certainly heard concerns from my constituents about the lack of clarity and standards in the rule concerning what constitutes this electronic health information. In fact, there is currently no standard for this broader group of data. Can you elaborate on this gap in existing standards and how requiring extraction of large, potentially undefined data sets may create obstacles for a vendor compliance or other risks to patient privacy.

Mr. MOSCOVITCH. Sure. The goal of that electronic health information provision is so that if patients want their data that, including it is outside of the core data elements that ONC wants exchange for APIs, that patients can get it. And that is correct for many of these data elements, that standards do not exist. And so, as ONC finalizes its regulations, it should absolutely clarify which data element, or which information more broadly, needs to be available to patients, and where possible, to do that in an easy way for patients.

Senator BALDWIN. Great. Thanks. I yield back.

The CHAIRMAN. Thank you, Senator Baldwin.

Senator Braun.

Senator BRAUN. Thank you, Mr. Chairman. For me it is surprising that we have to be talking about interoperability and information blocking, and I think it is part and parcel of what is wrong with the healthcare industry in general. I know in my own business, which is a logistics and distribution business, we due to competitive pressures and transparency, embraced the latest, the leading edge. And here, that we are having to nudge the healthcare industry itself to get with it on these topics, it is to me, it is what is wrong with the healthcare industry in general, which is a lack of transparency.

The industry knowing all this stuff, has been out there for a long time, and when it comes to, drug pricing, when it comes to embracing transparency to engender competition that drives most other industries, I think that is why we are talking about it. And every time I get the opportunity, I want to challenge the industry to get with it. To do what almost all other industries have done, and when you have got a leading edge of anything, you grab it, because if you do not, you are left in the dust by your competition. The cloaking and shrouding of the healthcare industry, mostly due to the industry itself embracing that rather than transparency and technology, leads us to this discussion.

I, again, challenge the industry to get with it or else you are going to have one business partner, the Federal Government. Let us go back to interoperability and information blocking. Which of the two, and any of the panelists can weigh in on it, is more important leading us to this point to where we are dysfunctional when it comes to information sharing, and where should we spend the resources, if we can in some way through Government, help speed the process? I would like to know the relative importance of these two issues. So, you can start.

Mr. MOSCOVITCH. The Congress had a lot of foresight in the 21st Century Cures Act in leveraging APIs, which as you mentioned,

many other industries are already taking advantage of these kinds of technological tools. And ONC has implemented that provision also with a lot of foresight in leveraging these standards that are already adopted throughout the industry and being refined through various collaborative groups like the Argonaut Project, which brings technology organizations together to identify a refined way to implement the standard.

Senator BRAUN. You sense that if we were not here today talking about it, the industry would be pushing forward on its own? And you can either answer that or not. I would love your opinion.

Mr. MOSCOVITCH. Congress certainly have accelerated the adoption of APIs in a meaningful way.

Senator BRAUN. Thank you.

Ms. SAVAGE. I would like to say that is true. I think the nudges both from high-tech and from Cures have been crucial. And all you have to do is go on the right Twitter feed and you will see the hashtag #axethefax because everyone is still using faxes in healthcare. So, we need to move beyond that just like the rest of industry has.

Dr. REHM. I would just double down on that. I think the focus on forcing the industry, when I say industry the technology side for the interoperability piece because data blocking—some of it is just you cannot accomplish it or sometimes it is so costly or outside your normal workflow that you do not accomplish it, but if the technology was more plug-and-play from an interoperability perspective, you would see data flow more freely because the providers, they want access to information to care for the patient. Right place, right time, right now. And so, the providers are pushing from their side, but the struggle is in the middle where time, money, and effort to overcome the interoperability challenges.

Ms. GREALY. I would just underscore how welcomed these proposed rules are. It is not often that you see, I think, such great alignment between what the Government is offering here and what the private sector has been asking for and wants to work with them. But I think an area that you touched on is one that we really need to do more work on, and that is how do we create better consumer, or more consumer demand for this?

We need to engage patients and consumers as to what should be available to them, how it is going to improve their health, and the efficiency of the healthcare system. So, I think we would welcome a public-private partnership type of campaign to really educate people on how best to use this information, and that they should have access to it. Just like when you change cell phone carriers, you do not have to get a new cell phone number anymore, you get to transfer that number. We should have that same ease of operation with electronic health information.

Senator BRAUN. For consumers to be part of the process, which is what we did in my own company, to make it consumer-driven, you have got to have transparency. And all I am saying, in the entire industry, across the board, start working on this stuff, doing it on your own where you do not need to be nudged by hearings like this because I think you will regret the outcome down the road if you do not start embracing what all the rest of us do, transparency and competition. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Braun.

Senator ROSEN.

Senator ROSEN. Thank you. I would like to thank you, Mr. Chairman. Thank you for your testimony today. You know, I am a former applications programmer so a lot of this interface stuff is near and dear to my heart, but recent study by the Kaiser Family Foundation show that 88 percent of patients say their medical provider does use electronic medical records. That is up almost 50 percent from 10 years ago, but the biggest concern everybody has is privacy, of course. And so being a former applications programmer, systems analyst, this is something that I focus on a lot.

What I want to ask you, Ms. Savage, is this, who in your view is ultimately responsible for the integrity of an individual's medical record? Is it the doctor, provider, electronic health vendor, the hospital? I mean, who? All of them? I mean, where does accountability ultimately lie?

Ms. SAVAGE. In our system, we have pieces of our record in the hands of various entities. When they are covered entities under HIPAA, each entity is responsible for what is in its custody. At Omada, we have we are responsible for what we have custody for. If we are sharing that data at a patient's request with their physician's office, the transom is a great visual. It crosses the transom, the physician takes responsibility for it. And that is how the current rules work.

Similarly, outside of that sort of the system the individual is responsible, just like an individual is responsible for what they do about their own banking, or how they describe their children on social media, or any of those things.

Senator ROSEN. Now, if we consider medical devices, perhaps plug and play, I do not want to make the pun about your pacemaker perhaps, but we know that medical device does upload to your medical health record. And so, depending on what you have, now we have this open platform with many kinds of medical devices, many kinds of things feeding in, that can give us a gateway, a doorway, into the system for cyberattacks, for hacking, things that may ultimately change or modify your record. So, how are we preventing that doorway in? What are we doing about that? Anyone can take that question.

Ms. SAVAGE. I will take a first stab at it. So, FDA is very hard at work, certainly in helping device manufactures understand how they can upgrade the security of their equipment without having to do additional filings or changing the safety and functionality of that equipment. But the FDA actually does not enforce security standards, except on those devices, and the legal authority sits with OCR, who is enforcing it at the doctor's office or hospital office level.

Back to what Senator Murray was asking about, as we think about convergence and digital life, I think the policy question for all the Senators is, how do we bring these things together and kind of thread stuff together that previously was happily living in distinct silos. That is not the case anymore. We do not want silos for individual data, and we do not want silos for security authority—

Senator ROSEN. What if something is wrong and you realize that. How does a patient—how does “us” as a consumer get a correction through all of this?

Ms. SAVAGE. For their data?

Senator ROSEN. Yes.

Ms. SAVAGE. We all have the right to ask a physician’s office or a hospital, any record holder, to correct data, and then hopefully the right physician will say, oh, yes that correction needs to be made. I just corrected my own data recently with my physician. But it is a little bit of a kludgy process, and it could be automated. For example, if you could ask for a correction through logging into your secure portal, then your identity would be proven and it would all be electronic, and the physician could just make the change. I do not know if Dr. Rehm wants to add anything to that.

Dr. REHM. I was just going to add and kind of restate something I said earlier, which is with the open API, we are potentially opening up the electronic health data to a segment of technology that currently is not covered by HIPAA, which has been very prescriptive as to how we have to handle health information as a provider organization, or any organization covered by HIPAA. So, I think that is the thing to just—what are we going to do legislatively to make sure that when we put in the door for people to pull in their information out of the electronic health record into some other application, how is that application governed?

Senator ROSEN. Then, I have a quick question for you at the end. The huge responsibility put on the end care provider on a small family practice and on the individual at the end of the system. What is the burden for you to hire more people to take care of all this data and information?

Dr. REHM. The provider burden today, because it is not interoperable, is huge. Because we at LifePoint, we are fortunate enough with our size and scale so that we can throw an army of people at the bridging the gaps between—

Senator ROSEN. But if you are a small practice?

Dr. REHM. But if you are a small practice, you do not have those folks. And so that puts you at risk for one. Are you data blocking because you do not have the resources to do the custom interfaces to allow this ADT message to flow from here to here. I mean, you might be caught in the middle of, yes, that is data blocking, and that is because you do not have the expertise or the resources. So, I think we have run out—there is a great risk in the current technology environment for practices that do not have the resources because the systems are not interoperable today. It takes effort and expertise, and not everybody has that.

Senator ROSEN. Thank you.

The CHAIRMAN. Thank you, Senator Rosen. Well, thanks to all. I have—Senator Rosen brought up devices. These rules are not about devices, I guess. They are about data, but there is an outfit in Nashville called a Center for Interoperability that is a combination of hospitals, nonprofit and profit, all around, who realized they have a lot of buying power and they are trying to create a common platform so that anyone from whom they buy things has to plug into a common platform. They use an analogy of why we do not worry much about cable television, that way back in the early days

they got a common platform, so all the different cable companies use a common platform. What does what you are talking about today about devices, I mean about data and interoperability, have to do with devices and the data that comes from devices?

Ms. SAVAGE. I will take a stab at that. So, in my longer comments we gave an example of a person who has a surgery, and they get a brace, and the brace has a radio chip and a gyroscope, and it attaches to their app, and that feeds to the brace manufacturer's servers. And it may or may not feed to a physician's practice. It depends on what the patient chooses.

When it is not going to the EHR, all of that activity is both not within HIPAA, and we have talked about that quite extensively, but it is also health information technology with important information gate and success of the surgery, that is not subject to this rule. And so that is really something to think about back to this idea of convergence.

Mr. MOSCOVITCH. The CMS rules also focus on getting patients their claims' data. And claims today for the millions of patients with implants lack key information. That is the device identifier of the implant they have in their body. So, when they are getting their claim's data, they will not know which brand of device or which model of the device they have in case something goes wrong. And CMS can close that gap by adding device identifiers to claims.

Dr. REHM. We have talked a lot about interoperability and usability, and I think those two are inextricably linked. And the usability is made better if medical devices—when you think about what is in the EHR, it is a store of data. And a lot of it is manually entered today by whether nurses, medical assistants, or physicians.

Devices are just one example where they are not covered but the interoperability between the device and the EHR is just as key as the interoperability from one EHR to another because that burden of getting the data from whether it's from a blood pressure cuff, a ventilator machine, whatever it might be, getting that into the system is today either manually entered or a custom interface to pull that in.

The CHAIRMAN. Ms. Grealy, anything to add?

I think Senator Romney is on his way back, but as he comes, let me ask each of you. If you were in my shoes or Senator Braun's shoes, what would be the one thing that you would like for us to do or you think we can most constructively do to encourage interoperability of data as we consider these two rules over the next year or so? What is the one thing you would like for us to keep our eye on or push?

Mr. Moscovitch?

Mr. MOSCOVITCH. Sure. One thing we have not talked a lot about today is patient matching. So, the ability to know that the patient at one health system is the same person at another health system. And match rates can fail today around half the time. Our research has found that better standards for demographic data can meaningfully improve match rates. So that is a next step that ONC can be taking as it finalizes its rules.

The CHAIRMAN. Ms. Savage?

Ms. SAVAGE. Well, I think the Committee is rightfully concerned about privacy and security, and you as Committee Members have

a lot of expertise about how this works in the healthcare system. And I think the best thing you can do is work with your colleagues on what is working in healthcare that would need to be migrated elsewhere because none of this will matter if the consumers do not have confidence, and their doctors do not have confidence that the consumers have confidence.

The CHAIRMAN. Dr. Rehm?

Dr. REHM. I mean she did not say and I think the standards FHIR, Argonaut, the USCDI, and the real-world testing. So as folks adopt those standards, the validation through the real-world testing that is working across vendors.

The CHAIRMAN. Ms. Grealy?

Ms. GREALY. I would endorse all of the comments you have just heard. And then the other thing I would really ask that you sort of maintain oversight on the implementation of this and the time really necessary to do it the right way. And I think you have pointed out that perhaps there may be more time required. We do not want to halt this. We do not want to prevent moving ahead or progress, but I think we also have to be very cognizant of the challenges that providers and others are facing in trying to this complex work.

The CHAIRMAN. You have asked for 30 more days?

Ms. GREALY. At least for the comment period.

The CHAIRMAN. For the comment period for the rules.

Ms. GREALY. Yes.

The CHAIRMAN. We will let Senator Romney provide the benediction.

[Laughter.]

Senator ROMNEY. I think I will ask questions instead, Mr. Chairman.

[Laughter.]

Senator ROMNEY. Thank you. I appreciate the work that is being done to provide standardization and I happen to believe that this is a scenario we have lagged in and there is a real cost financially but more importantly in terms of the quality of care delivered to patients by virtue of not having been able to have this information. I am pleased, as I consider the providers of health care in my state, to recognize that they have interoperability within their own systems. At LifePoint, of course, within your system. Intermountain Healthcare within their system. And from what I can tell from the outside, the interoperability within the specific systems is having a very significant impact, particularly on the cost and quality overall in the enterprise.

I guess I have two questions that I am happy to direct this to anyone who wants to pick up on it. One is, does this information inform also the choice that the doctors choose to guide the type of treatment they might provide or the prescription they might provide? So, are they using the information to actually change their practice in providing care to the patient? That is No. 1. And then No. 2, is the data being used yet, the electronic medical record data, being used to allow the patient to inform their life choices?

If a record indicates that someone looks like they are at risk for developing diabetes, for instance. Is this flagged by someone? Is someone seeing that? Is it then flagged to the individual? Are they

given then instructions on what type of foods they should be eating and what types of things they should be avoiding? So, to what extent are we using medical, the advent of electronic records, not just to improve the cost of the healthcare system, whether it is at LifePoint or the Intermountain, or Mayo, or any of the others, but also to actually make decisions by physicians, and No. 2, allow patients to make—individuals to make decisions for their own health and well-being?

Ms. SAVAGE. With the diabetes prevention product, I will take the first step. Intermountain is actually one of our oldest customers. We started offering DPP to Intermountain employees and now it has been expanded out to their patients in certain populations. In fact, we used their EHR data to decide who to refer to Omada, and then we in turn engaged the person that is in an asynchronous platform. You can open your smartphone and see your weight record and your food intake at any point in time. There is a picture in our supplemental materials, and so I would say, in fact when you can figure out the business relationships and the data relationships, that magic alchemy occurs. And what we want to have happen is have it occur more widely throughout the whole healthcare system.

Mr. MOSCOVITCH. What Cures did and what these rules do is make sure that first and foremost patients can get their data and providers can get the data from other places. And better APIs to make sure the data are exchanged, and better patient matching can meet that end.

Senator ROMNEY. Thank you.

Dr. REHM. From the provider perspective, when the information is visible and present in many of our systems, even if it is interoperable, that information that is brought in from the outside, is outside of their workflow. So, when the patient is in front of you and you are trying to make clinical decisions, you have everything that is native to your EMR, and the outside information is frequently in a separate workflow that you have to go find and get.

Sometimes, in some of our EMRs, that information is closer to your workflow, so it is leveraged. The more difficult it is to leverage that outside information, the less likely our providers are to see it at the right time to make a care decision at that moment. So, the usability and interoperability again are, I think, go hand-in-hand.

Senator ROMNEY. Can we make progress on that front? Are we—

Dr. REHM. Yes. Sorry, I did not mean to cut you off there. Yes, so I believe some of the—what we are talking about today and what the rules are proposing bring us closer to narrowing the playing field so that interoperability is more useful because it becomes more usable by the clinicians who are in front of the computer and the patient at the same time.

Senator ROMNEY. Yes. Thank you.

Ms. GREALY. Well, I just want to highlight with a personal story. When you see this work and work well, it is amazing. Two years ago, my husband had a very unusual stroke which affected his vision. So, there was an ER visit, an overnight hospital stay, and then the next 2 days he had to see an ophthalmologist, cardiologist, neurologist, and then back to the primary care physician. All of the

recommendations for most different physicians came back to the primary care physician.

The most notable one being the cardiologist saying, I know this will sound unusual to you and your husband because his cholesterol level is extremely low, but the latest research shows that for this type of stroke, him going on a statin would be a good thing. I am not going to prescribe it now. I am making the recommendation but discuss it with your primary care physician. So, we go back to the primary care physician. He has been treating my husband for many years. He looks at it, goes, well this does not make sense, but that cardiologist had included the latest research. He took the time to look through that and said, she is correct.

Next day I did have an opportunity to attend an AMA function and talk to other cardiologists, and ophthalmologists, and primary care physicians. And again, it was cutting edge research. To me that is the real value of having an interoperable electronic health record where the physicians have the information and you as the patient are able to engage in that discussion in how to manage your health. So, this is what we need to have nationwide, not just within these closed healthcare systems.

Senator ROMNEY. Thank you. Mr. Chairman, in keeping with your introduction, amen.

[Laughter.]

The CHAIRMAN. I agree with Senator Romney. That helped take what can sometimes sound complex and confusing and gave it the kind of meaning that we hope to give it. Thanks to each of you. You have been very helpful today. As I said earlier, this is a—we all believe the 21st Century Cures Act was, as the Majority Leader said, the most important bill we passed in that Congress, and we are determined that it be implemented correctly. It sounds like these two rules are important steps toward interoperability.

If you have other comments that you would like to make to the Committee after you leave and think, oh, I wish I had said this or I wish I had said that, the record will remain open for 10 days so you may do that. Members may submit additional information too.

The CHAIRMAN. The HELP Committee will meet again on Tuesday, April 2d for a hearing on higher education.

Thank you for being here. The Committee will stand adjourned.

ADDITIONAL MATERIAL

DIGITAL HEALTH DATA AND INFORMATION
SHARING: A NEW FRONTIER FOR HEALTH
CARE COMPETITION?

LUCIA SAVAGE
MARTIN GAYNOR
JULIA ADLER-MILSTEIN*

It has long been the case that information can confer competitive advantage. This has come to be increasingly important, and perhaps central, in many industries as digital interfaces and data storage and processing capacities have grown dramatically. In all sectors of the economy, companies are applying data science to their digital assets to gain insights into the people and behaviors represented in the data. While in many ways health care has lagged in the adoption and effective utilization of information technology,¹ the ability to access and analyze data has become increasingly important in health care, as it has in other sectors of the economy.

Analyzing health data can yield important insights for health care organizations. For example, through data they possess,² health care businesses can learn more about the people they are caring for, the practice patterns of their

* Lucia Savage is Chief Privacy and Regulatory Officer at Omada Health, Inc. and is former Chief Privacy Officer at the Office for the National Coordinator for Health IT in the Department of Health and Human Services. Martin Gaynor is the E.J. Barone University Professor of Economics and Health Policy at the Heinz College of Information Systems and Public Policy at Carnegie Mellon University and is former Director of the Bureau of Economics at the Federal Trade Commission. Julia Adler-Milstein is Associate Professor of Medicine and the Director of the Clinical Informatics and Improvement Research Center at the University of California, San Francisco. We thank Nathan Wilson and William Adkinson for helpful comments that substantially improved the article. Responsibility for all views and any errors or omissions are ours alone.

¹ Nikhil Sahni, Robert S. Huckman, Anuraag Chigurupati & David M. Cutler, *The IT Transformation Health Care Needs*, HARV. BUS. REV., Nov.-Dec. 2017, at 128.

² We refer to digital health data via custody rather than ownership because whether anyone besides an individual owns data about them is beyond the scope of this paper. We focus on digital data within the traditional health care system in this paper (also known as digital Protected Health Information under HIPAA). Health data collected in other settings, such as retail or direct-to-consumer services, is outside our scope.

doctors, and the capacity utilization of their facilities. This rich information can be used to assess and improve performance. It has the potential to improve the quality of care and lower costs, benefiting both patients, health care organizations, and the health care system overall. It can be used by individuals to create their own longitudinal health record and monitor their health.³ In fact, the promise of digital data exchange to improve health underlay Congress' enactment of the Health Information Technology for Clinical Health (HITECH) Act in 2009 as part of the American Recovery and Reinvestment Act,⁴ and most recently, the health information technology (IT) provisions of the 21st Century Cures Act in 2016⁵ (Cures). Both of these federal laws actively promoted a higher rate of exchange⁶ of identifiable health information for all the above reasons.

Yet, even with widespread digitization of health information and a \$36 billion-dollar taxpayer investment to make that happen,⁷ that information seems to be flowing at a sluggish pace, and the exchange of digital health information among competitors is the exception, not the norm.⁸ This is distinct from some other industries where sharing data is more common and firms compete on the basis of using that data to create value.⁹

³ Ellen M. Harper, *The Economic Value of Health Care Data*, 37 NURSING ADMIN. Q. 105 (2013).

⁴ American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 et seq. (codified in scattered sections of U.S.C.) [hereinafter ARRA], Title IV, Health Information Technology for Clinical Health Act, [hereinafter HITECH], 123 Stat. 226-79 (2009) (codified in scattered sections of 42 U.S.C.). Certain provisions of ARRA appropriated one-time dollars to stimulate the use of health information technology. Within ARRA, the HITECH §§ 13000-13424, *inter alia*, established the Office of the National Coordinator for Health IT as a full-fledged agency, authorized regulations that specify the technical specifications of certified EHRs, and amended portions of the Health Insurance Portability and Accountability Act and the Privacy, Security and Breach Notification regulations of HIPAA. Health Insurance Portability & Accountability Act, Pub. L. No. 104-191 (1996), 100 Stat. 2548 (codified as amended in scattered sections of U.S.C.) [hereinafter HIPAA].

⁵ 21st Century Cures Act, HR 34, Pub. L. No. 114-255, 130 Stat. 1033 (2016) (codified in scattered sections of U.S.C.) [hereinafter Cures].

⁶ As used in this article, "exchange" will have two meanings, understood from the context. It means (1) a provider sharing of identifiable health data with another provider for a common patient and (2) the ease with which EHRs enable that sharing.

⁷ HITECH & ARRA, *supra* note 4, Title V (money for incentive payments to physicians and hospitals who "meaningfully used" certified electronic health records).

⁸ The Federal Trade Commission explored competition and information exchange in a 2014 workshop. See *generally* Fed. Trade Comm'n, Examining Health Care Competition (Mar. 20-21, 2014), www.ftc.gov/news-events/events-calendar/2014/03/examining-health-care-competition.

⁹ Extensive information exchange between rivals occurs in some other industries (but not all). Financial institutions fiercely compete for customer business and regularly exchange information from their customers' accounts. Cellular phone customers can change carriers and equipment without the carrier refusing to exchange or transfer the data (although a federal law was required to make this easier for the consumer). In on-line search, customers can easily transfer their bookmarks, settings, and search histories across browsers, although search engines retain proprietary custody of the search histories they collect. Online shopping sites typically retain their custom-

In this article, we argue that the sluggish pace of information exchange results from firms' incentives and abilities to maintain or enhance their competitive advantage. Health care organizations and their software vendors control the data collected or generated in the course of patients' encounters with them. These organizations decide if, when, and how they will share that information with others, including other health care organizations, other software vendors, and, in some cases, even the patients themselves.¹⁰

Not surprisingly, if retaining data is profitable while sharing it is not, there will not be a large amount of data sharing. In particular, if firms perceive that control of these data confer competitive advantage, they will be reluctant to share the data with rivals, even if sharing the data likely enables better care to be delivered to patients. Holding on to data may allow market participants to maintain, and in some cases enhance, their market position.¹¹ We believe this "data blocking" is already a barrier to choice and competition and can make it difficult for new innovative organizations to successfully enter health care markets and compete. Furthermore, we anticipate that these issues will become even more pressing as data become an ever more important asset in health care, as it is in the rest of the economy.

The Executive and Legislative branches have recognized the apparent lack of data sharing by health care organizations may be attributable to data blocking (also called "information blocking"). In 2014, Congress requested that the U.S. Department of Health and Human Services Office of the National Coordinator for Health IT (ONC) publish a report on information blocking.¹² Information blocking occurs when an entity that controls health data—such as a

ers' data and do not share. Control of data and what that means for competition has become a major issue in high-tech industries. *See, e.g.*, OECD, BIG DATA: BRINGING COMPETITION POLICY TO THE DIGITAL ERA (Oct. 27, 2016), [one.oecd.org/document/DAF/COMP\(2016\)14/en/pdf](http://one.oecd.org/document/DAF/COMP(2016)14/en/pdf) (background note by the Secretariat).

¹⁰ While HIPAA, *supra* note 4, requires that providers give patients their Protected Health Information (PHI) when it is requested, patient complaints about inability to get their own data remains the number one type of complaint to OCR. U.S. DEP'T OF HEALTH & HUMAN SERVS., OFFICE FOR CIVIL RIGHTS, *Top Five Issues Investigated* (Jan. 31, 2018), www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/top-five-issues-investigated-cases-closed-corrective-action-calendar-year/index.html.

¹¹ Joy Grossman, Kathryn Kushner & Elizabeth November, *Creating Sustainable Local Health Information Exchanges: Can Barriers to Stakeholder Participation Be Overcome?* RESEARCH BRIEF, CENTER FOR STUDYING HEALTH SYSTEM CHANGE (2008), www.hschange.org/CONTENT/970/970.pdf. This study conducted interviews with health care stakeholders in four communities regarding the sharing of health data and found that hospitals "viewed clinical data as a key strategic asset, tying physicians and patients to their organization." *Id.* at 5.

¹² Consolidated and Further Continuing Appropriations Act 2015, Pub. L. No. 113-235, 128 Stat. 2138 (codified in scattered sections of U.S.C.). *See also* 160 CONG. REC. H9047, H9839 (daily ed. Dec. 11, 2014) (explanatory statement submitted by Rep. Rogers, Chairman of the House Committee on Appropriations, regarding the Consolidated and Further Continuing Appropriations Act, 2015) (2015 Budget Act).

health care organization or an electronic health record (EHR)¹³ software vendor—refuses to share the data or engages in practices that impede efficient access and use of the data by competitors or other individuals or entities.

In April 2015, ONC published the report requested by Congress on the nature and extent of information blocking.¹⁴ In late 2016, Congress passed the 21st Century Cures Act (Cures).¹⁵ Cures defines information blocking, and requires ONC in conjunction with the HHS Office of the Inspector General (OIG) to define business practices that do not constitute information blocking.¹⁶ It also authorizes OIG to root out information blocking, including authorizing levying fines of up to \$1 million per violation.¹⁷ On February 11, 2019, ONC released an “HHS approved” draft of its Notice of Proposed Rulemaking to Improve the Interoperability of Health Information, which will be published shortly in the Federal Register.¹⁸

Whether these provisions will be sufficiently strong to overcome firms’ incentives to engage in information blocking remains an open question. In what follows, we trace the background and public policy behind the federal government’s drive to dramatically increase the availability of clinical digital health data and its expectation that those data would be exchanged widely and appropriately.¹⁹ We focus on how the sharing (and lack of sharing) of clinical

¹³ HITECH subtitle A, part I, § 13001(1), defines Electronic Health Records statutorily. CMS (Centers for Medicare and Medicaid Services) offers a layperson’s definition as

an electronic version of a patient’s medical history, that is maintained by the provider over time, and may include all of the key administrative clinical data relevant to that person’s care under a particular provider, including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports.

U.S. Ctrs. for Medicare & Medicaid Servs., U.S. Dep’t of Health & Human Servs., Electronic Health Records (Mar. 26, 2012), www.cms.gov/Medicare/E-Health/EHealthRecords/index.html. Regulations promulgated by the Office of the National Coordinator for Health IT (ONC) (codified at 45 C.F.R. § 170.300 et seq.) specify the functions an EHR must meet to be “certified.” As is discussed, *infra* note 33, to be eligible to receive financial incentives from CMS, physicians and hospitals must use EHRs that are certified.

¹⁴ OFFICE OF THE NAT’L COORDINATOR FOR HEALTH INFO. TECH., U.S. DEP’T OF HEALTH & HUMAN SERVS., REPORT ON HEALTH INFORMATION BLOCKING (Apr. 2015) [hereinafter ONC INFORMATION BLOCKING REPORT], www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf.

¹⁵ Cures, *supra* note 5, Title IV, §§ 4001–4006.

¹⁶ *Id.* 130 Stat. 1177 (codified at 42 U.S.C. 300jj–52(a)(2)(C)).

¹⁷ *Id.* § 4004 (creating § 3022(b) of the Public Health Service Act, 42 U.S.C. § 300jj–52(b)).

¹⁸ 84 Fed. Reg. 7424 (Mar. 4, 2019), ONC Notice of Proposed Rulemaking to Improve the Interoperability of Health Information (Feb. 11, 2019), www.healthit.gov/topic/laws-regulation-and-policy/notice-proposed-rulemaking-improve-interoperability-health. ONC’s Notice of Proposed Rule Making is consistent with our analysis below because the proposed rule prohibits “information blocking” as defined, unless one of seven exceptions apply, but only when the activity is not anticompetitive, per a proposed 45 C.F.R. 170.404(a)(3)(i)(B)(4).

¹⁹ We focus on clinical digital health data from a care setting, as opposed to administrative digital health data, because the former has been the focus of HITECH and subsequent federal

R

R

digital health data affects competition. We analyze the problem from the perspectives of the health care providers and EHR vendors, the most important participants in the flow of patient medical data from an antitrust and policy perspective. We conclude with a look forward and suggestions of policy efforts that could shift firms' incentives from not sharing data to sharing it.

I. FEDERAL POLICY TO DIGITIZE HEALTH INFORMATION AND PROMOTE INFORMATION SHARING

In this Part, we first briefly describe the federal legal landscape that permits physicians and hospitals to exchange identifiable health information about patients they have in common. Next, we summarize how Congress built on that foundation in 2009 by enacting HITECH, creating significant financial incentives for physicians and hospitals to digitize their record keeping and to share the resulting digital data.

A. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT SUPPORTS INFORMATION SHARING

In 1996, Congress passed the Health Information Portability and Accountability Act (HIPAA).²⁰ Although this act is now synonymous with the health information privacy regulation it spawned, HIPAA actually focused on two other features. "Portability" refers to insurance coverage portability, not data portability. (Twenty years ago policy makers believed insurance coverage portability would help alleviate the worse health effects of pre-existing condition exclusions to insurance coverage.) "Accountability" referred to the federal legal requirement that, in order to be paid by CMS (Centers for Medicare and Medicaid Services), providers would have to bill CMS digitally and therefore digitize claims information. Thus, through HIPAA, Congress made its first attempt to bring the power of computing to health care, specifically in the context of data transmissions. To avoid unintended consequences deriving from the electronic billing requirement, Congress delegated to HHS the development of regulations that specified how digital health data can be accessed, used and disclosed.²¹ As a result, we have the HIPAA Privacy, Security and Breach Notification federal regulations still in use today.²² In general, unless

policy. While the sharing of claims data between payers and providers is an important topic, which is also subject to incentives and market forces, payers were not directly affected by the provisions of HITECH.

²⁰ HIPAA, *supra* note 4.

²¹ Daniel J. Solove, *HIPAA Turns 10: Analyzing the Past, Present and Future Impact*, 84 J. AHIMA 22 (2013).

²² Although 45 C.F.R. §§ 160–164 state all of the Privacy, Security and Breach Notification Rules, most of the Privacy Rule is found at 45 C.F.R. §§ 164.500–164.536, most of the Security Rule is found at 45 C.F.R. §§ 164.300–164.318, and most of the Breach Notification Rule, not relevant for the present discussion, is found at 45 C.F.R. §§ 400–414.

the context requires more specificity, we will simply refer to HIPAA for the totality of the Privacy, Security, and Breach Notification rules.

What HIPAA permits and requires by way of information sharing is important, because if HIPAA does not permit sharing, holders of data protected by HIPAA should not be accused of “information blocking.” But, where HIPAA permits or even requires data sharing, a failure to do so should be examined to make sure that HIPAA is not being employed as a pretext to justify data “hoarding,” as has been alleged by ONC,²³ or to prevent patients from being “poached.”²⁴ Therefore, we will briefly summarize what HIPAA permits and requires relative to information sharing.

The basic regulations governing when health information protected by HIPAA can be exchanged were written in 2000 and 2002, and are unchanged since then.²⁵ HIPAA applies to the holders of identifiable health information, called “protected health information” or PHI, when those holders (called “covered entities”) are physicians, hospitals, health plans (including self-funded employer medical benefits plans), and certain businesses that process digital health information for billing. We are focused on health information in the custody of physicians and hospitals. HIPAA further recognizes that covered entities will need to hire various “business associates” to serve special purposes. The Privacy and Security Rules apply to both covered entities and business associates either by regulation or contract. For hospitals and physicians, EHR vendors are their business associates under HIPAA.²⁶

HIPAA requires that when requested to do so, covered entities provide an individual with copies of that individual’s PHI. The individual can then do whatever he or she wants with it, including giving it to another covered en-

²³ Genevieve Morris, Principal Deputy Nat’l Coordinator for Health IT, Panelist at Annual Meeting of the Office of the Nat’l Coordinator for Health IT, at 27:16 (Nov. 30, 2017), events.tvworldwide.com/Events/ONCAAnnualMeeting2017_Breakout/Videoid/-1/UseHtml5/True.

²⁴ Seema Verma, Admin’r, Ctrs. for Medicare & Medicaid Servs., Remarks by Administrator Seema Verma at the ONC Interoperability Forum (Aug. 6, 2018), www.cms.gov/newsroom/press-releases/speech-remarks-administrator-seema-verma-onc-interoperability-forum-washington-dc.

²⁵ Office of the Nat’l Coordinator for Health Info. Tech. & HHS Office for Civil Rights Fact Sheets on exchange for treatment and exchange for health care operations of the recipient, published in 2016, describe and illustrate 45 C.F.R. §§ 164.501, 164.506, and some provisions of § 164.512. Office of the Nat’l Coordinator for Health Info. Tech., *Fact Sheets* [hereinafter *HIPAA Fact Sheets*], www.healthit.gov/topic/fact-sheets. In essence, as between two traditional health care organizations, like hospitals and physicians, the fact sheets show that exchange for treatment is *permitted* without first obtaining an individual’s written permission, but not *required*. In contrast, when an individual asks for a copy of his or her own health information, including electronically via a download or transmit function on an EHR, release of the data is *required*. See, e.g., 45 C.F.R. § 164.524. Thus, no federal regulations require physicians or hospitals to exchange health information with each other.

²⁶ See 45 C.F.R. § 164.504 (2000, amended 2013).

tity.²⁷ In HITECH, Congress interpreted this regulation, and required that where a person sought his or her PHI from a health care organization that used a certified EHR, the person must be able to view, download, or transmit their PHI to a recipient of his or her's own choosing,²⁸ including a competing provider. HIPAA also permits two covered entities to share PHI, without the person's written consent, about a person to whom they are both delivering care.²⁹ In 2015, the HHS Office for Civil Rights clarified that this permission includes sharing health information using ONC certified EHRs.³⁰ That guidance also specified that the disclosing covered entity was legally not responsible for the security conditions at the recipient covered entity. As a result, it is well documented that while other privacy rules may place additional restrictions on when and how sharing occurs, lack of health information sharing is not due to HIPAA specifically prohibiting it.³¹

B. HITECH INCENTIVIZES INFORMATION SHARING

HITECH,³² passed in 2009, provided over \$36 billion in incentive payments for physicians and hospitals to adopt and meaningfully use (as specified by CMS "Meaningful Use" criteria)³³ software (with functions prescribed by ONC)³⁴ to keep track of their patients' medical care through EHRs. HITECH provided further incentives for digitizing health records, this time clinical, not claims, data. Under HITECH, a physician or hospital that adopted a certified electronic health record that met minimum software specifications, and which used that software as specified by CMS Meaningful Use criteria, was eligible for significant payments—\$44,000 per physician for full Stage 1 compliance.³⁵ The incentive payments were intended to compensate providers for the acquisition costs of the EHRs.³⁶

²⁷ 45 C.F.R. § 164.524 (2000, amended 2013).

²⁸ HITECH, *supra* note 4, § 13405(e).

²⁹ 45 C.F.R. § 164.506(c)(2) & (c)(4).

³⁰ *HIPAA Fact Sheets*, *supra* note 25.

³¹ Michelle Mello, Julia Adler-Milstein, Lucia Savage & Karen Ding, *Legal Barriers to the Growth of Health Information Exchange—Boulders or Pebbles?*, 96 *MILBANK Q.* 110 (Mar. 2018) [hereinafter Mello et al., *Boulders or Pebbles*].

³² Pub. L. No. 111–5, 123 Stat. 226 (2009) (codified in scattered sections of U.S.C.).

³³ *See* HITECH, *supra* note 4, §§ 4101–4102; 42 C.F.R. §§ 412, 413, 422 & 495. This method—payment incentives for new behaviors it wants—now infuses many other CMS payment rules, such as the Medicare Inpatient Prospective Payment Rule for Hospitals and the Medicare Physician Fee Schedule for physicians. For example, see generally 2019 Medicare Inpatient Prospective Payment, 83 Fed. Reg. 41,144, 41,634–88 (Aug. 17, 2018).

³⁴ HITECH, *supra* note 4, § 3001; 42 C.F.R. § 170.300 et seq. (regulations).

³⁵ Ctrs. for Medicare & Medicaid Servs., Dep't of Health & Human Services, *An Introduction to the Medicare Meaningful Use Program for Eligible Professionals*, slide 12 (undated), www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/beginners_guide.pdf.

³⁶ HITECH, *supra* note 4, §§ 4101–4102.

R

R

R

R

R

This whole scheme was called “Meaningful Use” or “the Meaningful Use Program,” after language in HITECH.³⁷ Meaningful Use had three stages.³⁸ The criteria required to qualify for meaningful use payments became more demanding at each successive stage. For example, in Stage I physicians and hospitals had to attest to a criterion that required having received health information from someone else.³⁹ In Stage II, they had to attest to a criterion that required having sent it somewhere else, and to having allowed patients who wanted it the ability to download or transmit their own health information directly from the relevant EHR.⁴⁰

ARRA also made \$300 million available for seed money grants (to be awarded by ONC) to states or organizations designated by states, to build technical and governance infrastructure to enable physicians and hospitals to share information with each other.⁴¹ There were also funds available to Medicaid agencies within states to build connectivity and ensure that Medicaid beneficiaries also got the clinical and efficiency benefits of health information exchange.⁴² Even after the official “Meaningful Use” program began to end, CMS continues to use this method to change provider behaviors in general, and in particular about information sharing.⁴³

By the end of 2016, most of the \$36 billion had flowed to EHR vendors.⁴⁴ According to ONC, more than 95 percent of acute care hospitals and 78 percent of physicians were “meaningfully using” electronic health records, as a

³⁷ *Id.*

³⁸ Medicare & Medicaid Programs; Electronic Health Record Incentive Program, 75 Fed. Reg. 44,313 (July 28, 2010).

³⁹ Final Stage I regulations were effective in 2011 and superseded by subsequent regulations, all of which updated 42 C.F.R. § 170.300 et seq.

⁴⁰ 42 C.F.R. § 412 (for hospitals); 42 C.F.R. § 495 (for physicians). We note that with each year’s new measurement and incentive payment regulations, the regulatory nomenclature and incentive requirements change. For example, for calendar year 2019, what used to be called meaningful use for hospital is now called “promoting interoperability,” 2019 Medicare Inpatient Prospective Payment Rule, 83 Fed. Reg. 41,144, 41,635 (Aug. 17, 2018).

⁴¹ ARRA, *supra* note 4, Sec. 5, Div. A, Title I, ONC Appropriation, 123 Stat. 179 (2009).

⁴² Letter from Vikki Wachino, Dir., Ctrs. for Medicare & Medicaid Services, Dep’t of Health & Human Services, to State Medicaid Directors (Feb. 29, 2016), www.medicare.gov/federal-policy-guidance/downloads/smd16003.pdf.

⁴³ For example, the 2019 Medicare Inpatient Prospective Payment Rule still financially rewards hospitals which can attest to exchange for a single patient. 83 Fed. Reg. 41,144 (Aug. 7, 2018). As for financial penalties, the proposed 2019 Inpatient Payment Rule requested information on whether a failure to meet certain health sharing behaviors could lead to a hospital not being allowed to participate in the Medicare program at all. 83 Fed. Reg. 20,164, 20,550 (May 7, 2018). However, in the 2019 Medicare Inpatient Prospective Payment Rule, Medicare did not impose this type of penalty. 83 Fed. Reg. 41,144, 41,688 (Aug. 17, 2018).

⁴⁴ Joseph Conn, *Epic, Cerner EHRs Top the List for Hospital Meaningful-Use Payments*, MODERN HEALTHCARE (May 12, 2014), www.modernhealthcare.com/article/20140502/NEWS/305029944.

result of HITECH and its incentives.⁴⁵ This means that the vast majority of Americans have some, and possibly a lot, of their health data stored in digital form.

Although the volume of digital clinical health data grew substantially, data were not being exchanged. Many hospitals and providers met the Meaningful Use criterion that required electronic transmission of a summary of care record for at least 10 percent of transitions from provider to provider or one care setting to another (as part of meeting the second stage of Meaningful Use requirements).⁴⁶ Few of them, however, did so for the majority of care transitions.⁴⁷ National hospital data from 2014 reveal that only 25 percent of hospitals routinely engaged in four dimensions of interoperability—finding, sending, receiving, and integrating data from outside providers.⁴⁸ One year later, this had only increased to 30 percent, suggesting a slow transition to nationwide interoperability.⁴⁹

In parallel with national data revealing slow progress on interoperability, anecdotal reports of information blocking emerged.⁵⁰ Lawmakers and other stakeholders became concerned that the slow progress on interoperability was, at least in part, driven by information blocking behaviors. In response, Congress requested that ONC investigate.⁵¹

The resulting report⁵² summarized available evidence of information blocking and included examples of these practices, including unreasonably high fees for technical connections, pretextual use of privacy laws as a justification for not sharing information, and various contractual and other business practices that limit the exchange of information with competitors. The agency con-

⁴⁵ OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., OFFICE OF THE SEC'Y, U.S. DEP'T OF HEALTH & HUMAN SERVS., 2016 REPORT TO CONGRESS ON HEALTH IT PROGRESS: EXAMINING THE HITECH ERA AND THE FUTURE OF HEALTH IT SUBMITTED PURSUANT TO SECTION 3001(C)(6) OF THE PUBLIC HEALTH SERVICE ACT AND SECTION 13113(A) OF THE HITECH ACT (2016) at 5.

⁴⁶ CMS Electronic Health Record Stage 2 Final Rule, 79 Fed. Reg. 52,909 (Sept. 4, 2014).

⁴⁷ Sunny C. Lin, Jordan Everson & Julia Adler-Milstein, *Technology, Incentives, or Both? Factors Related to Level of Hospital Health Information Exchange*, 53 J. HEALTH SERVS. RES. 3278 (2018).

⁴⁸ A Jay Holmgren, Vaishali Patel & Julia Adler-Milstein, *Progress in Interoperability: Measuring US Hospitals' Engagement in Sharing Patient Data*, 36 HEALTH AFF. 1820, 1820 (2017).

⁴⁹ *Id.* at 1825.

⁵⁰ This is summarized in Nick Terry, *Information Blocking and Interoperability*, BILL OF HEALTH (Dec. 19, 2014), blogs.harvard.edu/billofhealth/2014/12/19/information-blocking-and-interoperability/.

⁵¹ 2015 Budget Act, *supra* note 12, 128 Stat. 2483–484. *See also* 160 CONG. REC. H9839 (daily ed. Dec. 11, 2014) (explanatory statement submitted by Rep. Rogers, chairman of the House Committee on Appropriations, regarding the Consolidated and Further Continuing Appropriations Act, 2015).

⁵² ONC INFORMATION BLOCKING REPORT, *supra* note 14, at 17.

R

R

cluded both that information blocking was occurring and that it was a serious impediment to the appropriate flow of health information.⁵³

Further, the ONC Information Blocking Report expressed concern that one aspect of information blocking represented potentially anticompetitive conduct. EHR developers and health care providers were not exchanging health information outside their closed systems. ONC's concern was that this failure to exchange information sometimes reflected deliberate attempts to disadvantage rivals by withholding information.⁵⁴

From a legal perspective, providers and hospitals received substantial financial payments for legally attesting to having undertaken certain activities, including a specific, albeit minimal level of exchange.⁵⁵ If the attestations were proved false, they would be subject to the same rules as any other false or fraudulent claim to CMS.⁵⁶ However, the second, and more likely, scenario was a set of activities that were not false attestations. For example, the amount of activity required to meet the incentive milestone was sometimes quite low, such as a single occurrence of information exchange with an unaffiliated provider in a 12-month period. In practice, providers and hospitals could both legally attest to the minimal quantity amounts of exchange and still engage in information blocking beyond those minimums.

We do not know whether CMS and ONC were "naïve"⁵⁷ regarding the prospect that organizations would meet the requirements while still engaging in information blocking, or realized the possibility but did not think it would be widespread. By the time it wrote the Information Blocking Report, however, ONC clarified that HITECH was enacted with the goal of spurring data-driven competition among health care delivery organizations.⁵⁸

As mentioned earlier, following ONC's February 2015 report, Congress responded in 2016 by enacting the 21st Century Cures Act,⁵⁹ outlawing information blocking, except as required by law or specified in future

⁵³ See, e.g., *id.* at 16.

⁵⁴ *Id.* at 15.

⁵⁵ See, e.g., *id.* at 4, 17.

⁵⁶ Press Release, U.S. Dept. of Justice, Electronic Health Records Vendor to Pay \$155 Million to Settle False Claims Act Allegations (May 31, 2017), www.justice.gov/opa/pr/electronic-health-records-vendor-pay-155-million-settle-false-claims-act-allegations.

⁵⁷ Sarah Kliff, *The Fax of Life: Why American Medicine Still Runs on Fax Machines*, Vox (Jan. 12, 2018), www.vox.com/health-care/2017/10/30/16228054/american-medical-system-fax-machines-why.

⁵⁸ Promoting "a more effective marketplace, greater competition . . . increased consumer choice, and improved outcomes in health care services" is one of the express purposes of a nationwide health IT infrastructure for health information exchange. ONC INFORMATION BLOCKING REPORT, *supra* note 14, at 10. See also Public Health Service Act § 3001(b)(10), 42 U.S.C. § 300jj-11(b)(10).

⁵⁹ Cures, *supra* note 5, §§ 4001-4006 (codified in scattered sections of 42 U.S.C.).

rulemaking.⁶⁰ It also directed the HHS Office of the Inspector General and ONC to collectively develop standards via rulemaking for recognizing unlawful information blocking.⁶¹

Meanwhile, there was an effort to examine the extent of information blocking by surveying leaders of digital health data exchange efforts across the country. The survey revealed that 60 percent of respondents reported that hospitals and health systems routinely or occasionally engage in information blocking, while 85 percent of respondents reported that EHR vendors do so.⁶² The survey also identified common forms of information blocking pursued by providers (e.g., controlling patient flow by selectively sharing data) and by EHR vendors (e.g., charging fees for sharing that were unrelated to actual cost to provide sharing capabilities).⁶³ While not all health care stakeholders are convinced that information blocking is real,⁶⁴ prominent stakeholders, including the American Medical Association, American Academy of Family Practitioners, and Health IT Now continue to advocate to ONC and OIG on whether information blocking is a significant problem and, if so, how it should be defined.⁶⁵ Recently, Principal Deputy National Coordinator Genevieve Morris declared, “We have to stop competing on hoarding data.”⁶⁶ And Medicare Administrator Seema Verma stated that hospital “[s]ystems too often refuse to share data because they fear their patients will be poached. This mentality has to be changed because it endangers the health of millions of Americans.”⁶⁷

As the preceding demonstrates, federal law requires or permits information sharing, and Congress has gone to great and repeated lengths to promote shar-

⁶⁰ *Id.* § 4004 (codified at 42 U.S.C. § 300jj-52(a)(1)).

⁶¹ *Id.* § 4006(a)(3), 130 Stat. 1177 (codified at 42 U.S.C. § 300jj-52(a)(3)) (“The Secretary, through rulemaking, shall identify reasonable and necessary activities that do not information blocking for purposes of paragraph.”).

⁶² Julia Adler-Milstein & Eric Pfeiffer, *Information Blocking: Is It Occurring and What Policy Strategies Can Address It?*, 95 MILBANK Q. 117 (2017).

⁶³ ONC INFORMATION BLOCKING REPORT, *supra* note 14, at 15.

⁶⁴ *Dr. John Halamka: 4 Thoughts on MU, Information Blocking and Interoperability*, BECKER'S HOSP. REV. (June 02, 2015), www.healthleadersmedia.com/innovation/countdown-information-blocking-rule-progress (quoting John Halamka, MD, CIO of Harvard-affiliated Beth Israel Deaconess Medical Center in Boston, “I’ve never seen it. Find me one example”); Mandy Roth, *Countdown to Information Blocking Rule in Progress*, HEALTH LEADERS MEDIA (Sept. 28, 2018), www.healthleadersmedia.com/innovation/countdown-information-blocking-rule-progress (quoting Marc Probst, CIO of Intermountain Health Care in Utah, “Data blocking is a bit like a mythical creature. . . . I think they [IHHS] are stretching it a bit when they talk about some of the things that have happened around data blocking.”).

⁶⁵ Press Release, Health IT Now, *Health IT Now Sends Information Blocking Recommendations to ONC, HHS and OIG* (Aug. 29, 2017), www.healthitnow.org/press-releases/2017/8/29/health-it-now-sends-information-blocking-recommendations-to-one-bhs-oig (reporting that a group of organizations, including IBM and the American Academy of Family Physicians, sent recommendations for addressing information blocking to ONC).

⁶⁶ Morris, *supra* note 23, at 27:16.

⁶⁷ Verma, *supra* note 24.

R

R
R

ing. Yet, exchange is not occurring at the rates hoped for, or even anticipated. Therefore, this prompts us to consider what else may be driving or contributing to the low rates of exchange. Below, we examine all the justifications that have been reasonably asserted and conclude that anticompetitive motivations may be suppressing the rate of health information exchange, despite a clear public policy favoring it. In Part IV, we suggest additional actions that could be undertaken to better understand why rates of health information exchange remain so low and potentially to help remedy the problem.

II. FACTORS AFFECTING INFORMATION SHARING

In what follows we consider legal or technical factors that may impede data sharing among health care organizations, then explain how these factors (privacy, security, technical challenges, etc.) relate to different health care organizations' financial incentives. We conclude that these firms too often make it harder than it needs to be (legally or technically) for patients to take their data to other firms because this can inhibit patients or customers from moving their business to competing providers. This conduct thwarts federal policy goals of increasing consumer choice and competition in health care.

A. JUSTIFICATIONS FOR NOT SHARING HEALTH INFORMATION

Health care systems and providers, as well as EHR vendors, have offered various justifications for not exchanging health information. These include patient privacy, ensuring proper security of health information, intellectual property, and the costs and complexity of software interfaces. While some of these are legitimate (at least in certain circumstances), some do not hold up legally or factually. We discuss each of these below. For example, health care providers have claimed that HIPAA regulations are a reason why information cannot be shared. However, as we demonstrated above, this nationwide health privacy law actually has more than a dozen reasons why sharing health information among providers is permitted or even required.⁶⁸ In addition, while there are some technical challenges associated with sharing digital health data, experts believe these technical barriers can be overcome, as they have been in other industries.⁶⁹

⁶⁸ See, e.g., 45 C.F.R. § 164.506(c) (listing some reasons why disclosure is permitted); C.F.R. § 164.524 (stating disclosures required to an individual of their own health information).

⁶⁹ ONC API Task Force Recommendations (May 12, 2016) [hereinafter ONC API Task Force], www.healthit.gov/sites/default/files/facsys/HTITC_APITF_Recommendations.pdf; see also ESAC Inc. & SRS, Inc., KEY PRIVACY AND SECURITY CONSIDERATIONS FOR HEALTH CARE APPLICATION PROGRAMMING INTERFACES (APIS) (Dec. 2017) (Contract: HHSP23320160022 4A), www.healthit.gov/sites/default/files/privacy-security-api.pdf; ONC INFORMATION BLOCKING REPORT, *supra* note 14, at 8; Mello et al., *Boulders or Pebbles*, *supra* note 31.

In what follows, we first discuss factors affecting information sharing by EHR developers, then health care providers. We analyze their financial incentives regarding information sharing, and legal or technical barriers to doing so.

B. FINANCIAL INCENTIVES AFFECTING EHR DEVELOPERS' INFORMATION SHARING

As discussed above, Congress provided significant financial incentives through the Meaningful Use program to make health information exchange more widespread, and the basic federal health information law permits the contemplated exchange without the written permission of the individual.⁷⁰ Despite this, there is still little exchange of data. In order to understand this, one must examine how firms' overall economic interests are affected by data exchange. At present no business model exists for EHR companies to profit from data sharing. In fact, holders of PHI are not allowed to sell it,⁷¹ and for permitted disclosures (discussed in Part I.A above), PHI holders are allowed to recover only their "reasonable" costs for preparing and transmitting data.⁷² On the other hand, EHR companies may have substantial financial incentives to retain data and avoid facilitating their physician and hospital customers from sharing the health information outside of business relationships the EHR company controls.

While the financial incentives at play for any given vendor depend on its business model, and precise information on the business models used is not publicly available, there is a common understanding of how different business models create competitive benefit from not sharing data.⁷³ The first and most direct incentive is the way vendors are paid. An EHR company that is paid based on the number of individuals whose records they process has strong incentives to retain the data and strong disincentives to make it easy for an individual to move their data to a competing provider. When patient data migrate from one vendor to another, the source vendor directly loses revenue, which is gained by competitors.

A second financial incentive to retain data is that the data held by an EHR company can be exploited for analytics. The greater the volume of data a firm

⁷⁰ 45 C.F.R. 164.506(c).

⁷¹ 45 C.F.R. 164.502(a)(5)(viii) (interpreting HITECH, *supra* note 4, § 13406 (codified at 42 U.S.C. 17936 (2009))).

⁷² 45 C.F.R. 154.502(a)(5)(iii) & (viii).

⁷³ Jordan Everson & Julia Adler-Milstein, *Engagement in Hospital Health Information Exchange Is Associated with Vendor Marketplace Dominance*, 35 HEALTH AFF. 1286 (2016) (finding that there is more information exchange in markets where the dominant EHR vendor has a smaller market share, suggesting that competition and information exchange may be positively related).

holds, the more informative, and hence valuable, the analytics it can produce are for customers, who may use them for research, clinical decision support, business decision support, etc.⁷⁴ An NIH blog suggests that EHR data may be “the most high-value data set to come.”⁷⁵ For example, this year, Flatiron Health, a privately held oncology EHR company, sold for \$1.9 billion because of the value of its data.⁷⁶

A third financial incentive affecting information sharing is that lack of interoperability between EHRs can financially benefit the EHR companies. If an EHR is more valuable to any user the more it is adopted by other users, then EHR companies have a strong incentive to build and retain market share to become the dominant EHR.⁷⁷ This is because if an EHR has more patients, it has more data for analysis, an attractive feature for prospective providers.⁷⁸ The EHR vendor is thus likely to become a “must have” data destination. Interoperability undermines that value, enabling providers to acquire patient records outside that particular vendor and its closed environment.

In its Information Blocking Report, ONC discussed the rise of these “walled gardens,” technical environments in which every provider who contracts with that EHR developer may be able to exchange with other customers of that vendor, but not outside the “garden walls.”⁷⁹ A dominant vendor has the most data on the most patients within the referral market, and on the most physicians in the referral market. This dominant position creates pressure for providers not using the dominant vendor to switch because that is where the patient data are. While, of course, there may be interoperability *within* one EHR developer’s data system used by many providers, effective competition among EHR developers and the innovation and downward price pressure it brings, languishes.

⁷⁴ An example is Flatiron Health, which developed and hosts data for an oncology-only EHR, with the express business model of aggregating data sets to improve cancer research, better clinical decision support, etc. Christina Farr, *At Flatiron Health, Keeping the Doctor Close*, FAST COMPANY (Apr. 19, 2017), www.fastcompany.com/3067893/at-flatiron-health-keeping-the-doctor-close.

⁷⁵ Patti Brennan, *Is the EHR the New Big Data?*, NAT’L INST. OF HEALTH, DataScience@NIH, (Mar. 24, 2017), datascience.nih.gov/BlogIsTheEHR.

⁷⁶ Sy Mukherjee, *Why Drug Giant Roche’s \$1.9 Billion Deal to Buy Data Startup Flatiron Health Matters*, FORTUNE (Feb. 16, 2018), fortune.com/2018/02/16/roche-flatiron-health-deal-why-it-matters/.

⁷⁷ This phenomenon is referred to as a “network externality.” A product or service is more valuable the more other people adopt or use it. This phenomenon is familiar from computer operating systems and software, microprocessors, telecommunications, and electronic marketplaces.

⁷⁸ Depending on the EHR developer’s business model, greater numbers of patient records may also mean greater revenue.

⁷⁹ ONC INFORMATION BLOCKING REPORT, *supra* note 14, at 17–18.

A fourth form of financial incentive is that EHR developers can and do charge providers high fees for connectivity to other vendor systems or with third parties, such as fees that a developer charges to engineer software to connect securely to another vendor's software. These make interoperability, and thus data sharing, expensive, but improve the developer's bottom line. Of course, fees at some level may be reasonable, but providers (especially small practices, which constitute the majority of providers outside of hospitals)⁸⁰ argue that the fees are disproportionately high compared to the technological challenge, do not account for economies of scale, and in fact are priced high to discourage connectivity and exchange.⁸¹ Thus, the fees can serve as financial barriers for physicians who want to exchange data with providers who use competing EHR systems, and confine those physicians to the aforementioned "walled gardens." Thus, charging high fees can be a strategy for data holders to impede data transfer and thwart competition. This may be a version of the strategy of raising rivals' costs to thwart competition.⁸²

Developers, however, argue that they need to restrict information sharing to protect the intellectual property underlying their systems. In particular, there is concern that making information available for sharing could reveal two business sensitive sources of IP: (1) their underlying data model (i.e., how information is stored and organized), and (2) how the data are presented (i.e., aspects of their user interface). For example, Cerner's terms of use prohibit the Los Angeles County Department of Health Services from disclosing "source code, prices, trade secrets, mask works, databases, designs and techniques, models, displays and manuals."⁸³

When source code cannot be disclosed, competing EHR developers, or physicians who hire their own software engineers, cannot develop the tools to

⁸⁰ According to the AMA, in 2015 more than 60% of physicians provide care in practices of 10 or fewer physicians. See Press Release, Am. Med. Ass'n, AMA Study Finds Majority of Physicians Still Work in Small Practices (July 8, 2015), www.ama-assn.org/content/new-ama-study-reveals-majority-americas-physicians-still-work-small-practices.

⁸¹ ONC INFORMATION BLOCKING REPORT, *supra* note 14, at 15–17. *America's Health IT Transformation: Translating the Promise of Electronic Health Records into Better Care: Hearing Before the S. Comm.*, 114th Cong. 114-578 (Mar. 17, 2015), 161 CONG. REC. D279 (Mar. 17, 2015); *Achieving the Promise of Health Information Technology: Information Blocking and Potential Solutions, Hearing Before S. Comm. on Health, Education, Labor and Pension*, 114th Cong. 670 (July 23, 2015), 161 CONG. REC. D870 (daily ed. July 23, 2015); *Achieving the Promise of Health Information Technology, Hearing Before S. Comm. on Health, Education, Labor and Pension*, 161 CONG. REC. D870 (daily ed. Oct. 1, 2015) [collectively, *Senate Information Blocking Hearings*], www.help.senate.gov/hearings/achieving-the-promise-of-health-information-technology.

⁸² Steven C. Salop & David T. Scheffman, *Raising Rivals' Costs*, 73 AM. ECON. REV. 267 (1983).

⁸³ Darius Tahir, *Doctors Barred from Discussing Safety Glitches in U.S.-Funded Software*, POLITICO (Sept. 11, 2015), www.politico.com/story/2015/09/doctors-barred-from-discussing-safety-glitches-in-us-funded-software-213553.

engineer appropriate data connections between two vendors' systems, even if this is what the providers want for patient care. The legitimacy of intellectual property must be recognized and protected, but as in other areas of IT,⁸⁴ developers need to make key information available to others who are engineering connections or applications to the platform.⁸⁵

In fact, creating open specifications, available to third-party developers, was a key goal of the API provisions of ONC's 2015 rule.⁸⁶ How EHR developers are responding is mixed. On the one hand, they seem to be listening: as of June 2018, 159 developers of certified EHRs have proven to ONC that they have shipped this update to their customers, even if their customers, the providers and hospitals,⁸⁷ are not required to make it available until January 2019.⁸⁸ But according to Aneesh Chopra, former Chief Technology Officer for the United States, only a handful of hospitals have actually turned on this functionality.⁸⁹ There is also public concern that despite including the API technology, the two largest EHR developers are charging high fees for third-

⁸⁴ See, e.g., Decision & Order, Intel, FTC Docket No. 9341 (Oct. 29, 2010), www.ftc.gov/enforcement/cases-proceedings/061-0247/intel-corporation-matter; MSC Software Corp., FTC Docket No. 9299 (June 10, 2003), www.ftc.gov/enforcement/cases-proceedings/0010077/msc-software-corporation; Silicon Graphics, 60 Fed. Reg. 35,032 (July 5, 1995); Press Release, Fed. Trade Comm'n, Silicon Graphics, Inc. (June 9, 1995), www.ftc.gov/news-events/press-releases/1995/06/silicon-graphics-inc.

⁸⁵ In its rule on Certified EHRs, ONC required for the first time that developers add to the next version an "open specification, read-only" application programming interface, such as is commonly used for financial data already. See 45 C.F.R. § 170.315(g)(7), (8) & (9); 2015 Ed. Health Information Technology (Health IT) Certification Criteria, 80 Fed. Reg. 62,602 (Oct. 16, 2015) [hereinafter 2015 Health IT Cert Criteria]. CMS then required in its payment rules under the Medicare Access and CHIP Reauthorization Act of 2015, Pub. L. No. 114-10, 129 Stat. 87 (codified in scattered sections of 42 U.S.C.), that physicians seeking incentive payments allow developers to use those open specifications to develop third-party apps, which individuals would use to get copies of their own health information, called "consumer mediated exchange," or a B2C transaction. Medicare 2018 Updates to the Quality Payment Program, 82 Fed. Reg. 77,908 (Nov. 1, 2016). CMS repeated this requirement for hospitals in its 2018 Medicare Inpatient Prospective Payment Rule, 82 Fed. Reg. 53,568 (Nov. 16, 2017), and reiterated that effective date in the 2019 Medicare Inpatient Prospective Payment Rule, 83 Fed. Reg. 41,144, 41,635-36 (Aug. 17, 2018). It remains to be seen if requiring this change in the software functionality will facilitate greater amounts of business-to-business/provider-to-provider exchange.

⁸⁶ 2015 Health IT Cert Criteria, *supra* note 85, 80 Fed. Reg. 62,602, 62,675-76 (Oct. 16, 2015) (noting that how organizations implement the required API should not "block" information sharing by API).

⁸⁷ ONC CERTIFIED HEALTH IT PRODUCTS LIST, CHPL.HEALTHIT.GOV (June 12, 2018), chpl.healthit.gov/#/collections/apiDocumentation (public dataset).

⁸⁸ 82 Fed. Reg. 53,568 (Nov. 16, 2017); Seema Verma, Admin'r of Ctrs. for Medicare & Medicaid Servs., Remarks at the HIMSS18 Conference (Mar. 26, 2018), www.cms.gov/Newsroom/MediaReleaseDatabase/Press-releases/2018-Press-releases-items/2018-03-06-2.html.

⁸⁹ Aneesh Chopra, Pres., CareJourney, Unleashing Data to Transform Health Care Panel, 2018 EHR National Symposium at Stanford Medicine, at 12:20 (June 4, 2018), youtu.be/qgLLiabDFU.

R

party apps to connect,⁹⁰ and as a result, may be inappropriately raising their rivals' costs.⁹¹

An EHR developer's intellectual property is worthy of protection. That protection does not extend, however to the health facts that comprise PHI.⁹² Those property rights have limits. For example, a patient's blood sugar test result describes what is occurring in his or her blood. The health fact—blood sugar—may be displayed in a certain manner, with the display potentially being a developer's intellectual property. But the existence of the display does not convert the naturally occurring health fact into the developer's intellectual property.

Furthermore, HIPAA makes it clear that people have a right to obtain from their physicians and hospitals their own PHI, even when extracted from an EHR, and notwithstanding any intellectual property that might exist in the display the developer developed. The patient's right, in existence at least since HIPAA was passed, pre-dates the development of any EHR software IP.⁹³ Moreover, under HIPAA the developer has no rights to use the PHI for its own business purposes, because under HIPAA, it is merely a business associate.⁹⁴

Data security is another factor that is cited as a barrier to information sharing. HIPAA requires that data must be kept secure. Health care providers are right to want to be confident that health information exchange does not introduce unexpected security risks into their environment, and to look to some extent to their EHR developers to provide a secure environment.⁹⁵ But often security and exchange can both be achieved, and providing a secure environment should not be an impediment to exchange.

⁹⁰ Arthur Allen, *Developers Complain of High EHR Fees for SMART Apps*, POLITICO (Aug. 6, 2018), www.politico.com/newsletters/morning-ehealth/2018/08/06/one-interop-forum-kicks-off-306709 (note: a longer version of this publication is available behind Politico's paywall).

⁹¹ Salop & Scheffman, *supra* note 82.

⁹² *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, 569 U.S. 576 (2013). There, the Supreme Court reversed an appellate court ruling that a DNA sequence found in nature could be patented. The Court wrote: "It is undisputed that Myriad did not create or alter any of the genetic information encoded in the BRCA1 and BRCA2 genes. The location and order of the nucleotides existed in nature before Myriad found them. . . . To be sure, it found an important and useful gene, but separating that gene from its surrounding genetic material is not an act of invention." *Id.* at 590–91.

⁹³ Lucia Savage, *To Combat "Information Blocking," Look to HIPAA*, HEALTH AFF. BLOG (Aug. 24, 2017), www.healthaffairs.org/doi/10.1377/hlblog20170824.061636/full/.

⁹⁴ 45 C.F.R. § 164.504.

⁹⁵ OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., DEPT. OF HEALTH & HUMAN SERVS., *EHR CONTRACTS UNTANGLED: SELECTING WISELY, NEGOTIATING TERMS, AND UNDERSTANDING THE FINE PRINT* 9 (2016), www.healthit.gov/sites/default/files/EHR_Contracts_Untangled.pdf.

In particular, “fake security”⁹⁶ concerns should not undermine interoperability or be an excuse for not allowing sharing of information through competing EHR vendors. For example, an open-specification API, such as ONC prescribed in its 2015 edition rule,⁹⁷ could be both secure and enable low cost exchange. Indeed, as was clear from evidence presented in public hearings convened by ONC, in most other internet-enabled industries (finance is often the example), businesses and their software engineers and security professionals have adopted methods to keep information flowing while maintaining security.⁹⁸ Certainly important regulators, like the CMS Administrator, think EHR developers may have strategically inflated security concerns as a way of impeding exchange.⁹⁹

Last, developers understand there have yet to emerge policies that could counter-balance any urge to hoard data. They may rightly calculate that, without the probability of significant consequences, making exchange hard makes business sense. As we discuss below, there are some steps that can be taken to better understand the impact on health care competition of low levels of information sharing.

C. FACTORS AFFECTING HEALTH CARE PROVIDERS’ INFORMATION SHARING

No one doubts that physicians, nurses, and the health systems and hospitals in which the majority of health care is delivered want to help their patients. But health care providers and health care systems are businesses, and therefore operate within the realities of the marketplace.¹⁰⁰ We note that while in general federal law does not require providers to exchange data with each other, it does give them quite a bit of flexibility to exchange when they choose to do so. Thus, we explore whether there are incentives on the provider side that explain the low levels of exchange, despite liberal permissions to exchange.

To understand how providers view the competitive implications of information exchange, we turn first to the traditional fee-for-service (FFS) payment system—that is, where the supplier is paid for each service. Doctors and hospitals are sales revenue driven organizations. The overwhelming majority of their revenues come from payments from private insurers and Medicare and

⁹⁶ Andy Slavitt, Admin’r of Ctrs. for Medicare & Medicaid Servs., Andy Slavitt and Dr. Karen DeSalvo Panel Discussion at HIMSS (Mar. 14, 2016), www.hitechanswers.net/andy-slavitt-and-dr-karen-desalvo-panel-discussion-at-himss/.

⁹⁷ 42 C.F.R. § 170.315(g) (7), (8) & (9).

⁹⁸ See, e.g., ONC API Task Force, *supra* note 69, at 27; ESAC Inc. & SRS, Inc., *supra* note 69.

⁹⁹ Slavitt, *supra* note 96.

¹⁰⁰ Grossman et al., *supra* note 11, at 1.

R

R

R

Medicaid. As a consequence, providers make money by attracting and retaining (profitable) patients. Making information readily available and transportable helps patients seek out new, and potentially competing, providers. This may make it harder to retain patients and the health insurance fees their care generates. Patients who are mobile may lead to tougher competition among providers. Patients benefit substantially from tougher competition that leads to lower prices and higher quality, but providers are typically worse off.

Furthermore, even as the fee-for-service system evolves to payment for value or population health outcomes, providers who are responsible for a patient's overall care may lose control if a patient receives care outside their system. Thus, even in this type of system, providers may want to keep their patients in the system, even if it is not where the individuals would receive the best or most appropriate care.¹⁰¹ In principle, it is possible for providers paid on a value basis to contract in a mutually advantageous way for patient care, so that patients are appropriately referred and incentives are maintained. In this situation information sharing is critical—indeed, appropriate and efficient referrals for care cannot take place without it.

As a specific example, Aledade is a start-up seeking to help independent (non-hospital owned) ambulatory practices deliver high-value care using a built-in infrastructure Aledade supplies to enable information exchange. Because Aledade's business model focuses on independent practices collaborating with each other and sharing financial risk for keeping their collective patients out of hospitals,¹⁰² it may prove a counterweight to any tendency of hospital-owned practices to exchange only with other doctors sharing a single information technology system or an integrated ownership structure.¹⁰³

Yet, even information exchange patterns among independent practices can create incentives for a different kind of walled garden, one bounded by referral patterns (instead of proprietary technology), where the institutions choose to allow (or prioritize) disclosure only to specific established electronic ad-

¹⁰¹ Evidence shows that physician referral patterns are substantially altered when a practice is owned by a hospital, in particular that physician practices owned by a hospital refer substantially more to that hospital than to other hospitals, even if the care at that hospital is of lower quality than elsewhere. Laurence C. Baker, M. Kate Bundorf & Daniel P. Kessler, *The Effect of Hospital/Physician Integration on Hospital Choice*, 50 J. HEALTH ECON. 1 (Dec. 2016). This illustrates that providers respond to incentives (in this example, hospital ownership) by altering their behavior to keep patients in the system.

¹⁰² Brian W. Powers et al., *Engaging Small Independent Practices in Value-Based Payment: Building Aledade's Medicare ACOs*, 6 HEALTHCARE 79 (2018).

¹⁰³ Farhad Manjoo, *A Start-Up Suggests a Fix to the Health Care Morass*, N.Y. TIMES (Aug. 16, 2017), www.nytimes.com/2017/08/16/technology/a-start-up-suggests-a-fix-to-the-health-care-morass.html.

dresses, or make it difficult for patients to identify secure electronic delivery locations for data they want sent to their other doctors.¹⁰⁴

As has been made clear, there are strong financial incentives to retain data and not to share it. In contrast, it is hard to identify a profitable business model that involves information sharing. These concerns about information blocking and provider competition are not merely theoretical. FTC officials blogged in October 2014 about their interest in the implications of provider competition on EHRs and the data they create.¹⁰⁵

III. CURRENT POLICIES TO ADDRESS DATA BLOCKING

Congress has noticed that health information is not flowing freely among health care providers and has some evidence to suggest that anticompetitive motivations are partly to blame.¹⁰⁶ However, the extent to which anticompetitive conduct is responsible remains unclear, as well as whether such conduct is due to the vendors, the providers, or both. Nor do we know if the incentives hindering exchange of information are symbiotic or merely happen to be contemporaneous. For example, is EHR connectivity costly and difficult because vendors are responding to their provider customers' desires to avoid exchanging data, or would providers be willing to exchange data, but lose interest because of the costs and difficulties with EHR connectivity and compatibility? Are the costs and complexity associated with connectivity legitimate, or are they driven by strategic motives on the part of EHR vendors? What role, if any, do developers' concerns about IP and their security obligations play?

On the provider side, the Meaningful Use regulations continue to require attestation to higher levels of electronic transmission of summary of care records during patient transitions. Specifically, Stage 3 criteria raise the bar from 10 percent to 50 percent, and impose penalties on eligible providers and hospitals that do not meet these thresholds. Nonetheless, thus far Meaningful Use has not been a sufficiently strong driver to result in widespread exchange. Therefore, in January 2015, Congress attempted to further increase incentives when it passed the Medicare Access and CHIP Reauthorization Act of 2015

¹⁰⁴ Keith Boone, *What's My Doctor's Direct Address*, HEALTHCARE STANDARDS (Aug. 18, 2017) (Dec. 16, 2017), motorcycleguy.blogspot.com/2017/08/whats-my-doctors-direct-address.html (an example of making opaque to a patient how to securely transmit PHI to another, unaffiliated provider).

¹⁰⁵ Tara Isa Koslov, Office of Pol'y Planning, Markus Meier, Bureau of Competition & David R. Schmidt, Bureau of Econ., Fed. Trade Comm'n, *Promoting Healthy Competition in Health IT Markets*, COMPETITION MATTERS (Oct. 7, 2014), www.ftc.gov/news-events/blogs/competition-matters/2014/10/promoting-healthy-competition-health-it-markets. See also Amalia R. Miller & Catherine Tucker, *Health Information Exchange, System Size and Information Silos*, 33 J. HEALTH ECON. 28 (2014) (finding that large hospital systems strategically prevent outflow of patient data to maintain their competitive advantage).

¹⁰⁶ *Senate Information Blocking Hearings*, *supra* note 81.

(MACRA).¹⁰⁷ This Act replaced the old Medicare payment formula with a sweeping new payment method that requires payments for Medicare physician services be based on value and measured outcomes. These measures and outcomes, in turn, were to be specified in regulations.¹⁰⁸ The resulting regulations for payment years 2017 and 2018 increase the amount of care that is paid based on measured outcomes, and those outcomes are calculated in part using the digital health data HITECH made widely available.¹⁰⁹ Among the new measures is an attempt to measure exchange as part of the “advancing care information” domain.¹¹⁰ To achieve top marks in this domain for calendar 2017, however, a physician needed only exchange a summary of care record with a single other physician.¹¹¹ For calendar 2019, CMS proposes only that hospitals need prove information exchange on behalf of only one individual.¹¹²

Despite enacting MACRA in late 2015 (with more incentives payable for exchange but no explicit provisions on information blocking), it appears that Congress remained concerned that information was still being blocked. After holding three hearings on the subject of information blocking,¹¹³ in December 2016, it enacted Cures, which contains elements designed to address this issue directly.¹¹⁴ Cures itself defines “information blocking,” and charged HHS with identifying conduct that is not “information blocking” and rooting out and punishing information blocking when it occurs.¹¹⁵

Specifically, 21st Century Cures says that a practice is information blocking: “(ii) if conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or mate-

¹⁰⁷ Pub. L. No. 114–10, 129 Stat. 87 (2015) (codified in scattered sections of 42 U.S.C.) [hereinafter MACRA].

¹⁰⁸ MACRA regulations for physician payment are published as part of the Medicare Physician Fee Schedule rules, and are updated annually. See 42 C.F.R. § 495. There are corollary rules for hospitals published in the Medicare Inpatient Prospective Payment System rule, also updated annually. See 42 C.F.R. § 412 as finalized in the rule published at 83 Fed. Reg. 41,144 (Aug. 17, 2018).

¹⁰⁹ 82 Fed. Reg. 53,568, 53,570 (Nov. 16, 2017). Measures and relation to certified EHR technology are explained at CMS, *2018 Promoting Interoperability, QUALITY PAYMENT PROGRAM*, qpp.cms.gov/mips/explore-measures/promoting-interoperability?py=2018measures.

¹¹⁰ CMS Quality Payment Program, *Merit-based Incentive Payment System (MIPS): Participating in the Advancing Care Information Performance Category in the 2017 Transition Year*, www.cms.gov/Medicare/Quality-Payment-Program/Resource-Library/MIPS-Advancing-Care-Information-101-Guide.pdf.

¹¹¹ CMS, *Promoting Interoperability (PI) Requirements, QUALITY PAYMENT PROGRAM*, qpp.cms.gov/mips/advancing-care-information (CMS explanation measures under its Quality Payment Program).

¹¹² 2019 Medicare Inpatient Prospective Payment Rule, 83 Fed. Reg. 20,164, 20,550 (proposed May 7, 2018), 83 Fed. Reg. 41,144, 41,637 (Aug. 17, 2018).

¹¹³ See *Senate Information Blocking Hearings*, *supra* note 81.

¹¹⁴ Cures, *supra* note 5, §§ 4901–4906, 130 Stat. 1157–1183 (codified in scattered sections of 42 U.S.C.).

¹¹⁵ *Id.*

R
R

rially discourage access, exchange, or use of electronic health information.” And it defines information blocking by developers as behavior that “if conducted by a health information technology developer, exchange, or network, such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information[.]”¹¹⁶ Providers will be permitted to attest that they have not blocked information; EHR vendors, however, will have to demonstrate that they have not information blocked in response to standards developed by the Secretary.¹¹⁷ Cures also authorizes fines against EHR developers of up to \$1 million.¹¹⁸

In addition, the HHS Office of the Inspector General (OIG) is using existing regulations to target data blocking by vendors. On May 31, 2017, the OIG and the DOJ’s fraud unit settled for \$155 million a case against eClinicalWorks, an EHR developer, under the False Claims Act. The government alleged in part that the developer’s “software failed to satisfy data portability requirements intended to permit health care providers to transfer patient data from eClinicalWorks’ software to the software of other vendors.”¹¹⁹ eClinicalWorks is one of the top 10 EHR developers in the United States by size.¹²⁰ The next day, OIG issued a report estimating that over \$700 million in Meaningful Use incentives had been paid based on meaningful use stage 1 and 2 attestations that OIG could not verify based on a random sample. Those attestations, including attestations that exchange occurred with unaffiliated organizations.¹²¹

States have concurrent jurisdiction over, and their own interest in, a competitive health care landscape. States are empowered to take action, and one has. Following the publication of ONC’s Information Blocking Report, Connecticut enacted a law that includes specific requirements for easily moving

¹¹⁶ *Id.* § 4004(a)(1)(B) (codified at 42 U.S.C. 300jj–52(a)(1)(B)).

¹¹⁷ *Id.* § 4004(a)(3) (codified at 42 U.S.C. 300jj–52(a)(3)).

¹¹⁸ *Id.* § 4004(b)(2)(A) (codified at 42 U.S.C. 300jj–52(b)(2)).

¹¹⁹ Press Release, U.S. Dep’t of Justice, DOJ Settles False Claims Act with eClinical Works, (May 31, 2017), www.justice.gov/opa/pr/electronic-health-records-vendor-pay-155-million-settle-false-claims-act-allegations.

¹²⁰ *eClinicalWorks Holds Highest Market Share for Ambulatory Cloud-Based EHRs*, BECKER’S HOSP. REV. (Jan. 26, 2016), www.beckershospitalreview.com/healthcare-information-technology/eclinicalworks-holds-highest-market-share-for-ambulatory-cloud-based-ehrs.html.

¹²¹ DANIEL R. LEVINSON, INSPECTOR GEN., DEP’T OF HEALTH & HUMAN SERVICES, MEDICARE PAID HUNDREDS OF MILLIONS IN ELECTRONIC HEALTH RECORD INCENTIVE PAYMENTS THAT DID NOT COMPLY WITH FEDERAL REQUIREMENTS (June 2017), oig.hhs.gov/oas/reports/region5/51400047.pdf. One finding was that 12% of stage 1 Meaningful Users inaccurately attested. Stage 1 included the requirement of at least one instance of exchange. *Id.* at 16.

health information from one provider to another.¹²² According to state Senator Martin Looney, one of the bill's sponsors:

[H]ospital systems in Connecticut have been pressuring independent physician practices to join their network by denying them electronic access to a patient's full medical records unless they join. [Looney] said these health systems, namely Yale New Haven Health and Hartford Health, have used their Epic Systems-made EHRs to create a private health information exchange accessible only to affiliated providers or those providers willing to pay thousands of dollars to connect to the hospitals' IT systems. "Epic has become a monopolistic practice," Looney said. "If you're not part of Epic through the hospitals you're left out and your practice is at a great disadvantage."¹²³

In other words, State Senator Looney was concerned that the "walled gardens" described in ONC's report were simply becoming bigger on the inside, and that dominant hospital systems were intent on creating technology captives among their physicians with admitting privileges and those physicians' patients. Whether the Connecticut law will be successful at breaking down the walls remains to be seen.

IV. NEW POLICIES TO PROMOTE DATA SHARING

There is a strong public policy rationale for more freely flowing information. Freely flowing information between providers will make patients more mobile and promote competition between providers. Further, improved provider data sharing will improve care coordination, which should enhance quality of care and could reduce costs. Greater EHR interoperability will also promote the flow of information and the benefits that accrue from it. Finally, enhanced interoperability should increase competition between EHR vendors.

As indicated above, policymakers have taken some important initial steps, but there are some additional things that can be done to help improve matters.

First, we suggest that the FTC conduct a study of the exchange of health data and whether health information exchange is being impeded because of attempts to avoid competition. We know that less health data are being exchanged than expected or desired, but we need to know more about what is happening, what actions specifically are being taken by organizations that affect data sharing, and how these affect competition. Specific information could be collected such as (but not limited to the following):

¹²² An Act Concerning Hospitals, Insurers & Health Care Consumers, 2015 Conn. Pub. Act 15-146.

¹²³ Alex Ruoff, *In Connecticut, Debate Starts over Information Blocking*, HEALTH IT LAW & INDUSTRY REPORT (BLOOMBERG/BNAL) (Nov. 9, 2015) (on file with authors).

- (1) How many health information exchange transactions occur between unaffiliated EHRs or among providers who are not in the same medical group or corporate family in a wide variety of markets?
- (2) When information sharing occurs, what are the costs and the benefits the EHR vendors or providers experience? What is it that makes it beneficial for the various parties to the exchange? What are the key factors that support exchange?
- (3) When information sharing does not occur, what are the costs and benefits? What is it that does not make it beneficial for parties to the potential exchange? What are the key factors that prevent exchange?
- (4) How frequently is HIPAA used as a justification for not exchanging when, under the HIPAA regulations, exchange would be permitted and no other privacy laws apply?
- (5) What are the costs incurred in engineering connectivity between two different EHR systems for two providers who want to exchange data?
- (6) How frequently are developers of third-party apps authorized to connect to the open-specification API that ONC included in its 2015 regulation and, if the developer has to pay for that privilege, what are the prices the developer pays?
- (7) What are the fees data holders charge for transmitting data? How do those fees correspond to the costs of transmitting data? Does it appear that data holders are setting fees at high levels in order to deter demand for data or to raise the costs of rivals to put them at a competitive disadvantage?
- (8) What action are private payers taking to ensure their enrollees have their data available for all clinicians, particularly across institutions or EHR systems?

Further, in the period since the passage of HITECH, some health care mergers have been defended in part by citing the need for integrated, uniform health IT systems to improve efficiency and quality.¹²⁴ We need to know more

¹²⁴ See Respondent's Answer at 12, Advocate Health Care Network, FTC Docket No. 9369 (Jan. 5, 2016), www.ftc.gov/system/files/documents/cases/advocate_healthcare_respondent_northshore_university_health_systems_answer_to_administrative_complaint_580478.pdf (responding to FTC Admin. Complaint ¶ 48 (Dec. 17, 2015), www.ftc.gov/system/files/documents/cases/151218ahc-pt3cmpt.pdf (provisionally redacted public version)); see also Complaint at 3, 13 & 14–16, Penn State Hershey Med. Sys., FTC Docket No. 9368 (Dec. 7, 2015), www.ftc.gov/system/files/documents/cases/151214hersheyptnacmpt.pdf (provisionally redacted public version); Fed. Trade Comm'n Staff, Submission to the Southwest Virginia Health Authority and Virginia Department of Health Regarding Cooperative Agreement Application of Mountain States Health Alliance and Wellmont Health System 33–36 (Sept. 30, 2016), www.ftc.gov/sys

about the existence and magnitude of such efficiencies, the extent to which they are merger specific, as well as any impacts they have on competition.

If the information to answer these questions is readily publicly available, then the FTC can conduct a study using those sources. If the information is not readily publicly available, the FTC can use its powers in Section 6(b) of the Federal Trade Commission Act¹²⁵ to obtain the relevant information from those possessing it.¹²⁶

Second, while the FTC's role is significant, it is important to remember that only the DOJ has federal enforcement jurisdiction over anticompetitive practices by non-profit corporations,¹²⁷ including the 58 percent of hospitals that are non-profits.¹²⁸ These non-profit hospitals are custodians of significant quantities of clinical digital health information. Therefore, through its long collaboration with FTC,¹²⁹ the DOJ can use the results from any FTC study or FTC enforcement actions to evaluate whether there is information blocking that rises to the level of an actionable enforcement issue for non-profit health care actors.

Third, ONC and CMS can take actions to promote the adoption of the information technology that is used throughout the rest of the economy for internet-enabled transactions. For example, while ONC cannot require the

tem/files/documents/advocacy_documents/submission-ftc-staff-southwest-virginia-health-authority-virginia-department-health-regarding/160930wellmontswstaffcomment.pdf (rebutting claims that adopting unified EHR system is necessary to share patient data to achieve quality improvements); Fed. Trade Comm'n Staff, Supplemental Submission to the Tennessee Department of Health Regarding the Certificate of Public Advantage Application of Mountain States Health Alliance and Wellmont Health System 17-18 (Jan. 5, 2017), www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-supplemental-submission-tennessee-department-health-regarding-certificate-public-advantage/170105mshatennessesuppcmt.pdf.

¹²⁵ 15 U.S.C. § 46.

¹²⁶ Section 6(b) of the FTC Act "empowers the Commission to require the filing of 'annual or special reports or answers in writing to specific questions' for the purpose of obtaining information about 'the organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals' of the entities to whom the inquiry is addressed." Fed. Trade Comm'n, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority* (July 2008), www.ftc.gov/about-ftc/what-we-do/enforcement-authority (quoting 15 U.S.C. § 46).

¹²⁷ The FTC's jurisdiction over non-profits is limited by the definition of corporation in Section 4 of the FTC Act, which includes those entities "organized to carry on business for [their] own profit or that of [their] members." 15 U.S.C. § 44. Thus, while FTC has authority under the Clayton Act to challenge mergers of non-profit corporations, it cannot assert jurisdiction over non-profits in other types of antitrust cases.

¹²⁸ Brooke Murphy, *Fifty Things to Know About the Hospital Industry 2017*, BECKER'S HOSP. REV. (Jan. 25, 2017), www.beckershospitalreview.com/hospital-management-administration/50-things-to-know-about-the-hospital-industry-2017.html.

¹²⁹ Bill Baer, Assistant Att'y Gen., Antitrust Div., U.S. Dept. of Justice, Remarks at The New Health Care Industry Conference, The Role of Antitrust Enforcement in Health Care Markets (Nov. 13, 2015), www.justice.gov/opa/file/794051/download.

adoption of any particular technology, it can continue to champion technologies that facilitate low-cost interoperability, such as open-specification (non-proprietary) Application Programming Interfaces (APIs).¹³⁰ If used, this could drastically reduce the technical friction of secure, auditable information sharing. CMS's role is to financially incentivize use of the technology. The ONC requires of certified EHR systems. Starting in January 2019, CMS will require physician practices (as a condition of payment for services delivered to Medicare beneficiaries) to use the open API.¹³¹ Specifically, the open API will enable, from a technical perspective, authentic and secure apps from unaffiliated businesses to access EHR data for legitimate purposes, as already occurs in finance and retail.¹³² Since adoption of the open API will drastically reduce technical barriers to exchange,¹³³ if information flow is not substantially increased thereafter, persistent low levels of exchange will make a strong case that information hoarding is occurring, impeding competition. Such evidence may warrant investigation by federal or state antitrust authorities.

Fourth, ONC and CMS could more aggressively create financial incentives for providers to engage in exchange by tying provider payments to process and outcome measures that are directly affected by the level of information exchange. ONC has taken an initial step in this direction by funding the National Quality Forum to begin to develop such measures, and the resulting set of measure concepts span both exchange activity (e.g., percentage of available structured elements that were electronically exchanged per patient) and outcomes that are likely to be improved by exchange (e.g., percentage reduction in duplicate labs and imaging over time).¹³⁴ These were only concepts, how-

¹³⁰ Consistent with its mission to facilitate nationwide health information exchange, ONC in 2015 updated its software rule to require that to be certified by ONC, a developer had to include an open-specification, i.e., read-only "Application Programming Interface," which would enable unaffiliated application developers to write apps to extract (read-only) data from one system and transport it elsewhere. 42 C.F.R. § 170.315(g)(7) (2015). Unfortunately, in its most recent proposed rules on expected behavior by hospital and providers to earn incentive payments or to avoid penalties, CMS did not require that hospitals or providers allow this API to be used, whether by individuals to get their own health data (as is required by law, 82 Fed. Reg. 30,610, 30615 (June 30, 2017)), or by allowing an app to work to exchange with an unaffiliated physician for a shared patient, both of which HIPAA has always allowed. See *HIPAA Fact Sheets*, *supra* note 25.

¹³¹ 45 C.F.R. § 170.315(g)(9) (2015) states the API certification rule. CMS delayed required use by Eligible Physicians and by the Eligible Hospitals until 2019, but has finalized this deadline. 2019 Medicare Inpatient Prospective Payment Rule, 83 Fed. Reg. 41,144, 41,637 (Aug. 17, 2018). See also 2018 Medicare Physician Fee Schedule Rule, 82 Fed. Reg. 52,356 (Nov. 13, 2017); Medicare 2018 Inpatient Prospective Payment Rule, 82 Fed. Reg. 37,990 (Aug. 14, 2017).

¹³² ONC API Task Force, *supra* note 69.

¹³³ *Id.*; see also 2015 Edition ONC Certified Electronic Health Information Technology, 80 Fed. Reg. 62,601, 62,675–79 (Oct. 16, 2015).

¹³⁴ NAT'L QUALITY FORUM, A MEASUREMENT FRAMEWORK TO ASSESS NATIONWIDE PROGRESS RELATED TO INTEROPERABLE HEALTH INFORMATION EXCHANGE TO SUPPORT THE NATIONAL QUALITY STRATEGY (Sept. 1 2017), www.qualityforum.org/Publications/2017/09/Interoperability

R

R

ever, and no such measure specifications presently exist. Moreover, it is not clear who will take up the work to develop the measures and shepherd them through the endorsement process so that they can be used in practice. Typically, development of measure specifications is undertaken in response to a robust evidence base by government agencies or private nonprofits, and resulting measures are then endorsed by professional societies and/or consumer groups.¹³⁵ While the evidence base for the benefits of exchange is expanding, it is still fairly limited and, because information exchange cuts across so many contexts and clinical conditions, it does not have an obvious set of stakeholders to take on the development or pursue subsequent endorsement. Of course, the benefits and costs of such enhanced financial incentives should be evaluated carefully before adopting such a policy.

Making funding available to entice measure developers to speed the creation of promising measures may also be worthwhile. In the interim, a practical option, but one with potential unintended consequences, could involve tying stronger financial incentives to existing measures of performance that are likely to reflect high levels of information exchange. For example, there is a measure in the Hospital Consumer Assessment of Healthcare Providers and Systems “Clinician & Group” survey that asks patients about whether their provider had access to all prior information about their care.¹³⁶ Tying CMS provider payment to high performance on this measure, or a close derivative of it that asks about prior information from “external” providers, could be a powerful driver of greater information exchange (as well as ensuring that information is not only exchanged, but is also made easily available to frontline providers at the point of clinical decision making).

While such incentives would serve as a powerful counterbalance to current incentives not to share data, it is important to recognize that this approach could also be gamed or have unintended negative consequences. For example, if only some providers are subject to these payment incentives, it could create a scenario in which the providers that need to engage in exchange to meet the measure are beholden to another set of providers who do not need to meet the measure but care for the same patient population. In this scenario, the latter group, which hold the patient data needed for high measurement achievement would have leverage over the former group. That leverage might even inten-

_2016-2017_Final_Report.aspx (pursuant to contract HHSM-500- 2012-000091, Task Order HHSM-500-T0021).

¹³⁵ FamiliesUSA, *Measuring Healthcare Quality: An Overview of Quality Measures* (May 2014), familiesusa.org/sites/default/files/product_documents/HSI%20Quality%20Measurement_Brief_final_web.pdf.

¹³⁶ Agency for Healthcare Research & Quality, *CAHPS Clinician & Group Survey* (July 1, 2015), www.ahrq.gov/sites/default/files/systwyg/cahps/surveys-guidance/cg/survey3.0/adult-eng-cg30-2351a.pdf.

sify any existing market consolidation pressures (i.e., formally aligning with or acquiring a provider group in order to achieve the measure through exchange).

Fifth, there is a role for payers in promoting information exchange. For example, Intel Corporation in 2013–2015 experimented with creating a narrow network for its employees (in certain locations where it was a dominant employer), where participation in the network required providers to exchange data with each other.¹³⁷ While Intel apparently had good results on quality improvement and cost savings, its approach has not been widely duplicated. It is not clear why private payers generally have not been more aggressive in pursuing such strategies.

There are some counterexamples. Interestingly, Blue Shield of California recently announced that in order to contract with it in-network, providers had to also exchange data through the California state HIE, at no cost to the providers.¹³⁸ Furthermore, for accountable care organizations (ACOs) and other value-based payment models to take root in the private sector, health information must be exchanged. Organizations like the public-private “learning and action network” and commercial payers are working towards wider adoption of alternative payment models, and recognize that data sharing is “foundational for operationalizing” such models.¹³⁹ To date, however, their work is still in an early stage. Finally, although some state Medicaid agencies and commercial payers have used their oversight and market powers to accelerate the rate of health information exchange,¹⁴⁰ this approach is not widespread.¹⁴¹ In spite of these examples, for the most part payers have not taken an active role in promoting information exchange. The role of payers is not well under-

¹³⁷ Prashant Shah, Angela Mitchell & Brian DeVore, Intel Corp., *Advancing Interoperability in Health Care: Employer Led, Standards-Based Collaboration to Advance the Triple Aim* (2015), www.ssiintel.com/content/www/us/en/healthcare-it/solutions/documents/advancing-interoperability-healthcare-paper.html.

¹³⁸ Press Release, Blue Shield of Cal., Blue Shield of California Commits to Work with Providers to Bring Health Care into the Digital Age (Mar. 6, 2018), www.businesswire.com/news/home/20180306006518/en/Blue-Shield-California-Commits-Work-Providers-Bring.

¹³⁹ HEALTH CARE PAYER LEARNING & ACTION NETWORK, ACCELERATING AND ALIGNING POPULATION-BASED PAYMENT MODELS: DATA SHARING (Aug. 8, 2016), hcp-lan.org/groups/pbp/ds-final-whitepaper/.

¹⁴⁰ See Governor of Ohio, Office of Health Transformation, *Ohio Medicaid Reform* (Aug. 2015), healthtransformation.ohio.gov/Portals/0/OhioMedicaidReforms8-11-2015.pdf?ver=2015-08-17-142316-027; Blue Cross Blue Shield of Mich., *2017 PGIP Fact Sheet: Health Information Exchange Initiative*, VALUEPARTNERSHIPS.COM (Mar. 2017), www.valuepartnerships.com/wp-content/uploads/2017/03/2017-HIE-Initiative-Fact-Sheet.pdf. Medicaid is a complex system in its own right, given federal funding and state eligibility rules, and a deeper discussion of Medicaid and information exchange or information blocking is beyond the scope of this article.

¹⁴¹ Dori A. Cross, Sunny C. Lin & Julia Adler-Milstein, *Assessing Payer Perspectives on Health Information Exchange*, 23 J. AM. MED. INFORMATICS ASS'N 297 (2016).

stood, and as indicated above, could be a valuable subject for investigation by an FTC study.

V. CONCLUSION

While there is widespread agreement on the benefits from routine sharing of digital health data, and specific federal goals that seek to achieve it, data sharing is still the exception rather than the rule. As we have indicated, EHR vendors and providers likely find it to their advantage to refuse to share data with rivals. While this is understandable, it can harm competition and consumers.

Furthermore, while these issues are important now, we expect them to only grow in importance. Our world is being transformed to one in which data are central to individuals and businesses. This digital transformation is coming to health care the same way it has come to much of the rest of the economy. In this state of the world, the portability of data, or lack thereof, may become a major driver of competition, costs, and outcomes. We need to better understand the factors driving the current lack of health data exchange and formulate policies that facilitate its use and transmission to benefit society.

ONC's Proposed Rule On Information Blocking: The Potential To Accelerate Innovation In Health Care, HEALTH AFFAIRS BLOG, February 15, 2019. DOI: 10.1377/hblog20190215.3077
Copyright 1995 - 2019 by Project HOPE: The People-to-People Health Foundation, Inc., eISSN 1544-5208.

Lucia C. Savage, JD

FEBRUARY 15, 2019
[10.1377/HBLOG20190215.3077](https://www.hhs.gov/healthaffairs/blog/2019/02/15/10.1377/hblog20190215.3077)

In 2015, when the Office of the National Coordinator for Health IT (ONC) – where I served as chief privacy officer at the time -- started planning what would become the “open specification API” rule of ONC’s [2015 Edition Certification Rule](#), we purposefully grounded that rule, and the corollary CMS rule (now called “[promoting interoperability](#)”), on an individual’s [right](#) to get, use and send their protected health information. We did so because this right cannot lawfully be denied. Unlike information sharing between health care businesses (B2B), which is permitted but not required, disclosure to an individual is *required*. Driven by the vision that this strategy would help APIs take root and flourish in healthcare, we hoped that over time, apps and APIs would be used for exchange of information B2B, and not just in disclosures to consumers (B2C).

Now, with the recent publication of the [Notice of Proposed Rulemaking to Improve the Interoperability of Health Information](#) (NPRM), ONC and Health and Human Services (HHS) have firmly committed themselves to this vision. ONC made specific proposals for how apps and APIs could be used B2B for extraction and transport of data on whole patient populations, not just for an individual’s needs. Bravo, ONC, for this bold proposal. As a proposed rule, however, it remains to be seen how many of these big ideas remain in ONC’s final rule. The public comment period on this rule closes 60 days after the rule officially publishes in the Federal Register, with a comment deadline of approximately April 11. For more detail on the NPRM, visit the fact sheets on ONC’s [website](#).

The NPRM has the potential to advance interoperability in surprising ways, while preserving privacy. The NPRM covers many additional topics including: pediatric EHRs; technical rules for maintenance of certification, attestation and testing and a prohibition on “gag” clauses; a request for information on clinical registries; revisions to the “common clinical data set” that include new categories of data and a new method for updating this minimum data set; and which version of the [Fast Health Information Resource](#) should be required to be used. Such topics are beyond the scope of this post. Below, I will outline a few aspects of the rule, and note a few policy-oriented provisions that bear watching.

Provisions To Watch

For context, this NPRM was released one day before final comments were due on the HHS Office for Civil Rights (OCR) [Request for Information on Modifying HIPAA Rules To Improve Coordinated Care](#). OCR sought input on 54 questions about potential changes to the HIPAA Privacy Rule which might advance care coordination and dovetail to ONC’s proposals. The ONC

NPRM was released simultaneously with a [CMS proposed rule](#) that, if enacted, would make it a condition of participation that “that Medicaid, the Children’s Health Insurance Program, Medicare Advantage plans and Qualified Health Plans in the Federally-facilitated Exchanges *must provide enrollees with immediate electronic access to medical claims* and other health information electronically by 2020.”

Improving care coordination has been a top priority for HHS, as demonstrated by their commitment to empowering patients through the [MyHealthEData](#) campaign, and ensuring that taxpayers get more value from the [\\$37 billion in incentives](#) to use electronic health records. Accordingly, the NPRM focuses on implementing the presumption in [The 21st-Century Cures Act \(Cures\)](#) that there are *very few* circumstances when exchange of electronic health information (EHI) should not occur. It lists seven activities which, when they occur, would not be considered “information blocking” prohibited by Cures: (1) preventing harm; (2) promoting privacy; (3) promoting security; (4) Recovering costs reasonably incurred to make the API technology available; (5) infeasible requests for data; (6) License conditions that the data discloser or API technology supplier imposes on the app developer and which are reasonable and non-discriminatory; and (7) system maintenance.

Among the seven activities listed, preventing harm, promoting privacy, and promoting security are to be expected on this list. One specific element of the promoting privacy exclusions, however is worth noting and watching in the final rule. ONC proposes that it would not be information blocking for an organization to follow, according to the fact sheet, “certain practices not regulated by HIPAA but which implement documented and transparent privacy policies [of the organization]”. However, as ONC itself pointed out in its [2015 Interoperability Roadmap \(page 18\)](#), sometimes it is organizational policies and unduly restrictive or even incorrect interpretations of HIPAA or state privacy law that lead to a lack of interoperable movement of information. Here, despite its 2015 diagnosis, ONC seems to be allowing organizations to continue to comply with internal policies, however well or ill founded. The worry here is that in cases where an organizational policy misapplies legitimate privacy laws as a pretext for business decisions to not share, such conduct would still not be considered information blocking. See, e.g. Savage, L, Adler-Milstein, J., and Gaynor, M, “*Digital Health Data and Information Sharing: a New Frontier for Health*” forthcoming in 82 American Bar Association Antitrust Law Journal p 701, at 706) (March 2019).

Another area that bears watching is ONC’s proposals for recovery of reasonably incurred fees and for license conditions that could be imposed on the apps using the required APIs. The proposed rules in this portion are complex. The way ONC officials described it at HIMSS 2019 this week, some fees could be negotiated by the API technology supplier (aka EHR developer) and the API data discloser (aka the health care provider or plan) but charged to the app developer who is accessing the data held by the data discloser. However, the app developer, will not have been a party to the price negotiations. One can well imagine different ideas of “affordable” and “reasonable” as between a start-up and a multi-site health system or a multi-billion-dollar EHR developer. Yet, to obtain the competitive, innovative health care ecosystem ONC and HHS explicitly desire, prices cannot be so high as to themselves be a barrier (this

concept is discussed at length in Savage, et al., cited above). And, while the Federal Trade Commission has significant authority to address price-setting that may be anti-competitive, the process of doing so takes many years.

Furthermore, as I have [written previously](#), HIPAA does not permit organizations to monetize protected health information. ONC has attempted to address this by articulating when an API technology supplier or data provider may NOT recover fees. But, it remains to be seen whether incumbent health care stakeholders, who have financial incentives to not let their patients get care elsewhere, can develop cost recovery schema that do not monetize PHI impermissibly, and that enhance competition. While ONC has proposed careful detail about what licensing means, (highlighted in this [detailed fact sheet](#)), EHR developer efforts to protect intellectual property via licensing have heretofore [interfered with interoperability](#), as ONC itself acknowledges.

Patients' Perspective

For patients, the NPRM offers two significant improvements. First, while it is clear that reasonable fees that are not anti-competitive *may* be charged to app developers, especially for apps using the NPRMs B2B features, individuals are not to be charged when they use an app to get their own PHI. Second, ONC has added to its certification criteria that certified EHRs must make use of an HL7-approved standard for marking certain data as subject to special handling for privacy reasons. This standard is known as Data Segmentation for Privacy, or "DS4P". With this technology in place, health care providers will be able to more automatically ensure that special data -- such as that from an Opioid Use Disorder program or the reproductive health data of a teenager -- is handled in a manner consistent with the special privacy rules that apply to it. Another instance of special data is the privacy choices offered by an organization to individuals -- that is, granular privacy choices such as "share with my sister but not my ex-husband". DS4P could also be used to document such a choice. An individual's privacy choice, when given a choice, is different from an organizational policy. Individual choices reflect the specific privacy choices one person makes to help them manage their health, and are highly unlikely to be anti-competitive. Organizational policies reflect the organization's desires and business operations. As discussed above, business policies may be based on privacy, but may veer into anticompetitive intent, which should not be allowed.

Bringing an app enabled eco-system to life in health care would change many things. It would advance innovation in: where care is delivered, how care is delivered, how we understand the healthcare needs of individuals, and how we make sure health care professionals have all the information they need when collaborating for care with patients. The HITECH act is just ten years old, and investments in health IT did indeed unleash economic stimulation of new care delivery modes. ONC's information blocking rule has real potential to accelerate that innovation.



February 10, 2019

Roger Severino, JD
 Director,
 HHS Office for Civil Rights
 200 Independence Ave, SW
 Washington DC 20201
 By Electronic Submission

RIN: 0945-AA00

Dear Director Severino:

Omada Health, Inc., respectfully submits the below comments in response to the U. S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) Request for Information (RFI) dated December 14, 2018 (HHS-OCR-0945-AA00).

Omada Health, Inc. (Omada) is one of the nation's largest digital health care service providers. Founded in 2011, Omada provides health care services (as defined in 45 CFR 160.103) by connecting professional coaches to individuals through a secure communications platform. That platform allows our professional coaches to use clinically validated intensive behavioral counseling techniques and related services for clinically validated activities such as:

- Diabetes Prevention Program (DPP)¹,
- Diabetes self-management education,
- Coaching for hypertension management, and
- Coaching for medication adherence.

Within the next 12 months, we will also expand our services to deliver care for individuals dealing with anxiety and depression. We are the largest DPP in the country to have achieved CDC full recognition, and have served over 200,000 people from age 18 beyond age 65 in our eight-year history.

¹ The criteria for what constitutes a CDC Fully Recognized DPP and which programs are fully recognized can be found at: https://nccd.cdc.gov/DDT_DPRP/Registry.aspx

As a health care services provider as defined by 45 CFR 160.103, we have since our founding operated as, and considered ourselves to be, a covered entity under the Health Insurance Portability and Accountability Act (HIPAA). In 2016, the Centers for Medicare and Medicaid Services (CMS) reiterated what we had always known: that entities that provide health care services using secure 21st Century digital communications services are still providing health care services within the meaning of HIPAA. 81 Fed. Reg. 80170, 80472 (Nov 16, 2016).

As a provider and covered entity, albeit one that provides services using the latest digital health, sensors, and data science for population health analytics and to personalize how our we deliver our health care services, we are pleased to provide what we hope is helpful information set forth below.

I. INTRODUCTION

At Omada, we have built an outcomes-based reimbursement model utilizing HIPAA rules as a foundation. The statute enables sharing of PHI for program evaluation, care coordination and quality improvement. For customers that contract on outcomes-based pricing, we provide the minimum necessary data to validate clinical success and enable our claims-based billing. We also believe that the way HIPAA permits but does not require sharing of PHI with other covered entities appropriately balances the dignity of individuals with standard rules that keep the health system running.

When OCR finalized the Privacy Rule in 2002, claims data was quite structured, but clinical data was not. Since then, Congress enacted the Health Information Technology for Clinical Health Act (HITECH) and the Meaningful Use (now Medicare Incentive Payment System, or MIPS) program, which vastly changed the quantity of structured clinical data. Also, since 2009, advances in computing and smart phone/mobile technology have resulted in new sources of digital clinical data, while significantly lowering barriers to collecting that data.

While many features of the Privacy Rule are resilient and flexible because they specify required outcomes, other features could be updated to help individuals, covered entities, and health care innovators better understand and comply with the important dignitary rights embodied in the Privacy Rule.

First, OCR should consider updating in a rule, or publishing sub-regulatory guidance, that accounts for the fact that PHI now consists of health facts about an individual (like blood sugar test result ratio), as well as metadata and other data structural components that have nothing to do with health facts. Separating these concepts out in regulation will, as we describe in section II.A., help OCR and HHS improve disclosure back to individuals and improve subsequent sub-regulatory guidance as well as HHS ability to promulgate future revisions to existing rules.

Second, any changes that OCR proposes or enacts should advance towards convergence with other privacy standards, including those from FTC, HHS OIG, or FDA SaMD.² By bringing standards from various agencies in line, the federal government will create a more easily understood set of standards. This will benefit consumers and accelerate innovation³.

Within the framing that the two bookended recommendations above provide, we offer the following substantive comments.

II. SUBSTANTIVE COMMENTS

A. HIPAA's Definition of PHI Should Match and Keep Pace With Regulatory Standards for How Health Information Is Structured.

Congress enacted HIPAA in 1996 to usher in an era of electronic billing by physicians and hospitals of federal programs. In 1996, and even in 2000 and 2002 when HIPAA Privacy regulations were first finalized, digital health information was in its infancy. The only digital information available were sets of data that contained demographic information, CPT and ICD Codes. These codes provided an important cumulative picture of the care for which a provider sought payment. With the advent of digital claims data and the HIPAA Transactional Code Sets, health care stakeholders were, for the first time, able to effectively find patterns in the data that related to the process of care. With the advent of the Health Care Effectiveness Data Information Set (HEDIS) came rudimentary measures of the actual care that was billed. We still lacked the ability to measure how effective the care was, relative value of different types of care on outcomes, or to easily share and use clinical records across a team of healthcare professionals who might even be in physically disconnected locations.

The 2000 and 2002 Privacy and Security regulations clearly prescribed how physicians, hospitals, nurses and other professionals could share data across institutions in ways that the vast majority of individuals expected would occur,⁴ including treatment and care coordination. See the specific rules at 45 CFR 164.506(c)(1). These rules are data format neutral. They apply to PHI whether on paper, in a fax, or electronic. As to electronic health information, they apply to all types, from CPT codes to the type of health information that Omada collects. These rules also presciently anticipated a value-based healthcare system, providing leeway for providers to share information to payers (and vice versa) for a recipient's ability to understand, measure, evaluate and improve the quality of health care delivery. 45 CFR 164.506(c)(4). Through these rules, the U.S. system of choice and private insurance ran; individuals did not have to stop their

²The Food & Drug Administration "Software Precertification Program: A Working Model" v. 1.0 published January, 2019, includes evaluation of both an organization's cybersecurity processes and culture and its data integrity [acdd cites]. This is appropriate given the technical convergence of the Internet of Things in Healthcare. See also [FTC report on Healthcare IOT]

³ Cite Non -Covered Entity Report.

⁴ See Letter of Privacy Tiger Team of the federal Health Information Technology Policy Committee to the National Coordinator for Health IT dated September 1, 2010, page 4, found at: https://www.healthit.gov/sites/default/files/hitpc_transmittal_p_s_tt_9_1_10.pdf.

busy lives to give permission to a physician to send a bill to the individual's insurance company. In 2000 and 2002, however, clinical data was almost entirely unstructured.⁵

At present, clinical data is highly structured, and not just in certified electronic health records regulated by HHS. Today, structured, clinically informative health data exists widely throughout the healthcare system, and generally consists of health facts about each individual (for example a name, a complete date, a clinical marker such as an CPT code or a code for a prescription). Today's clinical data also consists of many other data elements that make the clinical markers useful, but are not themselves clinically indicative. From our perspective, neutral to any particular platform or digital health product, we see several functions occurring in digital data, as follows:

1. **Core Health Facts:** digital information that illustrates or describes core health conditions for an individual from lab test results to diagnoses to physician notes or patient generated health data.
2. **Peripheral/Non-Core Health Facts:** health care providers, and especially digital providers collect a lot of data that, while it is about the individual, and is collected by a health care provider, is not core to the patient's health. For example, Omada collects individuals exercise information when the individual authorizes it. This helps engagement and individual accountability, but a step count alone does not tell our CDE coaches how well managed a diabetic's blood glucose is.
3. **Operational Facts:** digital providers generate a variety of operational facts that are useful for the operations and efficiency of the provider, but provide little value for the patient. As an example, if a patient loses access to a provider's portal and needs to perform a password reset, this may create operational facts. These facts are tied to the patient but offer no value to the patient from a health care perspective. Knowing if operational facts were "protected health information" and part of a 'designated record set' would help entities that generate these operational facts know what was legally required.
4. **Metadata:** digital providers and traditional providers who use certified electronic health records systems generate a large volume of metadata (data about data) during the natural course of providing care. As an example, an audit log may contain metadata including a patient's IP address, unique identifiers, specific features the patient accessed (how the individual used the digital tool), time and date stamps, and error codes. This data is often unstructured and used to operate the digital platform, but not for patient care. These data are quite useful for maintaining data integrity and for leaving a trail that can be followed should the Core Health Facts be inappropriately accessed or disclosed. But these data are not directly related to an individual's health the way a weight, diagnostic code, or lab value is.
5. **Metadata tags,** which may help an organization sort, compile and analyze data and is connected to health facts, but is not itself a health fact or even about an individual. Tagging like this can help a data holder know what is permitted or not, such as the "data

⁵ See RS Evans, *Electronic Health Records: Then, Now, and in the Future*, Yearbook Med. Inform., 2016; (Suppl 1): S48–S61. Published online 2016 May 20. doi: 10.15265/IYS-2016-s006.

segmentation for privacy” or DS4P tag described in 45 CFR 170.315(b)(7) and (b)(8). Other beneficial uses of metadata tags include:

- Determining the provenance of data to trace it back for data integrity, fraud investigations, etc. For example, it is through the metadata that forensic analysis can more specifically pinpoint who or when may health facts have been fraudulently changed.
- Enabling the development of a growing library of consensus-bundles of data, like the result of one lab test, that enable, in turn, more and more data to be made available to individuals through apps of their choosing when those apps use the Fast Health Interoperability Resource, or FHIR.
- Recognizing an authentic electronic credential of a user seeking their own data, so that they don’t have to stop and sign a piece of paper to get their own PHI.

In 2000, OCR divided mostly unstructured data in the healthcare system into Protected Health Information, Summary Health Information, and Personally Identifiable Information. OCR then applied certain privacy and security processes specified in the relevant regulations to each of these broad buckets.

In 2019, we believe that to further advance crucial efforts to expand care coordination and allow health care to be effectively supplied through advanced digital tools and data science, OCR should consider revising the definition of PHI so that it accounts for the types of structured data in a more specific way than the 2000 broad categories did. Better distinction will support widespread interoperable exchange of standardized, structured, machine-readable health facts for care, personal care management, research and science, and population health.

We also believe that modernized definitions would improve organizations’ ability to provide individuals with access to their own data, and to provide appropriate accountings for disclosure of health facts subject to the Privacy Rule, as we discuss in greater detail below.

We recognize that revising the definition of PHI itself will require input from potentially thousands of interested parties and will require thoughtfulness, foresight, and care. Should OCR and HHS want to elicit more information on this topic, it might consider public listening sessions, so that all stakeholders can provide input in a way that more organically reflects the totality of input.

B. An Individual’s Right to Access Their Own Health Facts (Questions 1-6)

At Omada, we succeed only when we engage our individual participants in our program. When individuals engage, they achieve the health outcomes for which Omada is paid. Therefore, unlike the much-decried fee-for-service health care system, it is in Omada’s interest to robustly and consistently engage our individuals. We do that by continuously sharing data back to them in real-time about their successes, or about their particular needs for coaching on issues that are unique and specific to them.

It all starts with our digital scale, which is shipped to new participants already configured for their secure online account with us. The scale tells us instantly what the individual's weight is that day, but how they use that scale tells us instantly how the individual is using our program. And, for the participant, we curate and feed back to them in real-time what is happening to their weight as they participate in the program. Below is a screenshot of what one of our participants sees on their Omada app (this is from a real participant, used with their permission and de-identified to show you).



In response to Question 1, we have designed our program to feed some Core and Peripheral Health Facts back to individuals in real time. For health facts that an individual can obtain through our program or our app directly, there is no time delay.

For other health information that an individual wants but which is not available through our interface, our process is simple and rarely takes us more than two weeks to complete. Occasionally, however, we do use the full 30 days allotted by regulation. As a health care service provider with a predominantly digital infrastructure, we have very little paper and never require an individual to fill out a specific piece of paper in a specific way to get their own health facts. Nor do we ever require an individual to visit our office to request their health information. Times listed below are estimated averages, and individual requests may take more or less time.

In order:

1. The participant contacts us requesting health facts through our call center, through an email to our call center, or by messaging their coach who in turns forwards to our support staff. All three methods are handled by our call center support staff.
2. Within 2 business days, the support staff confirms the individual's identity with an outbound phone call. Our support staff also confirms the medium the individual wants, among the choices of PDF, paper, or an Excel file.
3. With the individual's preferences in mind, our support staff requests our data analytics team to extract, quality check and prepare the data. This process takes 3-8 business days, depending on load.
4. Typically within one more day, our support team then transmits it in an appropriate manner given the medium and where the individual requested we send the data.

5. If the request comes in from someone other than the individual, such as a physician's office or an attorney, and is presented to us on a HIPAA Authorization developed by the requestor, we confirm with the individual that they agree with the request, and proceed as above.

We recognize, however, that what individuals experience at Omada is the rare exception, not the norm. We believe that more health care stakeholders—even traditional ones like hospitals and physician practices-- could use digital technology and authentic digital identification methods more consistently. This would no doubt speed up and otherwise improve the experience for individuals. Modern methods that OCR and HHS might consider requiring through additional regulations include:

- a. Requiring that covered entities that use certified EHRs (all of which now must include a patient portal) allow individuals to request their Core Health Facts using the portal's secure messaging system, for which the individual has already been issued identity credentials.
- b. Through ONC's certification rule, requiring EHR developers to implement standard structured on-line forms, such as those developed by the American Health Information Management Association (AHIMA), as an EHR portal feature. This would enable individuals to more easily request both standard data sets, like a CCDA or an allergy list, and comprehensive data sets, like the records of a recent surgery, or radiology records.
- c. Requiring that when a covered entity that does not use an EHR portal to allow individuals to request their own health facts, that covered entity must make its "paper form" for available for e-signature and submission through the portal, subject to identity proofing consistent with standards published by the National Institute for Standards and Technology (NIST), instead of making the individuals interact with a remote document processing location that may only accept faxes.
- d. Financially penalize any covered entity that repeatedly fails to make health facts promptly available to individuals—OCR should not allow repeat offenders on this issue.
- e. Strengthen and clarify the rule that state laws that make it harder for individuals to get their health facts are preempted by HIPAA.

As you can see from our practices, we are strong believers in an individual's right to obtain and use their own PHI. In 2018, we amended our [program terms](#) to confirm that every Omada participant owns the information they supply to us or that we collect about them with their permission.

Nevertheless, as we discussed above, we also think that should OCR update the definition of PHI to better account in the regulatory requirements for the actual data structures within digital health information today, to make it easier for organizations to ensure that individuals get their health information in a useful and accessible manner.

For example, if there are firm, clear regulatory distinctions between a Core Health Fact and a piece of Metadata, covered entities will be able to help individuals get more of the data to which individuals are entitled. An individual who wants lab values from a recent test will be able to choose the core health facts of lab values, but audit logs might not be necessary. More detailed definitions of the types of data also have the ability to improve efficiency by ensuring that resources are not wasted disclosing data that the individual actually does not want.

C. Sharing Data Between Covered Entities for Care Coordination (Questions 7-21)

As set forth above, Omada in many ways has built its business model--proving value and being paid for it--on the *existing* rules that permit but do not require a covered entity to share health facts with another covered entity. We have served over 200,000 individuals under this model. We have reported millions of health facts, such as the attainment of weight milestones or lesson completions, to payers and other providers who are covered entities. These covered entities in turn use this PHI for those organizations' care coordination, quality measurement or other legitimate health care operations. In our experience, the current rules do not impede care coordination.

As a health care provider that uses a sophisticated and modern digital platform to deliver our program, privacy, trust and security are fundamental. Without them, individuals will not trust us and will not engage with our program. Without privacy and security, employers and health plans will not pay for our health care services. Our participants and their payers trust us to share data only in the circumstances where they expect it and in compliance with applicable laws. Therefore, we think that the current rules are appropriate and should be maintained.

Switching it to disclosure-on-demand would undermine the trust inherent between a provider and an individual.

Having permission, however, does not mean the party disclosing should make it unreasonably difficult, slow, or expensive for another provider to get information they need for care of the same individual. In fact, we eagerly await open-specification Application Programming Interfaces to spread across the health care system so that we can interoperate with our participants' physicians as easily as we automatically collect their step data from trackers when they authorize us to do so. We use secure APIs daily both with customers who are covered entities and for internal processing of our data system, which is 100% cloud-based. We have plans in the near future to fully connect to health systems and their electronic health records so that our participants' providers can have easy access to program results. We do this in the interest of also accessing other health facts which would improve the effectiveness of our programs, like active prescriptions and lab results. To date, we have not done that due to the prohibitive cost of proving ourselves legitimate and obtaining permission to operate within some EHR vendor's ecosystems. We very much look forward to the day when API specifications are open for our developers to take advantage of. Therefore, we look forward to further opportunities to comment on this when we have had a chance to fully review ONC's forthcoming Notice of Proposed Rulemaking On Information Blocking.

We also think that were OCR to revise the definition of PHI to distinguish between Core Health Facts and Metadata or other elements of data as discussed above, OCR would be better able to describe what constitutes prompt, useful, and appropriate sharing using APIs and APPs between covered entities and when barriers to that constitute “information blocking.”

Finally, OCR should accelerate and publish more interpretive guidance to improve the speed and efficiency of permitted (but not required) data sharing as follows:

1. OCR could develop, and then require, covered entities to use a standard form to request disclosure from each other. Once developed, a standard form could be made electronic, be e-signed, and built into electronic workflows. Such a standard form would, by necessity, have to rely on nationwide identity proofing standards ensure that use of a nationwide federally-developed form was not undermined by the idiosyncrasies of state signature laws, and would have to ensure that the party disclosing health information could rely on the HIPAA *bona fides* of the requester.
2. As discussed above, we use the existing rule at 45 CFR 16.506(c) as a fundamental part of our business model. However, we know that many healthcare technology companies fear expensive investigations and breach reporting if they in good faith try to share health facts with another covered entity for care coordination. Accordingly, OCR should consider eliciting more facts on the scope of this problem, potentially through public listening sessions. Based on the information elicited, if appropriate, OCR could consider adding to 164.506(c) or the Security Rule (as appropriate) a provision that a good faith attempt to share for care coordination, appropriately and securely transmitted but mis-delivered through no fault of the actual disclosing covered entity, is not a reportable breach by the covered entity (even if it remains a security incident that requires post-mortem analysis and remediation).

Because we think it is right to continue the current construct where sharing for care coordination permitted but not required, we do not think that sharing for care coordination should be a condition of participation for Medicare or Medicaid.

Omada is not submitting comments on questions 22-26.

D. Accounting for Disclosure (Questions 27- -41)

We applaud OCR for making another attempt to define and refine what is required to provide an Accounting of Disclosures to an individual. We note at the outset that Omada does not presently use a certified EHR. Nevertheless, as a health care provider, we do get asked for accountings and have had three such requests since January 2017.

For each response, we validate the individual's identity and that they were a participant in our program, research the types of disclosures we have made and whether they are required to be reported, and respond back to the individual accordingly. While this work takes only 2-5 hours per person, we do use the entire 30 days allowed by regulation.

That said, reporting individual outcomes to payers is a fundamental aspect of our business model, and we report frequently and in detail to relevant and appropriate payers, typically on a monthly basis for their population covered by Omada. Having served over 200,000 people to date, with hundreds of covered entity customers, we cannot estimate that number of disclosures. It is because of this outcomes-based model that we take the full 30 days to confirm that a person is our participant and how and to whom we have reported PHI before answering a request.

We do not allow our business associates to respond to request for accounting for us, and all disclosures of PHI are made based on decisions by Omada alone.

As Omada does not have an electronic health records system, we will not be responding to questions 35-41 directly. However, given our own data systems, and our recommendations in section II.A, above, we wanted to briefly comment on how better distinctions among the types of data would enable OCR to develop a more workable Accounting of Disclosures rule that is consistent with the individual's right to know AND with how modern data systems function.

The Accounting of Disclosures rule enables individuals to track who has seen or accessed or received their PHI so they can police the integrity, confidentiality and security of their very identity. Better separating Core Health facts from Metadata or audit logs will help OCR develop an Accounting of Disclosure rule for EHRS that does not result in the individual receiving reams of paper with one line of audit log and no obvious health facts. For example, clearly delineating among the different kinds of structured data will help OCR more easily develop a workable standard built around misuse or disclosure of core health facts, not audit logs or activity to correct bugs in Metadata Tags.

Privacy advocates that we are, we also believe that the identity of a covered entity's workforce members who have accessed, used or receive PHI should be disclosed only by court order, which is perfectly sufficient if criminal charges are pending or if a civil lawsuit about a breach of privacy is pending.

E. As HIPAA Evolves It Must Move Towards or Converge On Other Digital Information Privacy Standards

Since 2011, Omada has worked to establish personalized health care services using the latest digital tools. We connect our human coaches to individuals via secure messaging backed by data-science and population-wide analytics. Infrastructure like this is the next evolution of health care. One of the biggest themes throughout this eight year period is that more and more of the agencies that oversee or set standards for the health care system are becoming familiar with how the advent of 21st Century digital technology changes, and does not change, health care. We also observe that more and more of these agencies are interested in issues parallel to those of traditional concern to OCR, including:

| Agency | Interests |
|---|--|
| Food & Drug Administration | <ul style="list-style-type: none"> ○ Cybersecurity of devices ○ Privacy of data within Software as a Medical Device ○ Data integrity of software development (manufacturing processes) |
| HHS Office of the Inspector General | <ul style="list-style-type: none"> ○ Digital record keeping and data integrity ○ Interoperability of data among health care stakeholders and individuals operating according to regulatory standards |
| Center for Medicare & Medicaid Services | <ul style="list-style-type: none"> ○ Cybersecurity collaboration across the health care sector ○ Financially rewarding provider for patient engagement through access to the patient's own PHI |
| Federal Trade Commission | <ul style="list-style-type: none"> ○ Privacy of health information collected outside HIPAA ○ Fair information security practices, even of HIPAA covered entities, as in LabMD vs. FTC |
| National Institute of Standards & Technology (NIST) | <ul style="list-style-type: none"> ○ Privacy of health information technology ○ Security of health information technology |
| Federal Communications Commission | <ul style="list-style-type: none"> ○ Privacy of health data transmitted via broadband license holders, whether within HIPAA or not. |

Yet, to the outside observer, the rules and requirements remain as divergent as ever.

We are reiterating in this RFI comments that we made to FDA, as follows: In order for the U. S. health care system and the individuals, providers, and payers that constitute it to truly realize the benefits of digital technology, data science, and the power of big data, relevant agencies (and the above is just a small list) must redouble their efforts to coordinate and reach convergence on appropriate standards and expected business practices. Doing so sooner rather than later will:

1. Build trust by ensuring that consumer's information about their health is adequately, or even identically, private and secure, wherever it is collected and used.

2. Improve interoperability and appropriate information sharing for care coordination, population health, or scientific discoveries.
3. Improve efficiency by reducing wastefully overlapping compliance programs that are philosophically redundant but diverse in their details.

III. Conclusion

Omada has built its business as the nation's largest CDC-recognized provider of DPP health care services using the current HIPAA data sharing rules as a foundational element of our business model. We do not see a need to change that particular aspect of HIPAA.

We do, however, recognize that across the health care information spectrum, from FDA devices to HIPAA covered entities, to direct-to-consumer services and apps, the complex regulatory landscape is hindering innovation and eroding trust. It also is likely putting a chill on whatever data sharing for care coordination HIPAA allows, as data holders hesitate to share for fear of violating some other law that they have conflated with HIPAA.

To support continued innovation in health care delivery and strengthen consumer trust in an age where almost all data about a person can be directly or implicitly connected to health, we urge OCR to work with all stakeholders and agencies to ensure that any changes to the Privacy, Security or Breach Notification Rules move the regulatory environment closer to convergence, not farther away from it.

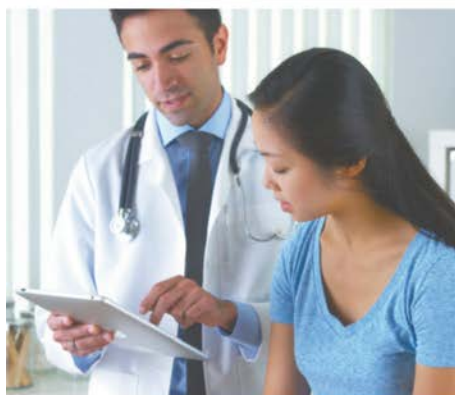
Respectfully submitted,



Sean Duffy, CEO



Lucia C. Savage
Chief Privacy & Regulatory Officer



**Advancing Interoperability,
Information Sharing,
and Data Access:
*Improving Health and
Healthcare for Americans***

February 2019



STAFF**Tina Olson Grande**

*Senior Vice President, Policy
Healthcare Leadership Council*

Janet Marchibroda

*Fellow and Lead, Health Innovation
Bipartisan Policy Center*

Devon Adams

*Policy Manager
Healthcare Leadership Council*

G. William Hoagland

*Senior Vice President
Bipartisan Policy Center*

CONSULTANTS**Julia Adler-Milstein, PhD**

University of California, San Francisco

Mark Segal, PhD

Digital Health Policy Advisors

ACKNOWLEDGMENTS

HLC and BPC acknowledge the more than 100 individuals from a number of organizations who lent their expertise and experiences to the development of this report. The list of organizations can be found in the Acknowledgements section in the back of the report. HLC and BPC would also like to thank Joann Donnellan, Kelly Fernandez, Michael Freeman, Anjali Garg, Ann Gordon, and Anna Vantsevich for their work on this report.

DISCLAIMER

The findings and recommendations expressed herein do not necessarily represent the views or opinions of the Bipartisan Policy Center's founders or its board of directors.

| | |
|----|--|
| 4 | Letter from Bipartisan Policy Center Healthcare Leaders |
| 5 | Letter from the Healthcare Leadership Council |
| 6 | Executive Summary |
| 9 | Introduction |
| 10 | Shared Vision for an Interoperable Healthcare System |
| 11 | Progress on Interoperability |
| 14 | Case for Change |
| 16 | Priority Areas |
| 18 | Measuring Interoperability Progress |
| 20 | Model for Accelerating Interoperability |
| 21 | Recommendations |
| 26 | Conclusion |
| 27 | Acknowledgements |
| 28 | Endnotes |

Letter from Bipartisan Policy Center Healthcare Leaders

Paper-based medical records are mostly a thing of the past, thanks in large measure to the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act and the hard work of many individuals and organizations both within the government and the private sector. Today nearly 90 percent of physicians and hospitals in the U.S. use electronic health records.

This is significant and noteworthy progress worth applauding, but we cannot stop there. In order to leverage the power of EHRs to improve care, we must advance interoperability—enabling health information technology systems used across the continuum of care to connect with one another—to improve information sharing among the many professionals and organizations that provide care to a single patient and increase access to data for both providers and for patients themselves.

This report represents the collective insights of more than 100 leaders in health care regarding these challenges. Together they developed both a shared vision of an interoperable health care system and recommendations on priorities, private sector actions, policies, and measures of interoperability progress.

Supporting better care—higher quality, safer, more cost-effective, patient-centered care—and better health outcomes requires that we diligently pursue the vision of interoperability to make it a reality. It is a complex pursuit. This report recommends prioritizing two key areas: 1) giving providers easier access to clinical information at the point of care, and 2) giving patients easier access to their own health information. Improvements in both these priority areas will result in better care and better health outcomes.

As the science of medicine continues to advance and new delivery system and payment models take hold, the tools that support caregiving must keep pace. The recommendations in this report are designed to bring better data to the bedside, the exam room, and to patients. They lay the foundation for how we improve the health of populations and advance medical breakthroughs that provide new therapies for patients in need. Data is knowledge, and knowledge is power. Let's harness that power to provide all patients with better care, better information, and, ultimately, better health.



Senator Tom Daschle
Former Senate Majority Leader
BPC Co-Founder



Senator Bill Frist, M.D.
Former Senate Majority Leader
BPC Senior Fellow

Letter from the Healthcare Leadership Council

It is difficult to comprehend the sheer magnitude of data that exists in various repositories throughout our healthcare system. Every day physicians' offices, hospitals, clinics, laboratories, pharmacies, health plans, and home care providers are generating information about patients and the care they receive, and patients themselves are increasingly generating and transmitting health data through wearable devices. Some have projected that 30 percent of all data worldwide is health-related.

If that data can be more effectively shared and made accessible through interoperable systems, we can accelerate progress toward solving the critical and complex challenges facing American healthcare. Health outcomes can be significantly improved. The cost of healthcare delivery can be reduced. The patient experience can be greatly enhanced. Data interoperability also opens the door to new advances in biomedical and technological innovations, elevating population health. And with easier access to data, patients can better engage in their healthcare.

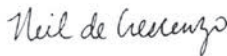
This future is within reach. Achieving it has long been a priority of the Healthcare Leadership Council, an alliance of chief executives from all sectors of American healthcare. We have been pleased to work with the Bipartisan Policy Center in developing a consensus understanding of the progress that has been made toward nationwide health data interoperability and improved information sharing, and overcoming the barriers that remain to attain that goal.

Healthcare leaders are unequivocally committed to removing all obstacles to the essential flow of health information while, at the same time, ensuring data security and patients' right to privacy. With our partners at BPC—and with research support from the University of California, San Francisco—we have crafted a report that not only describes the dynamic future that will take shape when electronic health systems can "talk" to each other, but outlines the private sector actions and public policies necessary to get there.

Today, consumers can change cell phone carriers without having to get a new mobile number. We can check our account balances no matter which bank's ATM we're using. It's time to bring that same 21st century interoperability to healthcare. The benefits to doing so extend well beyond simply convenience and will include better care, longer and healthier lives, and a more sustainable and innovative healthcare system.



Mary R. Grealy
President
Healthcare Leadership Council



Neil de Crescenzo
President and CEO
Change Healthcare, and Chairman,
Healthcare Leadership Council

Executive Summary

Information about an individual's health and healthcare is needed to support coordinated, safe, high-quality, cost-effective, patient-centered care. Much of this information resides in the multiple settings where patients receive care and services, including physician offices, clinics, hospitals and health systems, laboratories, pharmacies, radiology centers, health plans, and even with patients themselves. Interoperability of health information technology (IT) systems helps bring this information to the point of care to support clinical decision-making. It also supports individuals as they navigate their health and healthcare.

The vast majority of clinicians and hospitals have adopted electronic health records (EHRs).^{1,2} The next step is to accelerate interoperability of EHRs and other health IT systems to bring information to clinicians and patients seamlessly.

Progress is being made. The percentage of U.S. non-federal acute care hospitals that electronically find patient health information, and send, receive, and integrate patient summary of care records from sources outside their health systems, has nearly doubled in the last four years, from 23 percent in 2014 to 41 percent in 2017.³ Ninety percent of hospitals and 48 percent of office-based physicians are electronically sending or receiving (or exchanging) patient health information with health care providers outside their organizations.^{4,5} Individuals are increasingly able to access their health information electronically.⁶ But more work is needed.

The federal government has taken many actions to accelerate interoperability, including implementation of the bipartisan 21st Century Cures Act, which was signed into law in December 2016. On February, 11, 2019, the Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC) proposed new rules to support the access, exchange, and use of electronic health information. The private sector has also taken several actions.

The chief executives of organizations represented by the Healthcare Leadership Council (HLC) and the Bipartisan Policy Center came together in 2018 to identify ways to further advance the interoperability of systems and electronic information sharing to support better health outcomes and higher-quality, safer, more cost-effective, and patient-centered care for individuals and populations in the United States. HLC and BPC drew upon the experiences and expertise of more than 100 individuals representing every sector of health care, including clinicians, hospitals and health systems, long-term and post-acute care (LTPAC) providers, health plans, life sciences organizations, EHR and other technology developers, data analytics companies, and patients.

Supporting better health outcomes for individuals and populations requires an interoperable healthcare system in which the patient is at the center of care and the right data are available to the right person at the right time. Access to high-quality, accurate, and actionable data is seamless and integrated within clinical workflows, providing value and convenience, as well as reducing healthcare costs. There is trust in the system; privacy is protected, and information is kept secure.

Action to improve interoperability should initially focus on two priority areas: (1) bringing information to the point of care to support care delivery and (2) meeting the information needs of individuals to support their health and healthcare.

Advancing interoperability will require leadership and action in four key areas, outlined below.

1. STRENGTHEN THE BUSINESS CASE

1.1. Align Incentives Among Payers and Providers

Payers should collaborate with providers to gain agreement on and drive adoption of baseline expectations for interoperability and information sharing through payment incentives that focus on outcomes versus volume, contracts, and other mechanisms.

1.2. Align Incentives of Providers and Their Technology Partners

Providers, including clinicians, hospitals, health systems, specialty societies, and group purchasers, should collaborate with EHR and other clinical software developers to gain agreement on and drive adoption of baseline expectations for interoperability for products through incorporation into contract language. Existing requirements, such as those included in the ONC Health IT Certification Program, should be leveraged. Clinical software and other technology developers and vendors should collaborate with their customers to integrate expectations for interoperability within their products.

1.3. Engage Individuals

Providers, payers, and technology developers should engage individuals to identify and prioritize information access expectations.

2. IMPROVE TECHNICAL INFRASTRUCTURE

2.1. Adopt Common Baseline Standards to Improve Patient Matching

To improve patient matching, providers, software developers, payers, and other health care organizations should collaborate on the identification and collection of a common set of data elements using federally adopted standards.

Providers, software developers, payers, and organizations representing individuals, should collaborate on efforts to explore, pilot, and evaluate the feasibility of widespread adoption of patient-centered approaches to identification.

2.2. Prioritize Interoperability and Standards Conformance in ONC Health IT Certification

ONC should prioritize interoperability and require real-world testing to assess conformance with interoperability standards in future editions of the ONC Health IT Certification Program.

2.3. Pursue Rapid Adoption of HL7 FHIR®-Based APIs to Accelerate Information Sharing

Providers, EHR and other software developers, payers, and other health care organizations should expand upon existing interoperability efforts by pursuing rapid adoption and implementation of HL7 Fast Healthcare Interoperability Resources (FHIR®)-based or other open standards-based application programming interfaces (APIs), to accelerate interoperability, data access, and information sharing.

3. IMPROVE POLICIES AND REGULATIONS

3.1. Implement a Common Notice of Information Access for Patients

Healthcare organizations should collaborate with organizations representing individuals as well as with the federal government, to reach agreement on a standard "Notice of Information Access Practices" and voluntarily make such notice available to patients to reduce confusion and make it easier for individuals to access their health information.

3.2. Align Privacy Laws with HIPAA

States should consider harmonizing privacy laws to align with the Health Insurance Portability and Accountability Act (HIPAA).

The Department of Health and Human Services (HHS) should align consent policies for substance use disorder treatment under 42 CFR Part 2—Confidentiality of Substance Use Disorder Patient Records—with HIPAA.

4. GOVERNANCE AND LEADERSHIP

4.1. Collaborate on Measurement and Improvement

Public- and private-sector leaders should collaborate on the identification and annual reporting of key measures that assess national progress on interoperability and information sharing to support bringing information to the point of care and providing individuals access to their own health information. They should convene efforts to define and launch the execution of private sector actions that will accelerate progress on measures.

Introduction

Interoperability of systems, information sharing, and data access play a critical role in improving health outcomes, lowering healthcare costs, and improving the patient experience of care.

Much of the information about an individual's health and healthcare reside in the many settings where care and services are delivered. This includes physician offices, clinics, hospitals and health systems, laboratories, pharmacies, radiology centers, health plans, and even with patients themselves. Mobilizing such information not only supports coordinated, safe, and high-quality care, it also supports delivery system and payment reforms, transparency efforts, advances in research and biomedical innovation, public health priorities, and the ability of individuals to manage their health and healthcare.

As a result of the federal government's investment of nearly \$40 billion in health information technology (IT) through implementation of the Health Information Technology Economic and Clinical Health (HITECH) Act, the vast majority of clinicians and hospitals have adopted electronic health records (EHRs).^{7,8} Efforts are now underway to improve interoperability of these systems to support improvements in health and healthcare and significant progress is being made. For example, the percentage of U.S. non-federal acute care hospitals that electronically find patient health information, and send, receive, and integrate patient summary of care records from sources outside their health systems, has nearly doubled in the last four years, from 23 percent in 2014 to 41 percent in 2017.⁹ Ninety percent of hospitals and 48 percent of office-based physicians are electronically sending or receiving (or exchanging) patient health information with health care providers outside their organizations.^{10,11} Individuals are increasingly able to access their health information electronically.¹² But more work is needed.

Several actions have been taken by both the public and private sectors to advance interoperability and information sharing. For example, the 2015 Edition of the ONC Health IT Certification Program contains several provisions designed to advance interoperability including new interoperability-focused standards and requirements associated with application programming interfaces (APIs).¹³ The 21st Century Cures Act—a bipartisan bill passed nearly unanimously in December 2016—also contains several provisions designed to advance interoperability, including those related to reducing information blocking and advancing a trusted exchange framework and a common agreement for exchange between health information networks nationally.¹⁴ Implementation of the Act is now well underway. On February 11, 2019, CMS and ONC released proposed rules to support seamless and secure access, exchange, and use of electronic health information.

The chief executives of organizations represented by the Healthcare Leadership Council (HLC) and the Bipartisan Policy Center came together in 2018 to identify ways to further advance the interoperability of systems and electronic information sharing to support better health outcomes and higher-quality, safer, more cost-effective, and patient-centered care for individuals and populations in the United States.

This report describes the results of this work, including a shared vision for an interoperable healthcare system, a review of public- and private-sector progress, the case for change, priority areas of focus, measures of interoperability progress, and recommendations for both the private sector and the public sector.

The report was informed by more than 100 individuals representing every sector of health care, including clinicians, hospitals and health systems, long-term and post-acute care (LTPAC) providers, health plans, life sciences organizations, EHR and other technology developers, data analytics companies, and patients. HLC and BPC engaged University of California, San Francisco (UCSF) researchers who interviewed more than 50 individuals representing HLC and BPC members, as well as other health IT and interoperability experts. Detailed methods, along with the UCSF report, can be found at [Appendix II](#). HLC and BPC also gained input during multiple meetings with members—including CEOs—and public sector leaders, including an all-day roundtable discussion conducted in October 2018 with representatives of about 50 organizations which yielded valuable insights.

Shared Vision for an Interoperable Healthcare System

Supporting better health outcomes and higher quality, safer, more cost-effective, patient-centered care for individuals and populations requires advancing interoperability of systems and electronic information sharing. In an ideal vision for an interoperable healthcare system, the patient is at the center and the right data are available to the right person at the right time. Access to high-quality, accurate, and actionable data is seamless and integrated within clinical workflows, providing value and convenience, as well as reducing healthcare costs. There is trust in the system; privacy is protected, and information is kept secure.



"The journey to a value-based, efficient healthcare system must be built on a foundation of seamless, interoperable health data. This research effort informs the industry of where we are today, and points to the roles private and public sectors can play to make further progress on interoperability—ultimately making the healthcare system better for all stakeholders—most importantly patients. We look forward to collaborating with policymakers and all industry participants on the path forward."

—NEIL DE CRESCENZO, PRESIDENT AND CEO, CHANGE HEALTHCARE AND
CHAIRMAN, HEALTHCARE LEADERSHIP COUNCIL

Progress on Interoperability

Numerous actions have been taken by both the public and the private sectors to advance interoperability in recent years.

Many of the federal government's activities related to interoperability have been centered on implementation of the 21st Century Cures Act, the key provisions of which are summarized below:

- Clearly defining interoperability: “[E]nables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user; allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and does not constitute information blocking.”
- Requiring that health IT developers or entities, as a condition of certification: (1) publish APIs and allow health information from such technology to be accessed, exchanged, and used without special effort and (2) successfully test the real-world use of the technology for interoperability.
- Requiring the U.S. Department of Health and Human Services (HHS) ONC, within to “develop or support a trusted exchange framework, including a common agreement among health information networks nationally.”
- Requiring the Office of the Inspector General to carry out enforcement activities related to information blocking, including working with ONC to issue rules on “reasonable and necessary” exceptions to the information blocking prohibition.
- Requiring the Government Accountability Office to conduct a study to review the policies and activities of ONC and other stakeholders to ensure appropriate patient matching and survey ongoing efforts to assess effectiveness.¹⁵

A proposed rule addressing interoperability, information blocking, and the ONC Health IT Certification Program was sent to the Office of Management and Budget on September 17, 2018, launching a 90-day timeline for the agency's review.¹⁶ On February 11, 2019, CMS and ONC issued proposed rules associated with the use of APIs, information blocking, and the trusted exchange framework.

★ ★ ★

“One of the most powerful levers we have to improve health outcomes and reduce health care costs is the seamless sharing of clinical data with consumers and providers, regardless of technology systems. To realize the potential of the digital health era, we must empower individuals with information to engage in their own health, while creating pathways to ensure the right information is available at the right place and time for high-quality, cost-efficient care delivery. These priorities have guided Cerner's work for decades, and an open and interoperable health care ecosystem built on commonly adopted information-sharing standards remains fundamental to advancing person-centric care today. I'm supportive of the policy proposals the HLC and BPC have suggested to encourage further progress toward meaningful interoperability of systems and electronic information sharing in the United States.”

—BRENT SHAFER, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, CERNER

On January 5, 2018, ONC released the Draft Trusted Exchange Framework, which outlines a common set of principles that networks will need to follow to engender trust, as well as minimum terms and conditions for trusted exchange that would be incorporated into a Common Agreement.¹⁷ The Common Agreement, a national exchange agreement, is proposed to be a legal

binding contract that “qualified health information networks” and health information networks would voluntarily sign onto and agree to abide by. An updated version of the Trusted Exchange Framework and Common Agreement is expected to be implemented through formal rule-making and published in the Federal Register in 2019.¹⁸

The 2015 Edition of the ONC Health IT Certification Program includes provisions that will accelerate interoperability. For example, it contains additional advanced standards and implementation specifications to support interoperability and requires certified health IT to demonstrate that it can provide application access to a “Common Clinical Data Set” via an open API.¹⁹ Open APIs are technology that allow one software program to access the services provided by another software program. Open APIs can support patients’ ability to have greater access to their health information through, for example, smartphones.²⁰ They can also enable clinicians to access their patients’ health information individually, and as a summary of care document that they can exchange with other clinicians.²¹

In 2018, CMS issued hospital and physician payment rules that prioritize interoperability requirements, changing the name of the CMS Medicare and Medicaid EHR Incentive Programs to *Promoting Interoperability Programs*.^{22,23} CMS also launched the Medicare Blue Button 2.0, an API that provides access to four years of Medicare Part A, B, and D data for 53 million Medicare beneficiaries. This data includes the type of Medicare coverage, drug prescriptions, primary care treatment, and cost.²⁴

The Administration also launched the *MyHealthEData* initiative, which aims to empower patients by ensuring that they control their healthcare data and can decide how their data can be used, while keeping that information safe and secure. The White House Office of American Innovation leads this federal government-wide initiative with participation from HHS—including CMS, ONC, and the National Institutes of Health, as well as the U.S. Department of Veterans Affairs. It is intended “to break down the barriers that prevent patients from having electronic access and true control of their own health records from the device or application of their choice. This effort will approach the issue of healthcare data from the patient’s perspective.”²⁵

There are also a number of private sector organizations and initiatives focused on various aspects of health information exchange and interoperability, including the Commonwell Health Alliance;²⁶ The Sequoia Project and its two subsidiaries Carequality and eHealth Exchange;²⁷ the CARIN Alliance;²⁸ Integrating the Healthcare Enterprise (IHE);²⁹ and the Strategic Health Information Exchange Collaborative.³⁰ There are also more than 100 regional health information exchanges (HIEs)³¹ and other private sector networks—such as Surescripts³²—that facilitate data exchange.



“As patients become more actively engaged consumers of healthcare, and as the industry transitions to a value-based payment model, care providers must have the ability to easily access and share patient health information at the point of care. The Surescripts Network Alliance, including health systems, technology vendors, payers, pharmacies, and pharmacy benefit managers, is working to accelerate healthcare interoperability each and every day. With the right information, at the right place, at the right time, providers can make more informed care decisions which leads to better outcomes, reduced costs, and improved patient and provider experiences.”

—TOM SKELTON, CHIEF EXECUTIVE OFFICER, SURESCRIPTS

Open APIs, such as HL7 FHIR®, have rapidly become a key component of public and private sector efforts to accelerate access to and exchange of health information.³³

The HL7 Argonaut Project, a private sector initiative, has been developing a core set of HL7 FHIR® implementation specifications which will enable expanded information sharing for electronic health records and other health IT solutions based on modern computing standards.³⁴ Substitutable Medical Applications, Reusable Technologies (SMART) Health IT is an open, standards-based technology platform that enables developers of apps to seamlessly and securely run across the healthcare system. Developed by Boston Children's Hospital Computational Health Informatics Program and the Harvard Medical School Department for Biomedical Informatics, SMART Health IT defines a health data layer that builds on the HL7 FHIR® API and resource definitions.³⁵

SMART on FHIR is a set of open specifications to integrate apps with EHRs, portals, health information exchanges, and other health IT systems.³⁶ Apple has implemented SMART on FHIR integration between EHRs and the iPhone, enabling iPhone users to visualize, securely store, and aggregate their health records from multiple institutions alongside their patient-generated data. Apple's connection between EHRs and the user's health app utilizes HL7 FHIR® standard APIs as defined by the Argonaut Project. Apple is working with Cerner, Epic, athenahealth, and others in the healthcare community to enable this feature. Supported data types currently include allergies, conditions, immunizations, lab results, medications, procedures, and vitals.³⁷ Finally, HL7's DaVinci Project is working with ONC and multiple payers, providers, and technology organizations to accelerate the adoption of the HL7 FHIR® standard to support exchange of information for value-based care.³⁸

A comprehensive list of public and private sector initiatives related to interoperability can be found in [Appendix I](#).

Case for Change

The benefits of interoperability and information sharing are well-documented. Bringing information about the patient—regardless of where care or services have been delivered—to the clinician and the care team enables well-informed, coordinated, patient-centered care. Supported by information from other care settings, clinicians can avoid duplicative tests, identify and address gaps in care, and avoid medication and other errors—all of which drive higher-quality and more cost-effective care.³⁹ Interoperability and the sharing of information are also necessary components of delivery system and payment models that reward value and outcomes versus volume, as well as transparency efforts. Interoperability also supports clinical research, post-market monitoring of medical products, and the detection of public health threats. Finally, interoperability and information sharing support individuals' access to their own health information, improving their ability to manage their health and healthcare.

★ ★ ★

"Healthcare interoperability is a critical step forward in advancing more patient-centric care. At Pfizer, a patient-focused mindset is deeply embedded within our organization, and we believe it is essential to developing medical innovations that can have a lasting impact on society. However, these medical innovations can only be effective if they are used by the right patient at the right time. Interoperability gives patients, providers, and caregivers access to the right information at the right time for the right patient, to make the right diagnosis and treatment decision. Ultimately, this will lead to improved health outcomes for all patients."

—MIKE GLADSTONE, GLOBAL PRESIDENT, INTERNAL MEDICINE, PFIZER BIOPHARMACEUTICALS GROUP

Advancing interoperability across multiple settings requires cooperation and joint effort across several different types of entities. HLC and BPC members agree that progress toward widespread, nationwide interoperability has been slow because it is not yet driven by a clear, collective business need that ties together the interests of providers, payers, technology companies, and patients.

★ ★ ★

"Interoperability of healthcare data will allow for more meaningful solutions to some of the biggest challenges in healthcare today. At Stryker, as we partner with our customers to make healthcare better, interoperability of data provides opportunity to create solutions that improve patient outcomes and bring new efficiencies to the delivery of care."

—TIM SCANNELL, PRESIDENT AND CHIEF OPERATING OFFICER, STRYKER

As illustrated in Figure 1 below, interoperability use cases that emerge from collective business need drive improvements in health outcomes and promote higher-quality, safer, more cost-effective, patient-centered care.

Figure 1. Addressing Business Needs and Improving Outcomes Through Interoperability⁴⁰



Payers generate aligned incentives by creating conditions that motivate providers to invest in and use interoperability and demand interoperability solutions from their vendors. This alignment of incentives, however, is not prevalent in the healthcare system. Large-scale investments in interoperability of systems and electronic information-sharing are rare due to higher-priority, competing business needs. As the U.S. healthcare system continues to migrate toward payment models that reward outcomes versus volume, organizations will have a stronger case for greater interoperability investment.⁴¹

Figure 2 summarizes the benefits of interoperability by stakeholder.

Figure 2. Benefits of Interoperability by Stakeholder

| Stakeholder | Benefits of Interoperability |
|--|--|
| Individuals | <p>When pertinent clinical information is available at the point of care, individuals benefit from care that is of higher quality, better informed, and timely. Individuals also benefit from improved safety, reduced costs, and fewer inconveniences caused by repeat appointments and unnecessary, duplicative tests, treatments, and services, which can be averted with complete clinical data at the point of care. Relevant, patient-generated data from all of a patient's medical services can also help prevent missed diagnoses and medication errors.</p> <p>Similarly, individuals with access to their own health information are more engaged, can make more informed patient and family care decisions, and can more easily share information among caregivers and providers.</p> |
| Providers | <p>Providers, including clinicians and hospitals, equipped with relevant patient information at the point of care are better prepared to provide high-quality, patient-centered care. Streamlined access to patient information from other providers, including hospitals, physician offices, clinics, as well as other care settings and ancillary service providers such as laboratories, radiology centers, and long-term and post-acute care providers, enables care coordination, improved clinical workflow, and better clinical decision-making.</p> <p>Improved interoperability can reduce provider burden and administrative costs. The typical primary care physician must coordinate care with 229 other physicians working in 117 practices.⁴² Having access to patient information also supports quality measure implementation and compliance with government regulations and payment program requirements.</p> |
| Payers | <p>Payers—or institutions that pay providers for healthcare services, such as health plans, private sector employers or purchasers, the government, and in some cases, individuals—bear financial risk for the costs associated with their beneficiaries' healthcare expenditures. They benefit from lower costs associated with reductions in diagnostic errors, unnecessary tests, and duplicate treatments—which are more likely when providers have comprehensive information at the point of care.</p> <p>Greater information access enables better care coordination and the ability to both measure and improve health outcomes. Payers need to be able to measure health outcomes to implement new payment models focused on value. Payers also benefit when individuals become more engaged in their health and healthcare through access to their own health information.</p> <p>Improved provider and patient access to health information can also help assure that patients take their medications as prescribed. Medication non-adherence has been estimated to cost the U.S. healthcare system between \$100 billion and \$289 billion annually.⁴³</p> |
| Business/Industry | <p>Health IT developers and EHR vendors have the incentive to support interoperability if their customers demand it. Pressures from emerging legislative and regulatory payment and compliance regulations also play a key role, including ONC's Health IT Certification program and pending rules on information blocking, which carry potential fines of \$1 million per violation.⁴⁴</p> <p>Innovators in business and industry benefit from greater data availability, which supports innovative new products and services, including those focused on data analytics, artificial intelligence, and patient-facing applications.</p> |
| Clinical Researchers and Manufacturers | <p>Data from the clinical care process play a key role in clinical studies that support the development, regulatory evaluation, approval, and post-market monitoring of drugs, biologics, and medical devices. For example, access to clinical data can support the recruitment of patients for clinical trials. Clinical data can also be used to generate real-world evidence to augment and support clinical studies used for regulatory evaluation and approval, including a new indication for an approved drug or post-approval study requirements as referenced in the 21st Century Cures Act.</p> |
| Public Health | <p>Access to de-identified patient data across settings significantly improves public health efforts, including surveillance, preparedness, and response efforts for public health threats, such as infectious disease outbreaks, natural disasters, and epidemics.</p> |

Priority Areas

Despite the temptation to assess the interoperability of health IT systems for a broad range of use cases, HLC and BPC members acknowledge that prioritizing a few key areas is necessary to effect meaningful change through measurement and private and public sector action. HLC and BPC members, with input from other experts, determined that focusing on the following two key interoperability priorities would be most impactful:

- Information needs at the point of care to support care delivery; and
- Information needs of individuals to support management of their own health and healthcare.

Focusing on these two priority areas, without losing sight of the individual as the ultimate beneficiary of interoperability, provides a manageable approach toward driving change. HLC and BPC members also recognize that other priority areas—including efforts to improve population health, research, and public health—will benefit from and leverage progress in the clinical and patient-focused priority areas.

★ ★ ★

“Use of data, analytics and tools such as artificial intelligence will transform our ability to cure and prevent illness. This depends on interoperability, especially the ability of providers to access data at the point of care and within workflow. This report recommends essential steps by private and public stakeholders. We look forward to working with HLC and BPC to make this a reality.”

SUSAN DEVORE, PRESIDENT AND CHIEF EXECUTIVE OFFICER, PREMIER HEALTHCARE ALLIANCE

Priority Area 1: Bringing Information to the Point of Care to Support Care Delivery

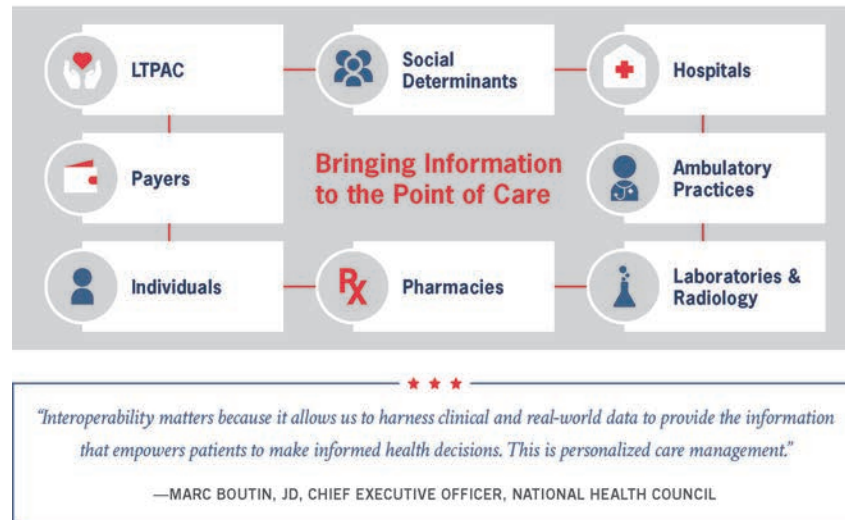
As illustrated in Figure 3, information from hospitals, ambulatory practices, laboratories, radiology centers, pharmacies, LTPAC providers, payers, and patients plays a critical role in assuring well-informed, patient-centered, safe, coordinated delivery of care. Information from patients can come in many forms, including data from wearables and remote monitoring devices, as well as health apps that capture health information from multiple sources. Increasingly, information from non-medical or social determinants of care is being used by providers to improve health outcomes and care. To be truly impactful, clinical data should be accurate, of high-quality, comparable (or standards-based), sourced, and complete. These data attributes will enable clinicians to filter and prioritize the data for more effective use in clinical decision-making. Access to such information should be seamless and integrated into clinical workflows. Given evolving trends in technology and care delivery, the point of care can extend beyond the office setting or the hospital into the home via telehealth and other digital modes of care. Information flows to the point of care reinforce the primary goal of supporting better health outcomes and higher quality, safer, more cost-effective, patient-centered care.

★ ★ ★

“Interoperability is essential to achieve our quality and affordability goals.”

—JAEWON RYU, INTERIM PRESIDENT AND CHIEF EXECUTIVE OFFICER, GEISINGER

Figure 3. Information Sources Needed at the Point of Care



Priority Area 2: Giving Individuals Access to Their Own Health Information

As illustrated in Figure 4, data from hospitals, ambulatory practices, laboratories, radiology centers, pharmacies, LTPAC providers, payers, non-medical sources that capture social determinants information, and patients also play a critical role in helping individuals and their proxies engage in and manage their health and health care. Individuals and their authorized caregivers should be able to easily obtain, use, and share their digital health information when, where, and how they want to achieve their goals. People who are actively engaged in their healthcare are more likely to stay healthy and manage their conditions by asking their doctors questions about their care, following treatment plans, eating right, exercising, and receiving health screenings and immunizations. Patients without the skills to manage their healthcare incur costs up to 21 percent higher than patients who are highly engaged in their care.⁴⁵ Enabling individuals' access to their own health information reinforces the primary goal of supporting better health outcomes and more cost-effective, patient-centered care.

Figure 4. Information Sources Needed by Individuals



Measuring Interoperability Progress

Achieving success in any endeavor requires measuring progress. Recognizing this imperative, Congress—through the Medicare Access and CHIP Reauthorization Act—called upon the HHS Secretary to develop metrics and to publicly report on progress in achieving widespread exchange of health information through interoperable certified EHR technology nationwide by December 31, 2018.⁴⁶

HHS both funds and reports publicly on key measures of interoperability related to several of the clinical and patient access priority areas described in this report. Measures associated with interoperability and information-sharing to support bringing information to the point of care are currently included in surveys of hospitals, physicians, and individuals; results are summarized in Figure 5 below.

Figure 5. National Measures of Progress for Interoperability

| MEASURE | NON-FEDERAL ACUTE CARE HOSPITALS (2017) ⁴⁷ | OFFICE-BASED PHYSICIANS (2015) ⁴⁸ | INDIVIDUALS (2017) ⁴⁹ |
|--|---|--|-------------------------------------|
| Electronically send (1) summary of care records in the case of hospitals or (2) patient health information in the case of physicians to any providers outside their organization | 88% | 38% | |
| Electronically receive (1) summary of care records in the case of hospitals or (2) patient health information in the case of physicians from other providers | 74% | 38% | |
| Electronically integrate (1) summary of care records in the case of hospitals or (2) patient health information in the case of physicians from other providers | 53% | 31% | |
| Electronically search for or find patient health information from other providers | 61% | 34% | |
| Electronically send, receive, integrate, and search for or find summary of care records of patient health information from other providers | 41% | 9% | |
| Offered online access to their medical record by a healthcare provider or insurer | | | 52% |
| Viewed their online medical record at least once in the past year | | | 28% |
| Used access to online medical record to: | | | |
| • View test results | | | 85% |
| • Perform one or more health-related tasks | | | 62% |
| • Download medical record | | | 17% |
| • Transmit data to outside party | | | 14% |

In the past, HHS has also tracked measures associated with health information sharing among skilled nursing facilities and other providers⁵⁰ as well as patient access to test results among clinical laboratories.⁵¹

Measure results currently supported by federal dollars offer a national snapshot of interoperability and information sharing—particularly among physician offices and hospitals. More work is needed to measure national progress on other important data sources identified within the two priority areas described in this report—bringing information to the point of care and enabling individual access to health information.

Model for Accelerating Interoperability

While the lack of a collective business need that aligns the interests of payers, providers, technology companies, and patients is the primary barrier to widespread interoperability, additional challenges exist. The costs associated with developing and implementing modifications to support interoperability; the lack of capability to either receive or send data among trading partners; difficulty finding providers' addresses; technical barriers, including slow and inconsistent adoption of standards, concerns about data quality, and challenges with accurately matching patient data; and the need for trust to address concerns about privacy and security all serve as barriers to interoperability and information sharing.^{52,53,54}

As illustrated in Figure 6 below, achieving better outcomes through interoperability requires actions that address the multiple barriers to interoperability, including those related to developing a shared business case; technical infrastructure issues, such as those related to standards development and adoption; policies and regulations; and governance and leadership.⁵⁵

Figure 6. Model for Accelerating Interoperability



HLC and BPC have identified a set of private and public sector actions in each of these areas—business case, technical infrastructure, policies and regulations, and governance and leadership—to accelerate progress toward nationwide interoperability.

Recommendations

Advancing interoperability to support better outcomes through the delivery of care and access to information among individuals will require leadership and action in four key areas, outlined below.

1. STRENGTHEN BUSINESS CASE

Interviews with members revealed a shared perspective that the U.S. health care system is not pursuing interoperability effectively because it isn't using approaches that have proven successful in other industries and contexts. This is apparent in the lack of widespread business incentives to achieve interoperability. Many efforts to pursue interoperability today pull the key market players along—sometimes unwillingly and sometimes willingly—but with little sense of urgency. This lack of commitment is a symptom of the reality that interoperability is “nice to have” but not a “stay in business” issue. The private sector should use the tools at its disposal to change market dynamics in ways that create a widespread business need for broad-based interoperability.

Key levers to strengthen the business case include healthcare purchasers' and payers' expectations of providers, including those that support delivery system and payment reforms, as well as providers' expectations of their software vendors. In an era of greater financial responsibility and increasing out-of-pocket costs for healthcare, patients can also exercise leverage through purchasing behaviors with their providers and payers.

Continued movement by payers toward value-based care delivery and advanced payment models that reward outcomes versus volume provide greater incentives for information-sharing across an individual patient's multiple providers and ancillary service providers. Just as public and private sector payers are collaborating through a multi-stakeholder, voluntary effort created to promote measure alignment and harmonization through the *Core Quality Measures Collaborative*⁵⁶ and its predecessor organizations, providers, payers, and vendors have opportunities to promote uniformity in information sharing.

As software purchasers, providers and clinicians can also play a key role in ensuring greater interoperability of systems, particularly as they replace and upgrade existing systems. The National Academy of Medicine recently published *Procuring Interoperability: Achieving High-Quality, Connected, and Person-Centered Care*, which details approaches for health care organizations to ensure interoperability, including an interoperability needs identification process and a procurement specification process.⁵⁷ To help providers select and negotiate the acquisition of an EHR system, ONC published a guide offering strategies and recommendations for negotiating best practice EHR contract terms, including example contract language for promoting interoperability.⁵⁸

Recommendation (Private Sector) 1.1: Payers should collaborate with providers to gain agreement on and drive adoption of baseline expectations for interoperability and information sharing through payment incentives that focus on outcomes versus volume, contracts, and other mechanisms.

Recommendation (Private Sector) 1.2: Providers, including clinicians, hospitals, health systems, and group purchasers, should collaborate with EHR and other clinical software developers to gain agreement on and drive adoption of baseline expectations for interoperability for products through incorporation into contract language. Existing requirements, such as those included in the ONC Health IT Certification Program, should be leveraged. Clinical software and other technology developers and vendors should collaborate with their customers to integrate expectations for interoperability within their products.

Recommendation (Private Sector) 1.3: Providers, payers, and technology developers should engage individuals to identify and prioritize information access expectations.

To facilitate this process, HLC commits to convening providers as well as EHR and other health IT developers to develop baseline expectations of and requirements for interoperability for inclusion in sample model contracts.

2. IMPROVE TECHNICAL INFRASTRUCTURE

Adopt Common Baseline Standards to Improve Patient Matching

Getting to nationwide interoperability and information sharing requires the ability to match a patient's data across health settings and information systems accurately. Unfortunately, patient matching rates vary widely, with health care facilities failing to link records for the same patient up to half of the time.⁵⁹ According to a study by the Pew Charitable Trusts, patient matching typically occurs through the use of algorithms, unique identifiers, manual review, or a combination of these methods. Innovation in this area is expected in the future, which may include patient-empowered approaches such as the use of smart phones.⁶⁰ Standardizing a set of data elements that providers collect to support patient matching, whether through algorithms or other methods, is expected to significantly improve matching.

The current ban on the federal government's ability to conduct work on a unique patient identifier has limited the federal government's ability to fully collaborate with the private sector on solutions. However, report language contained in appropriations legislation over the last three years encourages the HHS Secretary, working through ONC and CMS, to provide technical assistance to private-sector led initiatives focusing on a coordinated strategy for a patient matching solution.⁶¹ CMS' proposed rule on interoperability issued on February 11, 2019 seeks comment on ways for ONC and CMS to continue to facilitate private sector efforts on a workable and scalable patient matching strategy. Providers, software developers, and other healthcare organizations should therefore collaborate on the identification of a common set of data elements all of which should be collected by providers—using federally adopted standards (such as those contained in the ONC Interoperability Standards Advisory) to support matching. Private sector collaboration involving multiple stakeholders, including health care providers, technology vendors, payers, and health information exchange networks with technical assistance and support from HHS can help to drive a de facto standard for patient matching.

Recommendation (Private Sector) 2.1: Providers, software developers, payers, and other health care organizations should collaborate with technical assistance from HHS on the identification and collection of a common set of data elements using federally adopted standards, to improve matching.

Recommendation (Private Sector) 2.2: Providers, software developers, payers, and organizations representing individuals should collaborate on efforts to explore, pilot, and evaluate the feasibility of widespread adoption of patient-centered approaches to identification.

Prioritize Interoperability and Standards Conformance in ONC Health IT Certification

The ONC Health IT Certification Program is meant to signal which EHR and health IT systems meet federal requirements and include useful functionality. The expense of implementing, maintaining, and updating EHRs and other health IT systems is significant. The ONC Health IT Certification Program is a valuable indicator of whether the EHR technology being purchased meets all federal requirements. In addition to assuring that EHRs meet these requirements when purchased, users expect the EHRs they implement to function at their expected performance level *after* implementation. This expectation was codified into law under the 21st Century Cures Act, which requires “real-world” testing of health IT products under the ONC Health IT Certification Program.⁶² ONC's proposed rule issued February 11, 2019 includes provisions for testing. As noted by the National Institute for Standards and Technology (NIST), “[W]ell-defined standards, and conformance to those standards, provide the foundation for reliable, functioning, usable, and interoperable healthcare information systems...the proliferation of healthcare information systems designed without compliance to standards will likely exacerbate, not lessen, current patient care challenges by creating a landscape saturated with systems lacking usefulness, usability, and interoperability...standards must be used and deployed as intended, and conformance testing is the process that helps ensure adherence to the standards.”⁶³

ONC collaborates with organizations such as NIST as part of program operations to develop functional and conformance testing requirements, test cases, and test tools, and to conduct surveillance of certified health IT.⁶⁴ The current 2015 Edition ONC Health IT Certification includes updated criteria that support electronic exchange of interoperable health information.⁶⁵ CMS rulemaking to date signals increased emphasis on interoperability.^{66,67} To drive closer to the goal of interoperable health IT, ONC should also prioritize interoperability and assure continuous, real-world testing of health IT systems in future rulemaking to ensure that certified products meet the real-world expectations of their end users.

Recommendation (Public Sector) 2.3: ONC should prioritize interoperability and require real-world testing to assess conformance with interoperability standards in future editions of the ONC Health IT Certification Program.

Pursue Rapid Adoption of FHIR-Based APIs to Accelerate Information Sharing

There is growing momentum behind the broad adoption and use of open APIs and specifically HL7 FHIR®, to build upon existing efforts toward advancing interoperability. The 2015 Edition of ONC Health IT Certification requires capabilities for open APIs. However, ONC regulations do not specify HL7 FHIR® for these APIs, as it was an emerging standard at the time the regulations were developed. The expectation is that most certified health IT will use FHIR as the basis for open APIs, and that future regulations and requirements may consider updates to technology standards, including FHIR.

There is still substantial opportunity for organizations to engage more actively in API-related efforts, beginning with engagement in HL7 FHIR® development and implementation processes, and working with groups like the Argonaut Project to operationalize the standards. Also critical is engaging vendors to prioritize which available FHIR-related activities to implement and support in their future upgrades. Ultimately, it is most critical that organizations holding healthcare data turn on all available HL7 FHIR®-based APIs to make the greatest breadth of data available for exchange. Proposed rules issued by CMS and ONC on February 11, 2019 contain several provisions designed to accelerate the adoption of HL7 FHIR® among technology developers and payers.⁶⁸

Recommendation (Private Sector) 2.4: Providers, EHR and other software developers, payers, and other health care organizations should expand upon existing interoperability efforts by pursuing rapid adoption and implementation of HL7 FHIR®-based or other open standards-based APIs, to accelerate interoperability, data access, and information sharing.



"Greater interoperability will improve care quality and continuity and enhance market transparency, so that consumers can better understand costs and evaluate quality. More accessible information also allows Hearst Health's companies to deliver new tools to help positively impact the quality and cost of care."

—GREGORY DORN, MD, PRESIDENT, HEARST HEALTH

3. IMPROVE POLICIES AND REGULATIONS

Implement a Common Notice of Information Access for Patients

Individuals need access to their own health information to help them make decisions about their health and healthcare. Individuals are beginning to take advantage of these capabilities. The Health Insurance Portability and Accountability Act (HIPAA) gives consumers the right to access their health information. In 2017, half of Americans reported they were offered access to an online medical record by a provider or insurer, up from 42 percent in 2014.⁶⁹

A patient's health information ordinarily resides in multiple places, such as the offices of primary care providers and specialists, clinics, hospitals and health systems, laboratories, pharmacies, radiology centers, and health plans. Obtaining access to this information can be confusing and challenging for patients. Instructions and processes can vary significantly across entities.

Creating and adopting standard language for how patients can gain access to their health information across providers and other health care entities can increase clarity and improve patient access. A standard "notice of information access practices"—like the Model Privacy Notice Forms adopted by eight federal agencies in 2009—can make it easier for consumers to understand how they can obtain access to their health information.⁷⁰

Recommendation (Private Sector) 3.1: Health care organizations should collaborate with organizations representing individuals as well as the federal government, to reach agreement on a standard "Notice of Information Access Practices" and voluntarily make such notice available to patients to reduce confusion and make it easier for individuals to access their health information.

Align Privacy Laws with HIPAA

It has been nearly 20 years since the implementation of HIPAA privacy and security rules. The HIPAA privacy rule has established a uniform framework for acceptable uses and disclosures of individually-identifiable health information within healthcare delivery and payment systems for the privacy and security of information.⁷¹ The healthcare industry has become accustomed to and supportive of the HIPAA privacy and security rules framework and the strong protections it affords consumers. This has a direct impact on the flow of electronic health information. Yet, variations and inconsistencies in consent laws, including those for substance use disorder treatment under 42 CFR Part 2, remain a barrier to interoperability. Varying state and territory laws often serve as a bottleneck to information flow and add to the administrative and legal costs associated with complying with the patchwork of state-specific laws. In order to fully achieve nationwide interoperability, further alignment of state and federal privacy laws is necessary.

Recommendation (Public Sector) 3.2: States should consider harmonizing privacy laws to align with HIPAA.

Recommendation (Public Sector) 3.3: HHS should align consent policies for substance use disorder treatment under 42 CFR Part 2 with HIPAA.

In December 2018, the HHS Office for Civil Rights (OCR) issued a Request for Information, seeking input from the public on how the HIPAA privacy regulations could be modified to drive more care coordination and value in the healthcare system.⁷² While HIPAA has served as a constructive and effective framework to protect the privacy and security of individuals' health information, HHS has noted that the privacy rule may impede other forms of care coordination that can drive value.⁷³ Fine-tuning HIPAA's requirements to improve information-sharing for treatment and care coordination is a necessary step to advance the interoperability of health systems nationwide.

"Health data interoperability helps assure that our nation's citizens, veterans, and soldiers receive the best care available, even as they move from one provider to another. At Leidos, we believe that the best care is possible only when the consumer is placed at the center of his or her own health and well-being. Data interoperability is essential in making this a reality. Improving and promoting policy and standards to assure that health data is shareable and shared is something we take seriously at Leidos."

—JONATHAN SCHOLL, PRESIDENT, LEIDOS HEALTH GROUP

4. GOVERNANCE AND LEADERSHIP

The Trusted Exchange Framework and Common Agreement (TEFCA)—once finalized—will provide governance for interoperability and health information exchange. Private sector leaders should fully engage in offering comments on the proposed TEFCA once published in the Federal Register, and work together to advance successful implementation of the effort.

Public and private sector leaders can also demonstrate leadership by focusing the U.S. healthcare system and their individual organizations on key measures of interoperability progress and the actions that can be taken to drive improvement on those measures.

While the United States has made progress toward nationwide interoperability, raising awareness of progress and galvanizing private sector action will help the healthcare system overcome remaining barriers and advance efforts to improve information-sharing and interoperability.

Many measures already exist with progress tracked by federally funded efforts. These include measures associated with interoperability and information sharing among hospitals and physician practices.

Additional measures will be needed—many of which can be captured and reported by the private sector—to measure national progress on the information sharing practices of other data sources identified within the two priority areas identified in this report—bringing information to the point of care and enabling individual access to health information. They include the level of information sharing among clinicians and patients with laboratories, pharmacies, radiology centers, behavioral healthcare providers, LTPAC providers, and health plans, and the ability for individuals to access their health information via open APIs with all of such sources, as well as with physician offices, hospitals, and health systems.

Some experts call for additional measures that address the impact of interoperability or methods that eliminate confounders. Others call for methods that do not rely on self-reporting. Measurement can be complicated and difficult. Expanding the number or complexity of measures must be carefully considered, weighing the benefit versus the increased burden of data collection.

Private-sector leaders should highlight a small, impactful set of progress measures—captured at both the organization level and nationally—with their internal staff, as well as with their EHR vendors, customers, and information-sharing partners, to encourage both action and improvement.

Focusing on the key areas listed below, private sector health care leaders—including hospitals and health systems, physician practices, health plans, laboratories, LTPAC providers, pharmacies, radiology centers, and clinical software developers and vendors—should collaborate with federal government leaders to leverage federal measures and reporting where they do exist; develop and implement measures where none exist; convene efforts to identify and take private sector actions to improve performance on measures; and publicly monitor progress on an annual basis.

Key areas of focus should include the level of:

- Clinician and patient access to information from independent laboratories and radiology centers.
- Clinician access to pharmacy data indicating that a prescription has been filled.
- Information sharing between behavioral healthcare providers and primary care physicians, hospitals, and individuals.
- Information sharing between LTPAC providers and clinicians, hospitals, and individuals.
- Clinician and patient access to information from health plans.
- Physicians and hospitals that connect to at least one network.
- Individual electronic access via an open API to health information contained in physician offices, retail clinics, hospitals and health systems, laboratories, radiology centers, health plans, and LTPAC providers.

Recommendation (Private and Public Sectors) 4.1: Public- and private-sector leaders should collaborate on the identification and annual reporting of key measures that assess national progress on interoperability and information sharing to support bringing information to the point of care and providing individuals access to their own health information. They should convene efforts to define and launch the execution of private sector actions that will accelerate progress on measures.

Conclusion

The United States healthcare system is poised to transform in ways that will bring information to individuals and those who deliver care to drive improvements in the health of individuals and the quality, safety, and cost of care. Interoperability and information sharing play a key role in achieving this goal. Together, public- and private-sector leaders can take actions to accelerate interoperability to improve health, improve care, and improve the lives of all Americans.

Acknowledgements

HLC and BPC would like to thank and acknowledge individuals working within the following organizations who helped in the development of this report by contributing their time and expertise—through participation in interviews, meetings, and roundtable discussions.

| | | |
|--|---|--|
| AdventHealth | CommonWell Health Alliance | Merck |
| Aetna, a CVS Health business | ConnectiveRx | National Association for the Support of Long Term Care |
| American Academy of Family Physicians | Cotiviti | National Health Council |
| American Academy of Pediatrics | Eli Lilly | National MS Society |
| American College of Physicians | Epic | New England Healthcare Exchange Network |
| AmerisourceBergen | Fairview Health Services | NewYork-Presbyterian Hospital |
| Amgen | Franciscan Missionaries of Our Lady Health System | NorthShore University HealthSystem |
| AMN Healthcare | Geisinger Health System | Novartis |
| Anthem | Genosity | Office of the National Coordinator for Health Information Technology |
| Ascension | Hearst Health | Roivant Sciences and Datavant |
| athenahealth | HCA Healthcare | Pfizer |
| Beth Israel Deaconess Medical Center | HIMSS North America | Premier healthcare alliance |
| BioReference Laboratories | Intermountain Healthcare | SCAN Health Plan |
| BlueCross BlueShield of Tennessee | IQVIA | Senior Helpers |
| Bristol-Myers Squibb | Johnson & Johnson | Stryker |
| Cardinal Health | Kaiser Permanente | Surescripts |
| CareJourney | Leidos | Teladoc |
| CARIN Alliance | LEO Pharma | Tenet Health |
| Center for Medical Interoperability | LTPAC Health IT Collaborative | Texas Health Resources |
| Centers for Medicare and Medicaid Services | Mallinckrodt | The Pew Charitable Trusts |
| Cerner | Marshfield Clinic Health System | The Sequoia Project |
| Change Healthcare | Massachusetts eHealth Collaborative | UCB |
| ChenMed | Maxim Healthcare Services | University of California, San Francisco |
| Children's Hospital of Philadelphia | Mayo Clinic | University of Texas at Austin |
| CHIME | McKesson | Vizient |
| City of Hope | Medidata Solutions | ZS Associates |
| Cleveland Clinic | Medtronic | |
| Clinovations | MedStar Health | |
| Comfort Keepers | MemorialCare Health System | |

Endnotes

- ¹ Office of the National Coordinator for Health Information Technology. "Office-Based Physician Electronic Health Record Adoption." *Health IT Quick-Stat*, no.50. December 2016. Available at: <https://dashboard.healthit.gov/quickstats/pages/physician-ehr-adoption-trends.php>
- ² JaWanna Henry, Yuriy Pylypchuk, Talisha Searcy, and Vaishali Patel. "Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2015." *ONC Data Brief*, no. 35. Office of the National Coordinator for Health Information Technology. May 2016. Available at: <https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php#references>.
- ³ Yuriy Pylypchuk, Christian Johnson, JaWanna Henry, and Diana Ciricean. "Variation in Interoperability among U.S. Non-federal Acute Care Hospitals in 2017." *ONC Data Brief*, no.42. Office of the National Coordinator for Health Information Technology. November 2018. Available at: https://www.healthit.gov/sites/default/files/page/2018-11/Interop%20variation_0.pdf.
- ⁴ Ibid.
- ⁵ Eric Jamoom and Ninee Yang. "State Variation in Electronic Sharing of Information in Physician Offices: United States, 2015." *NCHS Data Brief*, No. 261. Centers for Disease Control and Prevention, National Center for Health Statistics. Available at: <https://www.cdc.gov/nchs/products/databriefs/db261.htm>.
- ⁶ Vaishali Patel and Christian Johnson. "Individuals' Use of Online Medical Records and Technology for Health Needs." *ONC Data Brief*, No. 40. Office of the National Coordinator for Health Information Technology. Available at: <https://www.healthit.gov/sites/default/files/page/2018-03/HINTS-2017-Consumer-Data-Brief-3.21.18.pdf>.
- ⁷ Office of the National Coordinator for Health Information Technology. "Office-Based Physician Electronic Health Record Adoption." *Health IT Quick-Stat*, no.50. December 2016. Available at: <https://dashboard.healthit.gov/quickstats/pages/physician-ehr-adoption-trends.php>
- ⁸ JaWanna Henry, Yuriy Pylypchuk, Talisha Searcy, and Vaishali Patel. "Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2015." *ONC Data Brief*, no. 35. Office of the National Coordinator for Health Information Technology. May 2016. Available at: <https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php#references>.
- ⁹ Yuriy Pylypchuk, Christian Johnson, JaWanna Henry, and Diana Ciricean. "Variation in Interoperability among U.S. Non-federal Acute Care Hospitals in 2017." *ONC Data Brief*, no.42. Office of the National Coordinator for Health Information Technology. November 2018. Available at: https://www.healthit.gov/sites/default/files/page/2018-11/Interop%20variation_0.pdf.
- ¹⁰ Ibid.
- ¹¹ Eric Jamoom and Ninee Yang. "State Variation in Electronic Sharing of Information in Physician Offices: United States, 2015." *NCHS Data Brief*, No. 261. Centers for Disease Control and Prevention, National Center for Health Statistics. Available at: <https://www.cdc.gov/nchs/products/databriefs/db261.htm>.
- ¹² Vaishali Patel and Christian Johnson. "Individuals' Use of Online Medical Records and Technology for Health Needs." *ONC Data Brief*, No. 40. Office of the National Coordinator for Health Information Technology. Available at: <https://www.healthit.gov/sites/default/files/page/2018-03/HINTS-2017-Consumer-Data-Brief-3.21.18.pdf>.
- ¹³ Office of the National Coordinator for Health Information Technology. *2015 Edition Final Rule: Expanding Electronic Health Information Access and Exchange*. Available at: <https://www.healthit.gov/sites/default/files/playbook/pdf/2015-edition-final-rule.pdf>.
- ¹⁴ 21st Century Cures Act, Pub. L No. 114-255, § 4002, 130 Stat. 1033 (2016), 386.
- ¹⁵ Ibid.
- ¹⁶ Office of Information and Regulatory Affairs, Office of Management and Budget. *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, Pending EO 12866 Regulatory Review*. September 17, 2018. Available at: <https://www.reginfo.gov/public/do/eoDetails?rid=128483>.
- ¹⁷ Office of the National Coordinator for Health Information Technology. *Trusted Exchange Framework and Common Agreement*. Available at: <https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement>.

- 18 Office of the National Coordinator for Health Information Technology. *2018 Report to Congress: Annual Update on the Adoption of a Nationwide System for the Electronic Use and Exchange of Health Information*. December 2018. Available at: <https://www.healthit.gov/sites/default/files/page/2018-12/2018-HITECH-report-to-congress.pdf>.
- 19 Office of the National Coordinator for Health Information Technology. *2015 Edition Final Rule: Expanding Electronic Health Information Access and Exchange*. Available at: <https://www.healthit.gov/sites/default/files/playbook/pdf/2015-edition-final-rule.pdf>.
- 20 Office of the National Coordinator for Health Information Technology. *2018 Report to Congress: Annual Update on the Adoption of a Nationwide System for the Electronic Use and Exchange of Health Information*. December 2018. Available at: <https://www.healthit.gov/sites/default/files/page/2018-12/2018-HITECH-report-to-congress.pdf>.
- 21 Office of the National Coordinator for Health Information Technology. *Health IT Playbook*. Available at: <https://www.healthit.gov/playbook/certified-health-it/#section-2-3>.
- 22 Federal Register. *Centers for Medicare and Medicaid Services FY 2019 IPPS Final Rule*. Available at: <https://www.govinfo.gov/content/pkg/FR-2018-08-17/pdf/2018-16766.pdf>.
- 23 Federal Register. *Centers for Medicare and Medicaid Services 2019 Physician Fee Schedule (PFS) and the Quality Payment Program (QPP)*. Available at: <https://s3.amazonaws.com/public-inspection.federalregister.gov/2018-24170.pdf>.
- 24 Centers for Medicare and Medicaid Services. *Medicaid Eligible Professionals Promoting Interoperability Program Stage 3 Objectives and Measures for 2018 Table of Contents*. 2018. Available at: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/TableofContents_EP_Medicaid_Stage3_2018.pdf.
- 25 Centers for Medicare and Medicaid Services. *Stage 3 Eligible Hospitals, Critical Access Hospitals, and Dual-Eligible Hospitals Attesting to CMS Health Information Exchange Fact Sheet*. Available at: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/HealthInformationExchange_2017.pdf.
- 26 Commonwealth Health Alliance. Available at: <https://www.commonwealthalliance.org/>.
- 27 The Sequoia Project. Available at: <https://sequoiaproject.org/>.
- 28 CARIN Alliance. Available at: <https://www.carinalliance.com/>.
- 29 Integrating the Healthcare Enterprise. Available at: <https://www.ihe.net/>.
- 30 Strategic Health Information Exchange Collaborative. Available at: <https://strategie.com/>.
- 31 Julia Adler-Milstein, Sunny C. Lin, and Ashish K. Jha. "The Number Of Health Information Exchange Efforts Is Declining. Leaving The Viability Of Broad Clinical Data Exchange Uncertain." *Health Affairs* Vol. 35 No. 7: July 2016. Available at: <https://doi.org/10.1377/hlthaff.2015.1439>
- 32 Surescripts. Available at: <https://surescripts.com/>.
- 33 Donald Rucker. "APIs: A Path to Putting Patients at the Center." *Health IT Buzz*, April 2018. Available at: <https://www.healthit.gov/buzz-blog/interoperability/apis-path-putting-patients-center>.
- 34 HL7. *The Argonaut Project: Accelerating FHIR*. Available at: https://www.hl7.org/documentcenter/public_temp_9EC7C298-1C23-BA17-0C06ED0AFB2C82E8/calendarofevents/himss/2018/The%20Argonaut%20Project%20and%20HL7%20FHIR.pdf.
- 35 SMART Health IT. *What is SMART?* Available at: <https://smarthealthit.org/an-app-platform-for-healthcare/about/>.
- 36 SMART Health IT. *SMART on FHIR*. Available at: <http://docs.smarthealthit.org/>.
- 37 Apple. *Empower your patients with Health Records on iPhone*. Available at: <https://www.apple.com/healthcare/health-records/>.
- 38 HL7. *About the DaVinci Project*. Available at: <http://www.hl7.org/about/davinci/index.cfm>.
- 39 Janet Marchibroda. *Health Policy Brief: Interoperability*. Health Affairs and Robert Wood Johnson Foundation. August 11, 2014. Available at: https://www.healthaffairs.org/doi/10.1377/hpb20140811761828/listitem/healthpolicybrief_122.pdf.
- 40 Julia Adler-Milstein, Anjali Garg, and Anna Vantsevich. *Advancing Interoperability in the United States: a report prepared for the Healthcare Leadership Council and the Bipartisan Policy Center based on interviews with more than 50 individuals*. 2018. School of Medicine, University of California, San Francisco.

- 41 Julia Adler-Milstein, Anjali Garg, and Anna Vantsevich. *Advancing Interoperability in the United States: a report prepared for the Healthcare Leadership Council and the Bipartisan Policy Center based on interviews with more than 50 individuals*. 2018. School of Medicine, University of California, San Francisco.
- 42 H.H. Pham, A.S. O'Malley, P. Bach, C. Saiontz-Martinez, and D. Schrag. "Primary Care Physicians' Links to Other Physicians Through Medicare Patients: the Scope of Care Coordination." *Ann Intern Med.* 2009;150(4):236-42.
- 43 M. Viswanathan, CE Golin, CD Jones, M. Ashok, S.J. Blalock, R.C. Wines et al. "Interventions to Improve Adherence to Self-administered Medications for Chronic Diseases in the United States: A Systematic Review." *Ann Intern Med.*;157:785-795. doi: 10.7326/0003-4819-157-11-201212040-00538
- 44 42 U.S. Code § 300j-52.
- 45 Robert Wood Johnson Foundation. *What We're Learning: Engaging Patients Improves Health and Health Care* (Issue Brief No. 3). March 2014. Available at: https://www.rwjf.org/content/dam/farm/reports/issue_briefs/2014/rwjf411217.
- 46 National Quality Forum, Interoperability Committee. *A Measurement Framework to Assess Nationwide Progress Related to Interoperable Health Information Exchange to Support the National Quality Strategy*. 2014. Available at: https://www.qualityforum.org/Publications/2017/09/Interoperability_2016-2017_Final_Report.aspx.
- 47 Yuriy Pylpuchuk, Christian Johnson, JaWanna Henry, and Diana Ciricean. "Variation in Interoperability among U.S. Non-federal Acute Care Hospitals in 2017." *ONC Data Brief*, no.42. Office of the National Coordinator for Health Information Technology. November 2018. Available at: https://www.healthit.gov/sites/default/files/page/2018-11/Interop%20variation_0.pdf.
- 48 Eric Jamoom and Ninee Yang. "State Variation in Electronic Sharing of Information in Physician Offices: United States, 2015." *NCHS Data Brief*, No. 261. Centers for Disease Control and Prevention, National Center for Health Statistics. Available at: <https://www.cdc.gov/nchs/products/databriefs/db261.htm>.
- 49 Vaishali Patel and Christian Johnson. "Individuals' Use of Online Medical Records and Technology for Health Needs." *ONC Data Brief*, No. 40. Office of the National Coordinator for Health Information Technology. Available at: <https://www.healthit.gov/sites/default/files/page/2018-03/HINTS-2017-Consumer-Data-Brief-3.21.18.pdf>.
- 50 Carla S. Alvarado, Kathleen Zook, and JaWanna Henry. "Electronic Health Record Adoption and Interoperability Among U.S. Skilled Nursing Facilities in 2015." *ONC Data Brief*, No. 39. Available at: <https://www.healthit.gov/sites/default/files/electronic-health-record-adoption-and-interoperability-among-u.s.-skilled-nursing-facilities-in-2016.pdf>.
- 51 Matthew Swain and Vaishali Patel. "Patient Access to Test Results Among Clinical Laboratories." *ONC Data Brief*, No. 13. February 2014. Available at: <https://www.healthit.gov/sites/default/files/nc-data-brief-13-labsurveydatabrief.pdf>.
- 52 Julia Adler-Milstein, Anjali Garg, and Anna Vantsevich. *Advancing Interoperability in the United States: a report prepared for the Healthcare Leadership Council and the Bipartisan Policy Center based on interviews with more than 50 individuals*. 2018. School of Medicine, University of California, San Francisco.
- 53 Office of the National Coordinator for Health Information Technology. *2018 Report to Congress: Annual Update on the Adoption of a Nationwide System for the Electronic Use and Exchange of Health Information*. December 2018. Available at: <https://www.healthit.gov/sites/default/files/page/2018-12/2018-HITECH-report-to-congress.pdf>.
- 54 Yuriy Pylpuchuk, Christian Johnson, JaWanna Henry, and Diana Ciricean. "Variation in Interoperability among U.S. Non-federal Acute Care Hospitals in 2017." *ONC Data Brief*, no.42. Office of the National Coordinator for Health Information Technology. November 2018. Available at: https://www.healthit.gov/sites/default/files/page/2018-11/Interop%20variation_0.pdf.
- 55 Julia Adler-Milstein, Anjali Garg, and Anna Vantsevich. *Advancing Interoperability in the United States: a report prepared for the Healthcare Leadership Council and the Bipartisan Policy Center based on interviews with more than 50 individuals*. 2018. School of Medicine, University of California, San Francisco.
- 56 National Quality Forum. *Core Quality Measures Collaborative: AHIP, CMS, and NQF Partner to Promote Measure Alignment and Burden Reduction*. November 2018. Available at: <https://www.qualityforum.org/cqmc/>.
- 57 Peter Pronovost et al. Eds. *Procuring Interoperability: Achieving High-Quality, Connected, and Person-Centered Care*. Washington, DC: National Academy of Medicine Available at: https://nam.edu/wp-content/uploads/2018/10/Procuring-Interoperability_web.pdf.
- 58 Office of the National Coordinator for Health Information Technology. *EHR Contracts Untangled: Selecting Wisely, Negotiating Terms, and Understanding the Fine Print*. 2016. Available at: https://www.healthit.gov/sites/default/files/EHR_Contracts_Untangled.pdf.

- 59 Genevieve Morris et al. *Patient Identification and Matching Final Report*. February 7, 2014. Available at: https://www.healthit.gov/sites/default/files/patient_identification_matching_final_report.pdf.
- 60 The Pew Charitable Trusts. *Enhanced Patient Matching is Critical to Achieving Full Promise of Digital Records*. October 2018. Available at: https://www.pewtrusts.org/media/assets/2018/09/healthit_enhancedpatientmatching_report_final.pdf.
- 61 Department of Defense and Labor, Health and Human Services, and Education Appropriations Act, 2019 and Continuing Appropriations Act, 2019, Pub L. No. 115-245 § 510 (2018).
- 62 21st Century Cures Act, Pub. L. No. 114-255, § 4002, 130 Stat. 1033 (2016), 386.
- 63 Rob Snelick. *Conformance Testing of Healthcare Data Exchange Standards for EHR Certification*. 2015. Available at: <https://pdfs.semanticscholar.org/703b/45b03b979bd180e96bf5df07dd6b9d89e17.pdf>.
- 64 Office of the National Coordinator for Health Information Technology. *Health IT Certification Program Overview*. 2016. Available at: https://www.healthit.gov/sites/default/files/PUBLICHealthITCertificationProgramOverview_v1.1.pdf.
- 65 Office of the National Coordinator for Health Information Technology. *2015 Health Information Technology (Health IT) Certification Criteria, Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications Final Rule*. Available at: https://www.healthit.gov/sites/default/files/factsheet_draft_2015-10-06.pdf.
- 66 Federal Register. *Centers for Medicare and Medicaid Services FY 2019 IPPS Final Rule*. Available at: <https://www.govinfo.gov/content/pkg/FR-2018-08-17/pdf/2018-16766.pdf>.
- 67 Federal Register. *Centers for Medicare and Medicaid Services 2019 Physician Fee Schedule (PFS) and the Quality Payment Program (QPP)*. Available at: <https://s3.amazonaws.com/public-inspection.federalregister.gov/2018-24170.pdf>.
- 68 Julia Adler-Milstein, Anjali Garg, and Anna Vantsevich. *Advancing Interoperability in the United States: a report prepared for the Healthcare Leadership Council and the Bipartisan Policy Center based on interviews with more than 50 individuals*. 2018. School of Medicine, University of California, San Francisco.
- 69 Vaishali Patel and Christian Johnson. "Individuals' Use of Online Medical Records and Technology for Health Needs." *ONC Data Brief*, No. 40. Office of the National Coordinator for Health Information Technology. Available at: <https://www.healthit.gov/sites/default/files/page/2018-03/HINTS-2017-Consumer-Data-Brief-3.21.18.pdf>.
- 70 Federal Trade Commission. *Federal Regulators Issue Final Model Privacy Notice Form*. November 17, 2009. Available at: <https://www.ftc.gov/news-events/press-releases/2009/11/federal-regulators-issue-final-model-privacy-notice-form>.
- 71 Department of Health and Human Services. *HIPAA Administrative Simplification Regulation Text*. 2013. Available at: <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf>.
- 72 Department of Health and Human Services Office of Civil Rights. *Request for Information on Modifying HIPAA Rules To Improve Coordinated Care*. December 14, 2018. Available at: <https://www.federalregister.gov/documents/2018/12/14/2018-27162/request-for-information-on-modifying-hipaa-rules-to-improve-coordinated-care>.
- 73 Department of Health and Human Services. *HHS Seeks Public Input on Improving Care Coordination and Reducing the Regulatory Burdens of the HIPAA Rules*. December 12, 2018. Available at: <https://www.hhs.gov/about/news/2018/12/12/hhs-seeks-public-input-improving-care-coordination-and-reducing-regulatory-burdens-hipaa-rules.html>.



The Bipartisan Policy Center is a non-profit organization that combines the best ideas from both parties to promote health, security, and opportunity for all Americans. BPC drives principled and politically viable policy solutions through the power of rigorous analysis, painstaking negotiation, and aggressive advocacy.

bipartisanpolicy.org | 202-204-2400
1225 Eye Street NW, Suite 1000
Washington, D.C. 20005

 @BPC_Bipartisan
 facebook.com/BipartisanPolicyCenter
 instagram.com/BPC_Bipartisan



The Healthcare Leadership Council (HLC), a coalition of chief executives from all disciplines within American healthcare, is the exclusive forum for the nation's healthcare leaders to jointly develop policies, plans, and programs to achieve their vision of a 21st century system that makes affordable, high-quality care accessible to all Americans.

hlc.org | 202-452-8700
750 9th Street NW, Suite 500
Washington, D.C. 20001

 @healthinfocus
 @HealthcareLeadershipCouncil



1225 Eye Street NW, Suite 1000 | Washington, D.C. 20005
202-204-2400 | bipartisanpolicy.org



750 9th Street NW, Suite 500 | Washington, D.C. 20001
202-452-8700 | hlc.org

[Whereupon, at 11:29 a.m., the hearing was adjourned.]

