

**IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF GEORGIA
MACON DIVISION**

**UNITED STATES OF AMERICA, ex rel.
ALEX PERMENTER,
ERIC RODIGHIERO, and
CHRIS WHEELER,**

Plaintiffs,

V.

eCLINICALWORKS, LLC,

Defendant.

CIVIL ACTION NO. 5:18-cv-382 (MTT)

ORDER*

This case involves a claim brought under the False Claims Act (“FCA”) against eClinicalWorks LLC (“eCW”), a company that develops electronic health record (“EHR”) software. Docs. 17; 216-2 ¶¶ 1-3; 266-1 ¶¶ 1-3. The plaintiffs, or Relators in FCA parlance, allege two theories of recovery for their claim. First, they claim eCW fraudulently obtained federal certification of its EHR software. Doc. 17 ¶¶ 115-129. That false certification assured healthcare providers that the software they purchased from eCW qualified for Medicare financial incentives. Docs. 216-2 ¶¶ 116, 184; 218-22 at 13; 266-1 ¶¶ 116, 184. But because of eCW’s alleged fraud, Relators claim those providers submitted false claims and provided false certifications to the Centers for Medicare & Medicaid Services (“CMS”) to obtain those incentives. Docs. 17 ¶¶ 115-157, 161-167; 266 at 28-32. Second, Relators allege that eCW’s EHR software does not comply with Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)

* The Clerk is **DIRECTED** to docket the redacted version of this order on the public docket and to file an unredacted version restricted to court users and case participants. The highlighted portions of the unredacted order represent the redactions on the public docket.

“security regulations.” Doc. 17 ¶¶ 107-114. Relators allege providers submitting claims for payments to CMS must certify that they have complied with those regulations; because eCW’s software did not comply with HIPAA security regulations, Relators claim “each and every claim submitted for government payment by a provider using eCW’s EHR software is a false claim, which ECW caused the provider to submit.” *Id.* ¶ 114.

eCW has moved for summary judgment. Docs. 215; 216-1. For the following reasons, eCW’s motion for summary judgment (Doc. 215) is **DENIED** in part and **GRANTED** in part.

I. BACKGROUND¹

A. eClinicalWorks and the Relators

eCW is a family-owned company established in 1999 to digitize medical records for physicians and hospitals. Docs. 216-2 ¶ 1; 266-1 ¶ 1; 266-2 ¶¶ 1-3; 300-9 ¶¶ 1-3. Over the past two decades, eCW has become one of the largest providers of EHR software in the United States; more than 180,000 providers and nearly a million medical professionals rely on eCW software to manage patient records, facilitate clinical workflows, and ensure compliance with various federal healthcare regulations. Docs. 216-2 ¶¶ 4-5; 266-1 ¶¶ 4-5; 266-2 ¶¶ 3-6; 300-9 ¶¶ 3-6. Initially, eCW’s EHR software was a desktop application installed on local computers utilizing customer servers. Docs. 216-2 ¶¶ 7-8; 218-2 at 172:3-173:17; 266-1 ¶¶ 7-8. eCW has since developed a cloud-based application hosted on remote servers maintained by eCW, which most providers now utilize. Docs. 216-2 ¶¶ 6, 8-10, 12; 266-1 ¶¶ 6, 8-10, 12; 266-2 ¶ 8; 300-9 ¶ 8. eCW handles the network operating system, infrastructure, disaster recovery,

¹ Unless otherwise stated, these facts are undisputed and are viewed in the light most favorable to the non-moving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986).

server, network, and storage for its cloud software. Docs. 216-2 ¶¶ 9, 12; 266-1 ¶¶ 9, 12; 266-2 ¶ 8; 300-9 ¶ 8.

Relators Alex Permenter, Eric Rodighiero, and Chris Wheeler are computer and information technology specialists. Docs. 17 ¶¶ 9-11; 62-1 ¶¶ 3-8; 216-2 ¶ 28; 266-1 ¶ 28. Relators' company, Tier2Technologies (formerly Alex's PC Solutions), provides IT, telecom, and web services to approximately 200 medical providers, most of whom use eCW software. Docs. 62-1 ¶¶ 4, 8-11; 216-2 ¶¶ 28-30; 266-1 ¶¶ 28-30. Relators have worked with various versions of eCW software since at least 2011 and provide technical support to medical practices that use the software. Docs. 62-1 ¶¶ 10-11; 216-2 ¶¶ 29-31; 266-1 ¶¶ 29-31; 266-81 ¶ 3.

B. Relators' Theories of Recovery

Relators assert two theories to support their claim. Their first theory, which is relatively narrow, alleges that eCW falsely represented that its software complied with certification requirements set by the Office of the National Coordinator for Health Information Technology ("ONC").² Doc. 17 ¶¶ 115-151. Based on that representation, eCW's software was approved as Certified EHR Technology ("CEHRT").³ See Docs. 266-2 ¶ 134; 300-9 ¶ 134. eCW then marketed its software to providers who needed to use CEHRT to be eligible for federal incentive payments. Docs. 17 ¶¶ 6, 145; 216-2 ¶¶ 51-52, 87-89; 266-1 ¶¶ 51-52, 87-89; 266-63 at 17. But because eCW's software allegedly did not meet CEHRT standards, providers seeking those incentive payments

² The Office of the National Controller for Health Information Technology is now the "Assistant Secretary for Technology Policy and Office of the National Coordinator for Health Information Technology ("ASTP/ONC"). Docs. 216-2 ¶ 34; 266-1 ¶ 34.

³ The overuse of acronyms is the lesser evil in this alphabet soup regulatory scheme.

submitted false claims. Docs. 17 ¶¶ 115-157, 161-167; 266 at 3. According to Relators, that caused the government to pay, based on one estimate, incentives totaling up to \$388 million that should not have been paid. Docs. 218-108 ¶ 9; 266-2 at 67 ¶ 322.

That doesn't seem very narrow but it is *relatively* narrow because the Relators' second theory is considerably broader. Relators allege that providers "expressly and impliedly certify their compliance with the HIPAA Security Rule when they submit claims to CMS." Docs. 17 ¶¶ 107-114; 266 at 28. These certifications allegedly are found primarily in a form providers must execute before a provider can submit claims electronically for government payment. Docs. 17 ¶ 108; 17-3; 266-2 ¶ 113. Because, as Relators allege, eCW's EHR software does not comply with HIPAA security regulations, providers' certifications of compliance are false and therefore all claims submitted by those providers are false and should not have been paid. Doc. 17 ¶ 114. Relators have not presented any estimate of damages for their HIPAA theory.

C. The Regulatory Framework

1. ONC Health IT Certification Program

Enacted in 2009, the Health Information Technology for Economic & Clinical Health ("HITECH") Act sought to promote the "meaningful use" of health information technology by providing financial incentives to healthcare providers who use CEHRT. Docs. 216-2 ¶¶ 37-39, 116; 266-1 ¶¶ 37-39, 116; 266-2 ¶¶ 57-63; 300-9 ¶¶ 57-63. Although developers are not required to obtain certification of their software, they do because uncertified EHR software is not "broadly marketable"—providers must use

CEHRT to participate in federal incentive programs administered by CMS.⁴ Docs. 266-2 ¶ 63; 266-14 at 102:6-12; 300-9 ¶ 63. The ONC defines the technical criteria for certification.⁵ Docs. 216-2 ¶¶ 39-41, 116; 266-1 ¶¶ 39-41, 116; 266-2 ¶ 64; 300-9 ¶ 64. ONC's third iteration of certification criteria, the 2015 Certification Edition, is relevant here, *see* 45 C.F.R. § 170.315. These criteria ensure specific standards for functionality, security, and interoperability. It is important to note that ONC certification is distinct from HIPAA, although some certification criteria address concerns also addressed by HIPAA. Docs. 216-2 ¶¶ 136-138; 266-1 ¶¶ 136-138.

Before ONC's 2015 Certification Edition, the certification process involved testing each certification criterion against a set of predefined standards and ONC test scripts. Docs. 266-2 ¶¶ 65, 67; 300-9 ¶¶ 65, 67. Additionally, "[i]f the criteria remained unchanged between versions and the software was unchanged, [ONC] allowed new editions of the software to be certified through 'gap' or 'inherited' certification whereby the developer attested that it had previously been tested and the software still met the applicable criteria." Docs. 266-2 ¶ 66; 300-9 ¶ 66; *see* Docs. 216-2 ¶¶ 55-56; 266-1 ¶¶ 55-56. For the 2015 Certification Edition, certain criteria moved to "attestation" only, meaning the developer certifies that its software meets requirements rather than undergoing formal testing. Docs. 266-2 ¶¶ 68-71; 300-9 ¶¶ 68-71.

⁴ eCW claims this is disputed. Doc. 300-9 ¶ 63. According to eCW, "[c]linicians are free to use non-certified software, including if they participate in federal health care programs ... given the exemptions and exceptions available to clinicians in certain enumerated categories," which may, among other things, justify the failure to use CEHRT. *Id.* (citing Doc. 218-107 ¶ 27).

⁵ ASTP/ONC provides clarifications to certification criteria through Certification Companion Guides designed to assist with health IT product development and Certification Program conformance. *See* <https://www.healthit.gov/topic/certification-ehrs/certification-health-it> (last visited May 8, 2025).

The ONC relies on independent third parties called Authorized Certification Bodies (“ACBs”) and Authorized Testing Laboratories (“ATLs”) to conduct testing, issue certifications,⁶ and engage in ongoing surveillance of CEHRT.⁷ Docs. 216-2 ¶¶ 42-47, 62-64; 266-1 ¶¶ 42-47, 62-64. Since 2017, Drummond Group has been both the ONC-ACB and ONC-ATL for eCW. Docs. 216-2 ¶ 48; 266-1 ¶ 48. Developers must submit quarterly attestations of any changes affecting certification, maintain records of complaints, and implement corrective action plans to address nonconformities.⁸ See, e.g., Docs. 216-2 ¶¶ 61, 65, 68; 266-1 ¶¶ 61, 65, 68.

Version 11 of eCW’s software is at issue here. Docs. 216-2 ¶ 69; 266-1 ¶ 69. From December 28, 2017 to December 28, 2021, Version 11 was eCW’s only relevant software certified under the ONC’s 2015 Certification Standards, 45 C.F.R. § 170.315. Docs. 266-2 ¶ 133; 300-9 ¶ 133.

2. Merit-Based Incentive Payment System

The Meaningful Use program was officially established by CMS in 2011 pursuant to the American Recovery and Reinvestment Act of 2009 to encourage providers to

⁶ For self-attestation, the ONC-ACB verifies the “health IT developer has attested conformance” and must accept developer “self-attestations.” Docs. 266-2 ¶¶ 70-71; 300-9 ¶¶ 70-71; see also Docs. 216-2 ¶ 61; 266-1 ¶ 61; 266-48 at 1 (“Developer self-declaration should be based on self-evaluation of product’s functionality and its conformance to certification requirements.”).

⁷ This includes receiving and assessing complaints, conducting periodic reviews, and ensuring compliance with any changes in the criteria. Docs. 216-2 ¶¶ 43-44, 64-68; 266-1 ¶¶ 43-44, 64-68. If a non-conformity is identified, the developer must submit a corrective action plan to address the issue. Docs. 216-2 ¶ 68; 266-1 ¶ 68. The ONC and/or ONC-ACB then work with developers to bring the software back into compliance. Docs. 216-2 ¶¶ 68, 172-75; 266-1 ¶¶ 68, 172-75. The ONC also has the authority to conduct direct reviews of certified health IT developers and their products. Docs. 216-2 ¶ 50; 266-1 ¶ 50. This can include suspending or terminating a certification if necessary. Docs. 216-2 ¶¶ 50, 171, 176; 266-1 ¶¶ 50, 171, 176. However, if an issue falls outside the scope of the certification criteria, “there would be no program-related connection” and ONC would not act. Docs. 266-2 ¶ 87; 300-9 ¶ 87.

⁸ “Relators dispute that eCW provides attestations to Drummond that ‘identify potential certification issues and remediations steps.’” Doc. 266-1 ¶ 65.

adopt and demonstrate meaningful use of CEHRT.⁹ Docs. 216-2 ¶¶ 104-105; 266-1 ¶¶ 104-105; see *also* 42 C.F.R. § 495.2. Healthcare providers who adopted CEHRT and demonstrated meaningful use were eligible for financial incentives. Docs. 216-2 ¶¶ 104-105; 218-22 at 9-10; 266-1 ¶¶ 104-105. Conversely, providers who failed to meet meaningful use requirements faced penalties, including reduced Medicare and Medicaid reimbursements. 42 C.F.R. §§ 495.2(g). With the introduction of the Medicare Access and CHIP Reauthorization Act, the Medicare EHR Incentive Program—commonly called Meaningful Use—became part of the “Promoting Interoperability” category, one of four components, under the new Merit-Based Incentive Payment System (“MIPS”).¹⁰ Docs. 216-2 ¶ 113; 266-1 ¶ 113; see Promoting Interoperability, Dep’t of Health & Human Servs. (ONC-ASTP), <https://www.healthit.gov/topic/meaningful-use-and-macra/promoting-interoperability> (last visited June 18, 2025) (“In MIPS, the Promoting Interoperability category focuses on meaningful use of certified EHR technology.”).

MIPS measures clinician performance across four categories: quality, improvement activities, cost, and promoting interoperability. Docs. 216-2 ¶ 115; 266-1 ¶ 115. Promoting interoperability, the category relevant here, addresses the use of technology to exchange and make use of information. Docs. 216-2 ¶ 117; 266-1 ¶ 117. Final MIPS scores determine the payment adjustments that clinicians receive for their

⁹ The Meaningful Use program evolved in three stages. Docs. 216-2 ¶ 109; 266-1 ¶ 109. Stage one (2011-2012) focused on data capture and sharing. Docs. 216-2 ¶¶ 109-10; 266-1 ¶¶ 109-10. Stage two (2014) focused on advanced clinical processes, and stage three (2016) focused on improved outcomes. Docs. 216-2 ¶¶ 109-12; 266-1 ¶¶ 109-12. The incentive payments continued under Medicare through 2016. Docs. 216-2 ¶ 107; 266-1 ¶ 107.

¹⁰ MIPS consolidates multiple quality programs, including Meaningful Use, the Physician Quality Reporting System, and Value-Based Payment Modifiers, into a single program to improve quality care. Docs. 216-2 ¶¶ 119-120; 266-1 ¶¶ 119-120.

treatment of Medicare patients. Docs. 216-2 ¶ 124; 266-1 ¶¶ 124. These adjustments can be positive or negative, based on the clinician's final score compared to a performance threshold established by CMS.¹¹ Docs. 216-2 ¶¶ 124-26; 266-1 ¶¶ 124-26; see, e.g., Doc. 218-156 at 63-65. To earn points for promoting interoperability, which makes up 25% to 30% of the total MIPS score, providers must attest to the use of CEHRT. Docs. 216-2 ¶¶ 115-116, 126; 266-1 ¶¶ 115-116, 126. “A physician with a zero score in the MIPS Promoting Interoperability performance category would not be eligible to receive a positive payment adjustment, and to avoid a negative payment adjustment would need to attain the maximum scores in the other performance categories.” Doc. 218-22 at 13; see Docs. 216-2 ¶ 127; 266-1 ¶ 127.

3. *Health Insurance Portability and Accountability Act of 1996*

The HIPAA Security Rule¹² establishes national standards to protect electronic personal health information (“ePHI”) that is created, received, used, or maintained by a covered entity.¹³ Docs. 216-2 ¶ 130; 266-1 ¶ 130. The Department of Health and Human Services Office for Civil Rights (“OCR”) is responsible for enforcing compliance with the HIPAA Privacy, Security, and Breach Notification Rules. Docs. 216-2 ¶ 129;

¹¹ “[S]ince the 2021 MIPS performance period, the threshold that determines whether a physician gets a positive or negative payment adjustment is a MIPS final score of 75 points.” Docs. 216-2 ¶ 125; 266 at 16, 34, 41; 266-1 ¶ 125.

¹² HIPAA security regulations for ePHI are commonly referred to as the HIPAA Security Rule. See <https://www.hhs.gov/hipaa/for-professionals/security/index.html> (last visited May 7, 2025). The amended complaint uses “security regulations,” but the parties’ briefs use HIPAA Security Rule. See, e.g., Doc. 17 ¶¶ 110, 111. The Court follows their lead. The Security Rule is found at 45 C.F.R. Part 160, and Subparts A and C of Part 164.

¹³ A “covered entity” includes physicians and other health care providers who transmit health information in electronic form in connection with covered transactions, as well as health plans and health care clearinghouses. 45 C.F.R. §§ 160.102 and 160.103. HIPAA also applies to business associates of covered entities who perform functions on behalf of these entities, e.g., EHR vendors and their customers. See *id.* at §§ 160.102 and 160.103.

266-1 ¶ 129. The Security Rule requires covered entities, among other things, to “[p]rotect against any reasonably anticipated threats or hazards to the security or integrity” of electronic PHI” and to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI. 45 C.F.R. §§ 164.306, 164.308; 164.310; 164.312.

Providers must sign an Electronic Data Interchange (“EDI”) Enrollment Agreement to submit Medicare claims for payment to CMS. Docs. 216-2 ¶¶ 145-48; 266-1 ¶¶ 145-48. The agreement states: “The provider agrees to ... use sufficient security procedures (including compliance with all provisions of the HIPAA security regulations) to ensure that all transmissions of documents are authorized and protect all beneficiary-specific data from improper access.” Docs. 17-3 at 14-15; 266-2 ¶ 114; 300-9 ¶ 114.

D. The *Delaney* Settlement

In 2017, eCW settled an FCA lawsuit that alleged that an earlier version of eCW’s software failed to meet the certification criteria of earlier ONC certification editions. *United States ex rel. Delaney v. eClinicalWorks, LLC*, No. 2:15-cv-95, Doc. 1 ¶¶ 63-107 (D. Vt. May 1, 2015); see Docs. 216-2 ¶¶ 197-98, 200-08; 266-1 ¶¶ 197-98, 200-08. As part of the settlement, eCW entered a five-year Corporate Integrity Agreement (“CIA”) with the government on May 30, 2017, and agreed to pay approximately \$155 million. Docs. 216-2 ¶¶ 205-19; 266-1 ¶¶ 205-219. The CIA required eCW to implement various compliance measures, report certain events to the Office of Inspector General of the U.S. Department of Health and Human Services (“OIG”), and hire an independent software quality oversight organization (“SQOO”) approved by OIG. Docs. 216-2 ¶¶

209-219; 266-1 ¶¶ 209-219. SQOO was tasked, among other things, to ensure that eCW's EHR software complied with applicable ONC certification criteria. Docs. 216-2 ¶¶ 218-20; 266-1 ¶¶ 218-20.

E. Alleged Flaws and Vulnerabilities in eCW's Software

While attempting to fix problems in their customers' software in 2018, Relators claim they discovered significant flaws in eCW's software.¹⁴ *E.g.*, Docs. 17 ¶¶ 23, 121-129; 218-7 ¶¶ 27-32; 218-8 at 30:3-25. Using only unencrypted source code eCW left on its customers' servers, Relators allegedly discovered that an unauthorized user could access and change PHI without entering a username or password. Docs. 218-7 ¶¶ 27-30; 218-104 at 9, 12-14; 266 at 3, 12; see *also* Doc. 266-2 ¶¶ 139-151. Minimum access users could change their access levels and, for example, make themselves practice administrators. Docs. 218-104 at 24, 30; 218-134 at 12-13, 17-20, 23, 29-30, 55-57, 59, 67-69. Users could bypass the eCW application entirely, meaning their activities would not be recorded in the audit logs. Doc. 218-104 at 63. eCW stored various authentication credentials in plain text in its source code, and a vulnerability in the internal EHR fax function allowed complete access to PHI without proper user verification.¹⁵ See, *e.g.*, Doc. 218-7 at 11-12.

¹⁴ Relators claim the flaws they discovered are distinct from the deficiencies raised in *Delaney*. See, *e.g.*, Doc. 266-2 ¶ 257.

¹⁵ [REDACTED]

[REDACTED]

eCW does not seek rulings that specific alleged flaws do not exist. Of course, eCW does not concede that its software is flawed, but its motion attacks Relators' claims at a higher level. Thus, it is not necessary to venture into the weeds of every alleged flaw, and the Court provides here only illustrative examples.

1. Insecure authentication and access controls

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

16 [REDACTED]

2. *Weak cryptographic and password security*

Relators have evidence that eCW relies on unsalted MD5, a hashing algorithm “deprecated” by the National Institute of Standards and Technology (“NIST”) due to known vulnerabilities.¹⁷ Docs. 218-104 at 33, 36, 65, 72-73, 80-81, 84, 89-90; 266-87 ¶¶ 43-60; see Doc. 17 ¶ 65 & n.14 (“[NIST] does not include MD5 on its list of recommended hashes for password storage.”); 218-67 at 288-292. MD5 is prone to “collision attacks,” where different inputs produce the same hash, and can be cracked rapidly with modern computing power, e.g., using precomputed tables or brute force. Docs. 218-104 at 13-14, 56-57, 60-61; 218-137 at 8-9; 266-52 at 38-39. Relators claim they decrypted 50% of user password hashes within 20 seconds. See Docs. 17 ¶ 68; 218-104 at 14.

¹⁷ See William E. Burr, Cryptographic Hash Standards – Where Do We Go From Here?, IEEE Security & Privacy, Vol. 4, No. 2 (Apr. 1, 2006), <https://www.nist.gov/publications/cryptographic-hash-standards-where-do-we-go-here> (“[T]wo ... commonly used cryptographic hash functions, MD5 and SHA-1, have been successfully attacked ... it is no longer advisable to use them in some applications. although other applications are not affected.”).

3. Server misconfiguration: SQL injection¹⁸ and other vulnerabilities

[illegible]

¹⁸ SQL Injection is a security flaw that occurs when an application allows unfiltered input to interfere with SQL queries made to a database. Docs. 266-15 at 6; 218-102 ¶ 146 (“[A] SQL injection attack is when someone can modify the query request of a database to be able to access information that they should not have access to.”).

19 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

20 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4. *Unencrypted local storage of PHI*

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

F. Timeline of Events

Relators filed their lawsuit on October 16, 2018, approximately 18 months after the *Delaney* settlement and the commencement of the CIA. Docs. 3; 266-97; see Docs. 216-2 ¶¶ 205-09; 266-1 ¶¶ 205-29; 266-2 ¶ 258; 300-9 ¶ 258. Evidence of events occurring before and after the *Delaney* settlement may or may not be admissible at trial. That evidence is, however, relevant to issues raised by eCW's motion for summary judgment.²²

1. *Pre-CIA period; known security vulnerabilities*

Before entering the CIA, eCW was allegedly aware of various security vulnerabilities in its software. For example, eCW intentionally configured its EHR to store local copies of unencrypted diagnostic tests to resolve a software bug in an eCW workflow.²³ Docs. 218-5 at 223:12-224:8, 226:3-24; 266-2 ¶¶ 194-96, 198; 300-9 ¶¶ 194-96, 198; see Doc. 218-134 at 56-58, 71, 73-74. This practice was in place from

²² Here again, eCW does not necessarily agree that these facts are undisputed. The Court does not find that they are.

²³ Specifically, "there was a software bug in the eCW workflow that was causing problems in the upload process" of ████████ EKGs, so "the company," meaning eCW, "made a decision that they were going to allow versions of EKGs to be stored locally on the computers that were running eClinicalWorks in the EKG testing rooms," which were "stored unencrypted on those devices." Doc. 218-5 at 224:9-24, 227:3-9. One of eCW's 30(b)(6) witnesses testified that this decision was a "temporary" fix. Doc. 218-5 at 222:17-22, 227:16-18; see Docs. 266-2 ¶¶ 194, 199; 300-9 ¶¶ 194, 199. However, it is undisputed that "[Relator] Wheeler has been working with eCW since 2010 and knew that the software created these backups since at least then." Docs. 266-2 ¶ 199; 300-9 ¶ 199.

2010 until mid-to-late 2021 when it was fixed by eCW, allegedly in response to Relators' revelation of the flaw. Docs. 266 at 12; 266-2 ¶ 199; 300-9 ¶ 199; see Doc. 266-83 at 6. For another example, many of the misconfigured .jsp files identified by Relators were included on a list of sessionless .jsp files maintained by eCW as early as 2012. *Compare, e.g.*, Docs. 218-110; 266-69. In 2016, an eCW employee reported that some of these files returned sensitive information such as credentials to eCW's file transfer protocol ("FTP") server. Doc. 266-74. An eCW programmer also asked eCW's head of Application Security ("AppSec"), Rahul Jaiswal, if the use of sessionless .jsp files could be a major issue.²⁴ Docs. 266-76; 266-2 ¶ 159; 300-9 ¶ 159. However, at least some sessionless .jsp files continued to return sensitive data, such as administrator usernames and their password complexity requirements, until at least 2021. *See, e.g.*, Doc. 218-137 at 7.

Finally, while settling *Delaney*, eCW was preparing to seek certification of Version 11. Docs. 218-20 at 63:9-21; 266-2 ¶ 128; 300-9 ¶ 128. During this time, and throughout the CIA, eCW allegedly was alerted to various security flaws by employees and external penetration testing. Docs. 266-51 at 7; 266-52 at 2-4; 322-3; 322-4 at 7, 13, 15. These flaws included, among other things, a privilege escalation flaw that let attackers manipulate HTTP responses to impersonate other users, and a lack of proper

²⁴ eCW's AppSec team was established in 2015 and "is responsible for scanning eCW's code for vulnerabilities and identifying issues, which are then documented and reported to development." Docs. 218-59 at 47; 266-2 ¶ 39; 300-9 ¶ 39. "[T]he AppSec team does not actually write code or fix the code if there is a security issue. Docs. 266-2 ¶ 49; 300-9 ¶ 49; see Doc. 218-59 at 47. The team also works with other departments to get the software recertified "from a functional point of view and make sure that patches get deployed." Doc. 218-59 at 47-48 ("[The] group does not currently develop test scripts related to software security, but they do work with [Quality Assurance] to review their scripts and work with development to fix any flaws identified.").

server-side validation.²⁵ Docs. 266-51 at 2; 266-52 at 2-4, 51; 322-3; 322-4 at 7, 15; see Doc. 270-7 at 20. There is no evidence that eCW shared this information with ONC or its ONC-ACB prior to obtaining certification for Version 11 of its software.

2. Initial SQOO assessments and findings

As required by the CIA, eCW retained Quandary Peak Research as SQOO to oversee its compliance under the CIA.²⁶ Docs. 216-2 ¶¶ 214-15; 266-1 ¶¶ 214-15. SQOO was tasked with conducting semiannual interval assessments of eCW's software, policies, and procedures, issuing recommendations, and ensuring that eCW addressed certification and patient safety issues. Docs. 216-2 ¶¶ 216-220; 266-1 ¶¶ 216-220.

On December 12, 2017, SQOO conducted an initial evaluation of eCW's policies and procedures to establish a baseline for future assessments. Doc. 218-59. This baseline assessment identified significant gaps in eCW's risk management processes, quality assurance systems, and software development practices. *Id.* at 7-11. The assessment found that eCW lacked a formal risk management plan and qualified

²⁵



²⁶ When referring to Quandary Peak in its CIA oversight role, the Court uses "SQOO." Quandary Peak had served as an Independent Consultative Expert ("ICE") during settlement negotiations in *Delaney*. Docs. 266-2 ¶ 269; 300-9 ¶ 269. The ICE Assessment identified gaps in eCW's risk management and software quality processes and recommended adopting certain standards, implementing a Quality Management System, and addressing risks preemptively. Doc. 218-42 at 5-8.

personnel to oversee compliance efforts. *Id.* It also highlighted systemic issues, such as inadequate testing processes, reliance on manual scripts, and a reactive approach to addressing errors. *Id.* at 8-9. Consequently, SQOO could not confirm whether eCW's software comprehensively met the certification requirements in real world settings.²⁷ Docs. 218-59 at 100; 270-1 at 2; see Docs. 266-2 ¶ 22; 300-9 ¶ 22. To address these issues, SQOO recommended that eCW comply with designated standards, such as International Organization for Standardization ("ISO"), to enhance software quality and reliability, implement these processes through detailed policy manuals, and improve tools like JIRA.²⁸ Doc. 218-59 at 9-11, 40, 47, 51, 57.

SQOO's first interval assessment in June 2018 noted that eCW had made some progress on its initial recommendations, such as implementing additional tests to verify mandated requirements for meaningful-use certification. Docs. 266-2 ¶¶ 285-86; 300-9 ¶¶ 285-86. However, SQOO noted that this testing was still inadequate and concluded that eCW lacked a structured approach to address the gaps identified in the baseline assessment. Docs. 218-66 at 4-8; 266-2 ¶ 287; 300-9 ¶ 287. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

²⁷ "[I]n 2017, eCW had an 'ACB testing team' that operated to prepare the EHR to pass certification testing." Docs. 266-2 ¶ 19; 300-9 ¶ 19; see Doc. 270-1 at 2. According to SQOO, "the team appear[ed] to have been tasked with passing the certification-testing process and little else." Docs. 266-2 ¶ 19; 300-9 ¶ 19 ("[W]e cannot ascertain whether [eCW's] EHR comprehensively [met] all of the certification requirements ... because eCW ha[d] done only the minimum amount of QA required to pass certification testing, ... which itself is not comprehensive.").

²⁸ JIRA is a software tool used by eCW to track changes and issues in its programming. See, e.g., Docs. 218-59 at 16, 19, 63-64, 95, 101, 106; 270-2 at 14.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] SQOO recommended that eCW employ consultants for penetration testing, catalog all known vulnerabilities, and prioritize fixing them at their source. Docs. 266-2 ¶ 289; 270-5; 300-9 ¶ 289. SQOO also recommended that eCW develop a traceability matrix to map certification criteria to test cases and scripts, which would ensure that eCW's software met certification requirements during quality assurance regression cycles. Docs. 216-2 ¶¶ 249-50; 266-1 ¶¶ 249-50.

3. Stipulated penalties; interval assessments; systemic issues

In July 2018, OIG demanded stipulated penalties because eCW failed to report patient safety risks within the CIA-mandated 48-hour window. Docs. 218-91; 216-2 ¶¶ 272-74; 266-1 ¶¶ 272-74. eCW paid a fine of \$132,500. Docs. 218-92; 216-2 ¶ 276; 218-93; 266-1 ¶ 276.

The second interval assessment in December 2018 found continuing problems. Docs. 218-62; 270-8 at 3-4, 6. SQOO concluded, among other things, that "eCW's pace of resolving security issues ha[d] been slow," that "[e]ven serious issues, such as exploitable SQL injection vulnerabilities, which eCW ha[d] been aware of for some time, ha[d] timelines of many months to correct," and that eCW needed "to develop clearer

timelines and procedures for remediation and prevention of application security issues, consistent with prior SQOO recommendations.” Docs. 218-62 at 83; 270-8 at 6; see Docs. 266-2 ¶ 290; 300-9 ¶ 290.

In April 2019, SQOO informed OIG of systemic deficiencies in eCW’s organizational culture, software development practices, and compliance efforts. Docs. 266-2 ¶ 292; 300-9 ¶ 292; see Doc. 266-25. SQOO described poor risk assessment processes, inadequate staffing, and a lack of urgency in addressing patient safety and certification issues.³⁰ Docs. 266-25 at 1-3; see Docs. 266-2 ¶¶ 293-95; 300-9 ¶¶ 293-95. SQOO claimed that eCW’s software development practices were unstable and poorly tested, leading to recurring security flaws. Doc. 266-25 at 2-3. SQOO concluded that eCW’s limited progress demonstrated a lack of coordinated, organization-wide effort to resolve these systemic problems. *Id.* at 4.

OIG issued a second demand for stipulated penalties in October 2019. Docs. 216-2 ¶ 277; 266-1 ¶ 277. OIG sought \$2,717,500 due to eCW’s alleged failure to install oversight processes, to adequately and timely respond to SQOO’s written recommendations, and to create policies and procedures to address certification issues. Docs. 86-1 at 2; 218-94. eCW negotiated additional compliance obligations instead of paying a penalty. Docs. 216-2 ¶¶ 282-83; 266-1 ¶¶ 282-83. This included the creation of a patient safety board and the hiring of directors for EHR certification compliance and quality assurance. Doc. 218-98.

³⁰ “While ... SQOO’s Systemic Issues Memo noted challenges with organizational accountability at large within eCW, the SQOO ... [ultimately] found the issue particularly prevalent within the Application Security Department.” Doc. 218-60 at 275.

4. *Response to Relators' 2018 complaint; continuing interval assessments*

Based on the allegations in Relators' October 16, 2018 complaint, the Department of Justice ("DOJ") wrote eCW outlining nine specific allegations, including unauthorized access to .jsp files, SQL injection vulnerabilities, and hardcoded cryptographic keys. Docs. 69-3 at 4; 216-2 ¶ 322; 218-110; 266-1 ¶ 322. DOJ directed eCW to "immediately address any such security vulnerabilities." Docs. 69-3 at 4-6; 218-110. eCW responded by releasing its first-ever security patch and engaging in ongoing discussions with SQOO and DOJ about its remediation efforts. Docs. 216-2 ¶¶ 324-42; 266-1 ¶¶ 324-42; 266-2 ¶¶ 241-42; 300-9 ¶¶ 241-42.

The third interval assessment, issued in June 2019, noted some progress in addressing vulnerabilities but found that eCW had provided lengthy timelines for resolution of outstanding issues.³¹ Docs. 266-2 ¶ 298; 300-9 ¶ 298; see Docs. 218-64; 270-6 at 4 ("These issues have been seen across penetration tests and need urgent correction. eCW has ... provided timelines which go out a year or more to fix all of these issues, some of which eCW has known about for several years."). According to SQOO, eCW's progress remained inconsistent, and the company had not yet addressed all issues identified in previous assessments. See, e.g., Docs. 218-64 at 243, 249; 270-6 at 4.

The fourth interval assessment was late because of eCW's efforts to edit the report before it was submitted to OIG.³² Doc. 157-15 at 74; see Docs. 218-60; 270-2.

³¹ [REDACTED]

³² On April 24, 2020, OIG notified eCW of its concerns regarding delays in the issuance of SQOO's Fourth Interval Assessment report. Doc. 157-15 at 74. OIG noted that it had reviewed correspondence between eCW and SQOO and was troubled by the tone and content of eCW's communications. *Id.* The letter

Consequently, OIG instructed SQOO to cease sending draft reports to eCW. Doc. 157-15 at 74-75. The fourth interval assessment ultimately revealed ongoing security issues and continued resistance from eCW's AppSec team. Docs. 218-60; 270-2 at 2. SQOO criticized eCW's AppSec leadership for resistance to implementation of basic security controls and a lack of urgency about security issues. Doc. 270-2 at 12. The assessment noted new issues, including the use of unsalted MD5 hashing algorithms and inadequate password policies. Docs. 266-2 ¶ 302; 300-9 ¶ 302. SQOO recommended expanded security staffing, timelines to fix vulnerabilities, and standardized password policies. Docs. 266-2 ¶ 303; 300-9 ¶ 303.

The fifth interval assessment, issued in July 2020, highlighted dangerous levels of "technical debt"³³ in eCW's software. Docs. 218-67; 270-3 at 2; see Docs. 266-2 ¶ 305; 300-9 ¶ 305. SQOO further noted that "the company appear[ed] to discourage and suppress the discussion of product flaws, project delays, and human errors" and that eCW's organizational culture discouraged transparency and accountability. Doc. 270-3 at 2, 12, 14. The assessment concluded that "**SQOO [wa]s concerned that eCW's EHR [wa]s unsafe, its progress ha[d] been far less than expected, and it [wa]s not on a trajectory that [wa]s likely to render its software reasonably safe before the end of the CIA.**" Docs. 218-67 at 7; 270-3 at 3 (emphasis in original).

made clear that under the CIA eCW had neither the right to a draft report, nor the authority to rewrite or negotiate findings, recommendations or other content of SQOO reports. *Id.*

³³ Technical debt refers to the long-term cost of taking shortcuts or making quick, easy, or suboptimal decisions in code, architecture, or design to meet short-term goals. Docs. 218-44 at 78:17-25; 270-3 at 2 ("eCW has been slow to address the dangerous levels of 'technical debt' in its software, *i.e., the accumulation of excessive complexity, poor coding practices, and violations of good architectural design.*") (emphasis added). [REDACTED]

On August 7, 2020, SQOO issued a formal “Expression of Concern”³⁴ to OIG, stating that eCW systematically failed to meet its obligations under the CIA and routinely missed deadlines or abandoned required activities altogether. Doc. 266-99. In that letter, SQOO repeated its concern that **“eCW’s EHR [wa]s unsafe, its progress ha[d] been unacceptable, and [again] it [wa]s not on a trajectory that w[ould] render its software reasonably safe before the end of the CIA.”** *Id.* at 1 (emphasis in original).

The sixth interval assessment, issued in January 2021, also reiterated these concerns and documented continuing issues with eCW’s software. Docs. 270-7, 218-72 at 19, 21, 44 (“[M]ore than three years in, the SQOO is concerned that eCW’s EHR is unsafe, its progress has been unacceptable, and it is not on a trajectory that will render its software reasonably safe before the end of the CIA.”). The assessment concluded that eCW “software [could not] and should not be considered secure, and it present[ed] significant patient safety risk related to, confidentiality, integrity and availability of their patient data.” Docs. 218-72 at 67-68; 270-7. Further, SQOO reported that eCW had “repeatedly reported inaccurate information ... to the SQOO over the course of the entire ... CIA[] which directly caused the SQOO to report inaccurate information” to OIG and ONC.³⁵ Doc. 218-72 at 268, 267-70. SQOO noted approximately ten anonymous

³⁴ The CIA required SQOO to report “concerns about action plans that are not being enforced or systemic problems that could affect eCW’s ability to prevent, detect, or remediate Patient Safety Issues or Certification Issues in the EHR.” Doc. 218-41 at 40, CIA III.E.9.d.i at 39.

³⁵ For example, based on information regularly reported to SQOO by eCW’s AppSec leadership, the fifth interval assessment indicated that issues identified in a baseline recommendation persisted for only 1.6% of identified eCW customers. Docs. 218-72 at 7, 263, 267-68; 270-7 at 3-4. As it turned out, SQOO found that the issue persisted for approximately 93% of customers. Doc. 270-7 at 15. eCW allegedly did not offer any reasonable explanation for the disparity in the information presented to SQOO. Doc. 218-72 at 7, 263, 267-70.

disclosures alleging falsification or destruction of contracts, reports, or records.³⁶ Docs. 218-72 at 27; 270-7 at 4-5.

On February 2, 2021, SQOO wrote to OIG about the falsification of documents. Doc. 266-101. SQOO investigated the anonymous disclosures and discovered during a random spot check that eCW's AppSec staff generated and delivered falsified third-party dependency reports for the months of July, August, and September 2020. *Id.* at 1-2. However, SQOO indicated that it could not adequately investigate all alleged falsification due to conflicting accounts from AppSec leadership. *Id.*

5. eCW claims "ethnic bias" and seeks new SQOO team

During eCW's administrative appeal of OIG's second demand for stipulated penalties, eCW asked OIG to fire Quandary Peak as SQOO. Doc. 266-106. eCW claimed that some SQOO team members were guilty of "ethnic bias." See Docs. 266-106; 266-107. Quandary Peak denied eCW's allegations and refused eCW's demand that it resign as SQOO. Doc. 266-108. OIG reviewed eCW's allegations and rejected eCW's request to fire Quandary Peak. Doc. 266-109. Undaunted, eCW pursued its claims directly against Quandary Peak. Quandary Peak eventually agreed to a confidential agreement to settle eCW's allegations that required Quandary Peak to replace key SQOO members, including the team leader. Doc. 266-41 at 6-12. The settlement agreement further required Quandary Peak to certify that it had not disclosed the settlement to the government and that it would not do so unless asked. *Id.* at 15. It is not clear how OIG, or other government entities, would know to ask about a

³⁶ SQOO wrote that eCW continued to rely on the "bad apple" or "blame the documentation" theory for poor organizational performance, attributing improper behavior to bad employees or missing documents rather than addressing underlying organizational issues. Doc. 218-72 at 27.

settlement agreement that no one was supposed to disclose to the government. Nor did eCW disclose the settlement agreement to Relators. Of course, events of that significance in a discovery-intensive case, which this case certainly has been, are almost impossible to keep hidden and Relators eventually stumbled upon clues that something was up.³⁷ The details of this discovery misadventure (and others) as well as the sanctions imposed by the Court can be found at pages 64 through 90 of the hearing transcript on Relators' motion for sanctions.³⁸ Doc. 185 at 64-90.

The new SQOO team leader testified that he did not have any training or education in software security. Doc. 218-18 at 20:2-4, 62:14-16 ("Right now, sitting here, I wouldn't even be able to tell you what the word JSP [i.e., Java Server Page,] stands for.").

³⁷ The government, not eCW, disclosed to Relators both eCW's request to remove Quandary Peak as SQOO and the October 1, 2019 Demand for Stipulated Penalties. Docs. 86 at 2; 185 at 64:9-65:25. In fact, the Court notes that eCW repeatedly represented at the motion to dismiss hearing that there had been no demand for stipulated penalties under the CIA. See, e.g., Doc. 85 at 7:22-8:11, 14:9-22; see also Doc. 69-1 at 42 ("The Amended Complaint does not (and cannot) allege that HHS has issued a stipulated penalty demand.").

³⁸ These sanctions included eCW's failure to produce over 11,000 JIRA tickets collected as part of a seven-year long program, the "AppSec Project," specifically focused on security enhancements and issues. Doc. 185 at 7-63. These tickets documented security vulnerabilities and the steps taken (or not taken) by eCW to address them, including the programmers involved, timelines, comments, and sometimes attachments like screenshots. See, e.g., Docs. 157 at 3-4; 171-14 ¶ 4. eCW claims this was an "inadvertent mistake." Doc. 171 at 8. However, as part of its discovery obligations to Relators, eCW agreed to produce everything given to DOJ as part of DOJ's investigation, which included a complete copy of eCW's JIRA server. Docs. 100 at 5; 185 at 8:1-20. eCW then repeatedly denied that the full JIRA server was produced to DOJ and, in December 2023, produced to Relators what eCW claimed was a complete copy of all relevant JIRA tickets. Doc. 157-6. Notably, in preparing its production to Relators, eCW created a copy of its entire JIRA server and then instructed an employee to manually delete all projects except for the EMR/PE project, including AppSec and 82 other projects such as "Faxing" and "Regulatory Requirements." Docs. 157 at 15; 171-15 ¶¶ 3-6; 185 at 42; see Doc. 171-14 ¶ 6 ("Since Jira was implemented, eCW maintained a 'project' (a collection of Jira tickets) that was associated with each of its products/services. For eCW's EHR software, this project was called 'EMR & PM (PE)."). This "oversight" was discovered in February 2024 when an eCW expert identified references to AppSec tickets in the source code. Doc. 171-14 ¶¶ 11, 13.

6. *Final interval assessments and recurring security issues*

SQOO's post-settlement interval assessments, according to Relators, were far less critical of eCW. Docs. 266-2 ¶¶ 278-79, 322; 300-9 ¶¶ 278-79, 322. Nevertheless, Relators claim the SQOO's final three interval assessments still documented mixed findings. Docs. 266-2 ¶ 323; 300-9 ¶ 323. Specifically, the final interval assessment noted that eCW had not resolved all vulnerabilities. See, e.g., Doc. 218-69 at 6-8, 117-118. eCW ultimately withdrew Version 11 on June 3, 2022, to resolve a direct review initiated by ONC in December 2020 regarding unremedied issues related to 45 C.F.R. § 170.315(b)(3). Docs. 216-2 ¶¶ 373-79; 266-1 ¶¶ 373-79; see Doc. 218-152.

In May 2021, Relators informed DOJ that security vulnerabilities supposedly patched in Version 11 had reappeared in Version 11.52. Docs. 266-2 ¶ 245; 300-9 ¶ 245; see Doc. 218-134 at 68. DOJ and ONC conferred, ONC asked SQOO to investigate, and SQOO confirmed several vulnerabilities including misconfigured .jsp files and inadequate password policies. Docs. 216-2 ¶¶ 353-61; 266-1 ¶¶ 353-361; see Docs. 218-25; 218-137. However, SQOO stated that each issue had either been or was being fixed, or did not constitute a security risk according to eCW. Doc. 218-137.

G. Procedural History

Relators filed their lawsuit on October 16, 2018. Doc. 3. They disclosed their findings to DOJ, and DOJ shared that information with OIG, ONC, and CMS. Docs. 216-2 ¶¶ 317-21; 266-1 ¶¶ 317-21. OIG, in coordination with DOJ, investigated Relators' allegations from November 2018 through September 28, 2021. Docs. 216-2 ¶¶ 319-21; 266-1 ¶¶ 319-21. The United States declined to intervene on October 18, 2021. Doc. 32. On October 26, 2021, DOJ informally notified eCW of its decision as

well as specific security vulnerabilities identified by Relators requiring additional attention. Doc. 218-139.

After the government declined to intervene, eCW unsuccessfully moved to transfer to the District of Massachusetts. Docs. 49; 64. eCW then moved to dismiss, which the Court also denied. Docs. 69; 90. eCW has now moved for summary judgment. Doc. 215.

II. STANDARD

A court must grant summary judgment “if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a). A factual dispute is not genuine unless, based on the evidence presented, “a reasonable jury could return a verdict for the nonmoving party.” *Info. Sys. & Networks Corp. v. City of Atlanta*, 281 F.3d 1220, 1224 (11th Cir. 2002) (quoting *United States v. Four Parcels of Real Prop.*, 941 F.2d 1428, 1437 (11th Cir. 1991)); *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). The movant may support its assertion that a fact is undisputed by “citing to particular parts of materials in the record, including depositions, documents, electronically stored information, affidavits or declarations, stipulations (including those made for purposes of the motion only), admissions, interrogatory answers, or other materials.” Fed. R. Civ. P. 56(c)(1)(A). “When the *nonmoving* party has the burden of proof at trial, the moving party is not required to ‘support its motion with affidavits or other similar material *negating* the opponent's claim[]’ in order to discharge this ‘initial responsibility.’” *Four Parcels of Real Prop.*, 941 F.2d at 1437-38 (quoting *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986)). Rather, “the moving party simply may ‘show[]—that is, point[] out to the district court—that there is an absence of evidence to support the nonmoving party’s

case.” *Id.* (quoting *Celotex*, 477 U.S. at 324) (alterations in original). Alternatively, the movant may provide “affirmative evidence demonstrating that the nonmoving party will be unable to prove its case at trial.” *Id.*

The burden then shifts to the non-moving party, who must rebut the movant’s showing “by producing ... relevant and admissible evidence beyond the pleadings.” *Josendis v. Wall to Wall Residence Repairs, Inc.*, 662 F.3d 1292, 1315 (11th Cir. 2011) (citing *Celotex*, 477 U.S. at 324). The non-moving party does not satisfy its burden “if the rebuttal evidence ‘is merely colorable or is not significantly probative’ of a disputed fact.” *Id.* (quoting *Anderson*, 477 U.S. at 249-50). Further, where a party fails to address another party’s assertion of fact as required by Fed. R. Civ. P. 56(c), the Court may consider the fact undisputed for purposes of the motion. Fed. R. Civ. P. 56(e)(2). However, “[c]redibility determinations, the weighing of the evidence, and the drawing of legitimate inferences from the facts are jury functions, not those of a judge. ... The evidence of the non-movant is to be believed, and all justifiable inferences are to be drawn in his favor.” *Anderson*, 477 U.S. at 255.

III. DISCUSSION

The FCA imposes financial liability on any person who “knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval,” 31 U.S.C. § 3729(a)(1)(A), or who “knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim,” ³⁹ 31 U.S.C. § 3729(a)(1)(B). “As an enforcement mechanism, the FCA includes a qui tam provision under which private individuals, known as relators, can sue ‘in the name of the [United States]

³⁹ Both theories require evidence of falsity, scienter, and materiality.

Government’ to recover money obtained in violation of § 3729.” *United States ex rel. Bibby v. Mortg. Invs. Corp.*, 987 F.3d 1340, 1343 (11th Cir. 2021), *cert. denied*, 141 S. Ct. 2632 (2021).

A. eCW’s Constitutional Challenge

eCW argues that the FCA’s qui tam provisions are unconstitutional under Article II of the U.S. Constitution because they delegate executive power to private individuals without sufficient government control. Docs. 216-1 at 57; 300 at 130. Notably, every Circuit court that has considered the issue has upheld the constitutionality of the FCA’s qui tam provisions. Many more district courts, including this one, have also rejected those arguments. *Gonite et al. v. UnitedHealthcare of Georgia Inc. et al.*, No. 5:19-cv-00246-MTT, at Doc. 93 (M.D. Ga., Apr. 23, 2025). Thus far, only one district court has ruled that the FCA’s qui tam provisions are unconstitutional. *See United States ex rel. Zafirov v. Fla. Med. Assocs., LLC*, 2024 WL 4349242 (M.D. Fla. Sept. 30, 2024); *United States ex rel. Gose v. Native Am. Servs. Corp.*, 2025 WL 1531137 (M.D. Fla. May 29, 2025). At this point, the Court sees no reason to swim against a tidal bore and again declines to rule that the FCA’s qui tam provisions are unconstitutional.

B. False ONC Certification Theory

Relators’ claim that eCW’s false attestations that its EHR software complied with ONC’s certification criteria fraudulently induced providers to submit false claims. Docs. 17 ¶¶ 115-151, 161-167; 266 at 3, 11-12. Under this theory, a defendant that procures a government benefit—here, certification of software—through material misrepresentations—the “original fraud”—can be liable for claims submitted on the strength of that certification. *United States ex rel. Marcus v. Hess*, 317 U.S. 537, 543–44 (1943); *see Marsteller for use & benefit of United States v. Tilton*, 880 F.3d 1302,

1314 (11th Cir. 2018) (“[S]ubsequent claims are false ‘because of an *original fraud* (whether a certification or otherwise).”).

To prevail, eCW claims, and Relators do not disagree, that Relators must show that eCW “(1) made a false statement or engaged in a fraudulent course of conduct (2) with scienter (3) that was material and (4) caused the government to pay out money or forfeit moneys due.” Doc. 216-1 at 20 (citing *Briggs v. QuantiTech Inc.*, 2022 U.S. App. LEXIS 11830, at *7 (11th Cir. May 22, 2022)). “Scienter” includes actual knowledge, deliberate ignorance, or reckless disregard of the truth. 31 U.S.C. § 3729(b)(1). The FCA defines “material” as having a natural tendency to influence the payment decision. 31 U.S.C. § 3729(b)(4); *see also Universal Health Servs., Inc. v. United States ex rel. Escobar*, 579 U.S. 176 (2016).

Under the ONC certification program, EHR developers seeking CEHRT certification of their software must provide an attestation of conformity with certain technical specifications. Docs. 216-2 ¶¶ 39, 65; 266-1 ¶¶ 39, 65; 266-2 ¶¶ 62, 75; 300-9 ¶¶ 62, 75. Providers must use CEHRT to receive MIPS incentive payments. Doc. 218-22 at 13; *see* 42 C.F.R. §§ 414.1305, 414.1375. If a developer misrepresents the capabilities of its software to obtain ONC certification then the performance scores for providers using that software are inflated. In that event, the EHR developer causes providers using its software to report, falsely, that they qualify for MIPS incentive payments. *See* Doc. 218-22 at 13. Here, there is evidence that eCW knowingly failed to disclose material vulnerabilities in its EHR software which caused ONC to certify its software. As a result, there is evidence that CMS paid MIPS incentives that should not have been paid to providers using eCW software.

1. Falsity

To obtain ONC certification for Version 11 of its software, eCW represented that its EHR software complied with 45 C.F.R. § 170.315(d)(1) through (e)(2). Docs. 266-60; 266-48 at 5-6; 300-11. These criteria require EHR systems to authenticate users with unique IDs and role-based access (§170.315(d)(1)); log tamper-resistant audit trails (§170.315(d)(2)); enforce timeouts and re-authentication (§170.315(d)(5)); allow emergency access (§170.315(d)(6)); encrypt or block local PHI storage (§170.315(d)(7)); verify data integrity using approved encryption/hashing algorithms (§170.315(d)(8)); use secure transmission protocols (§170.315(d)(9)); let patients securely view, download, and share health data (§170.315(e)(1)); and support encrypted, auditable patient-provider messaging (§170.315(e)(2)). eCW does not seek rulings that vulnerabilities do not exist. Rather, eCW claims that the alleged vulnerabilities do not make its attestations false. Doc. 216-1 at 11. Specifically, eCW claims the Relators have offered at most a “difference of reasonable opinion” about whether eCW’s EHR software satisfies the certification criteria.⁴⁰ *Id.* at 32-34. eCW argues that Relators must show an “objective falsehood” to prove falsity and that a reasonable difference of opinion does not constitute an objective falsehood, citing *United States v. AseraCare, Inc.*, 938 F.3d 1278, 1290 (11th Cir. 2019).⁴¹ *Id.* at 32. But

⁴⁰ eCW also argues it is entitled to summary judgment because it passed the required certification tests conducted by its ONC-ACB in April of 2021. Doc. 216-1 at 33. According to eCW, this demonstrates compliance with the applicable regulatory criteria. *Id.* However, Version 11 of eCW’s software was certified on December 28, 2017, so this argument is not at all dispositive. See Docs. 266-2 ¶ 132; 300-9 ¶ 132.

⁴¹ *AseraCare* held that a hospice claim certifying that a patient is terminally ill based on a physician’s clinical judgment cannot be false—and thus cannot be actionable under the FCA—unless the underlying clinical judgment reflects an “objective falsehood.” 938 F.3d at 1296-98. This is because a properly formed and sincerely held clinical judgment is not untrue even if another physician later disagrees with that judgment. *Id.* at 1297. Rather, a clinical judgment must be shown to be flawed through verifiable

the technical certification criteria, which eCW barely mentions, belie this argument. Examination of the criteria reveals that ONC sets sufficiently precise certification requirements and qualified professionals can determine whether EHR software meets those requirements. Noncompliance cannot be excused by claims of mere difference of opinions.

Before digging into those technical requirements, the Court addresses an argument that eCW turns to repeatedly—it's all someone else's fault. ONC certification requirements are premised on secure-by-design principles. *See, e.g.*, Docs. 218-14 at 8-9; 218-17 at 53:3-20; 266-31 at 15. eCW essentially attempts to shift the blame from the design and functionality of its software to user behavior or misuse. Doc. 216-1 at 32-36. However, the ONC criteria assume systems will face some unauthorized access attempts or other threats. Doc. 266-31 at 15. Therefore, vendors must: implement tamper resistance (§170.315(d)(2)); provide role-based access and session controls (§170.315(d)(1), (d)(5)); and use modern encryption/hashing algorithms (§170.315(d)(8)-(9), (e)(1)-(2)). If security vulnerabilities arise from design flaws in software architecture, poor encryption, insecure code, or inadequate default settings, blaming isolated user actions does not exonerate, it inculpates. Doc. 266-31 at 15; *see* 81 Fed. Reg. 72404, 72425 (Oct. 19, 2016). Moreover, EHR technology vendors do not merely attest that their technology will pass the limited testing prescribed by ONC; they assure ONC that their technology complies with certification requirements whether or not it is tested. Docs. 266-2 ¶¶ 70-79; 300-9 ¶¶ 70-79. An EHR developer must honestly attest that its software meets the certification criteria and disclose any known

facts to state a claim under the FCA. *Id.* As will be discussed at some length, representations of compliance with ONC technical criteria are not at all like a physician's clinical judgment.

issues that might affect compliance. Docs. 266-2 ¶¶ 70-79; 300-9 ¶¶ 70-79. The following discussion is illustrative, not exhaustive of the alleged failure of eCW's software to meet specific certification criteria.

i. Authentication, access control, authorization

Certified EHR software must verify user identities using unique identifiers (e.g., username or number) to ensure that the user seeking access is the one claimed and to set the type of access and actions users are permitted to perform based on these identifiers. 45 C.F.R. §170.315(d)(1). The expectation is that the system will deny unauthorized requests by verifying the permissions assigned to the user's unique identifier. Docs. 218-14 at 16; 238 at 137:16-138:12; 259-6 at 3. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Based on that evidence, the Court cannot say as a matter of law that eCW's attestations of compliance with 45 C.F.R. §170.315(d)(1) were not false, "objectively" or otherwise.

ii. Auditable events and tamper-resistance; audit report(s)

The ONC criteria require EHR software to have audit logging capabilities to track access and changes to PHI. 45 C.F.R. §§ 170.315(d)(2), 170.315(d)(3). This includes recording the date, time, patient identification, user identification, a description of the action taken, and changes to user privileges.⁴³ 45 C.F.R. §§ 170.315(d)(2),

⁴² [REDACTED]

⁴³ eCW has argued that the audit log requirements under 45 C.F.R. § 170.315(d) apply only to actions performed by authorized users, not unauthorized users who bypass the application entirely. See Docs. 90 at 17-18; 216-1 at 34-35 & n.11, 36; see also Doc. 218-14 at 24 ("[H]acker bypass not being recorded

170.210(e)(1). Relators present evidence that eCW's software did not meet 170.315(d)'s audit logging requirement because design flaws allowed downloads of PHI without logging and the logs could be evaded and/or lacked necessary entries.⁴⁴ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

in the audit reports ... is outside any of the certification criteria and not explicitly covered in expected auditing capabilities.”). As discussed above, eCW's efforts to shift blame to users are unavailing. This is a good example of why that is so. For instance, “EHR technology must be able to detect whether the audit log has been altered.” 45 C.F.R. § 170.315(d)(2)(v). This “requires EHR technology to be able to determine whether *activity outside of its control* has in some way altered the audit log.” 77 Fed. Reg. 54163, 54235 (Sept. 4, 2012) (emphasis added). ONC has also made clear that certified health IT must be designed and made available in ways that allow certified capabilities to be used securely and reliably, including in scenarios involving potential security breaches. 81 Fed. Reg. 72404, 72422, 72423 (Oct. 19, 2016). “Where certified capabilities do not perform in such a manner due to factors that the developer could have reasonably influenced or controlled, the certified capabilities do not conform to the requirements of the Program.” 81 Fed. Reg. 72404, 72425 (Oct. 19, 2016), see Example E, at 72422 (explaining exploitation of known design flaw via ransomware attack constitutes nonconformity because the risk was foreseeable and preventable by the developer).

⁴⁴ [REDACTED]

⁴⁵ [REDACTED]

[REDACTED]

Based on this evidence, a reasonable jury could find that eCW's attestations of compliance with § 170.315(d)'s audit logging requirements were false.

iii. End-user device encryption

Section 170.315(d)(7) requires EHR software to be designed to either encrypt locally stored PHI after a session ends or prevent local storage entirely. 45 C.F.R. § 170.315(d)(7). The default installation of eCW's software allegedly stores some PHI, such as scanned documents and diagnostic tests, locally in a folder that is accessible to anyone with access to the computer, regardless of whether the eCW software is

[REDACTED]

running. Docs. 218-5 at 224:2-225:8, 232:13-234:24; 218-8 at 118:12-14; 218-104 at 74-75; 218-134 at 56-58, 71, 73-74; see Docs. 266-2 ¶¶ 194-96, 198; 300-9 ¶¶ 194-96, 198. This means that PHI is not encrypted and can be accessed without logging into the software. eCW admits that it designed its software to create and locally store these documents without encryption. Docs. 218-5 at 224:10-24, 232:3-234:24; 266-2 ¶¶ 194-96, 198; 300-9 ¶¶ 194-96, 198. Additionally, Relators present evidence that “[t]hese EKG and ECG files were never deleted by the program and were created and saved locally each time an EKG or ECG was viewed from within the eCW software on any computer, not just computers in the actual room where the EKG and ECG files were created.”⁴⁷ Docs. 218-29 at 56; 218-134 at 56-58, 71, 73-74. eCW’s expert testified that this action— a doctor viewing a test result stored within the EHR—is within the scope of (d)(7)’s end user device encryption requirement, and that he would want to know if “every time a doctor viewed a certain type of patient record that is stored within the EHR, that the software saved a backup of that document locally to the computer in an unencrypted folder.” Doc. 238 at 156:3-22.

Based on this evidence, a reasonable jury could find that eCW’s attestations of compliance with § 170.315(d)(7) were false.

⁴⁷ While eCW argues this deficit would only affect clinicians who used [REDACTED] EKGs, and only for the time period when local storage of EKGs was permitted (Docs. 216-1 at 26 n.7; 300-9 ¶ 196), this argument is undermined by the fact that when eCW decided to fix the issue—“It was a configuration change. So the change was made ... for it to go out to all customers in a systematic manner.” Doc. 218-5 at 230:6-20. Further, because this was a configuration issue, Relators claim customers had no control over the software’s local storage of these documents. Doc. 218-104 at 74 (“No practice had any custom coding written and they did not have the ability to change the default settings on the server configuration, only ECW support staff could have done that.”); see Docs. 218-5 at 223:19-224:3 (“[T]hat feature, which was controlled by configuration, was [a] mechanism built into the software”); 300-9 ¶¶ 194, 198.

iv. Integrity, trusted connection, secure messaging

Section 170.315(d)(9) requires EHR software to offer encrypted and integrity message protection and provide a trusted connection for transport. Docs. 216-2 ¶ 79; 266-1 ¶ 79. To comply with §170.315(d)(9), the software must establish a trusted connection using secure communication protocols and implement encryption consistent with FIPS 140-2 and 180-4, e.g., using a hashing algorithm with a security strength equal to or greater than SHA-2. 45 C.F.R. §§170.210(a)(2) (adopting NIST, Federal Information Processing Standards (“FIPS”) Publication 140-2), (c)(2) (adopting NIST, FIPS Publication 180-4). The Court will not undertake to explain those technical specifications. The point is that the certification criteria set precise technical specifications.⁴⁸

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

⁴⁸ Similarly, under § 170.315(d)(8), EHR software must be able to create a message digest in accordance with the standard specified in §170.210(c)—i.e., using a hashing algorithm, “i.e., an encryption method,” with security strength equal to or greater than SHA-2—and verify that the message digest remains unchanged/verify that information has not been altered. Docs. 216-2 ¶ 78; 266-1 ¶ 78.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Given this evidence, a reasonable jury could conclude that eCW's representations of compliance were false.

In sum, Relators have produced evidence that eCW's software transmitted PHI unencrypted, allowed access to PHI without proper authentication, failed to enforce access controls, stored PHI locally, and improperly stored and displayed sensitive data. Given the requirements of ONC certification criteria, these flaws cannot be explained away as mere differences of opinion.

2. *Scienter*

Relators must show that eCW acted "knowingly," which the FCA defines as actual knowledge, deliberate ignorance, or reckless disregard for the truth.⁴⁹ *United States ex rel. Schutte v. SuperValu Inc.*, 598 U.S. 739, 749-50 (2023) ("The FCA's scienter element refers to respondents' knowledge and subjective beliefs—not to what an objectively reasonable person may have known or believed."). However, the statute does not require proof of specific intent to defraud. 31 U.S.C. § 3729(b)(1)(B).

⁴⁹ This requires proof that the defendant was actually aware of the information; the defendant intentionally avoided confirming the truth or falsity of the information; or the defendant was conscious of a substantial and unjustifiable risk that the claims were false but submitted them anyway. *Yates v. Pinellas Hematology & Oncology, P.A.*, 21 F.4th 1288, 1303 (11th Cir. 2021).

eCW's sole scienter argument is that efforts to comply with the law negate scienter. Doc. 216-1 at 37. eCW believes it finds support for this argument in *Urquilla-Diaz v. Kaplan Univ.*, 780 F.3d 1039, 1061-62 (11th Cir. 2015). In *Urquilla-Diaz*, the court concluded that "[relator]'s attempt to create a jury question by cherry-picking ... testimony [wa]s unavailing," "[g]iven [relator]'s lack of evidence and [the defendant]'s *robust compliance* system that relie[d] upon multiple employees as well as the independent advice of outside counsel." 780 F.3d at 1061-62 (emphasis added). On this record, "robust" is not an adjective that comes to mind when reviewing eCW's compliance "system."

First, eCW, it seems, had no formal compliance structure before its CIA with OIG.⁵⁰ Docs. 266-2 ¶ 9; 300-9 ¶ 9. Second, there is evidence that things did not significantly change after the CIA went into effect. SQOO's baseline assessment found that eCW did not have a formal and well-documented risk management plan, that "eCW d[id] not maintain clear and useful documentation of security policies and procedures related to application and database security and key architectures," and that eCW lacked qualified personnel to oversee quality assurance and risk management processes. Doc. 270-1 at 6.

⁵⁰ "Prior to the CIA, eCW did not have a Compliance Officer, Compliance and Quality Assurance Committee or Program, or policies and procedures related to certification requirements." Docs. 266-2 ¶ 9; 300-9 ¶ 9. Although this is undisputed, eCW claims it "had personnel and policies in place that were the functional equivalents of a Compliance Officer or a Compliance and Quality Assurance Committee or Program, and it had policies and procedures related to certification requirements that were reduced to writing during the CIA period." Doc. 300-9 ¶ 9. In other words, eCW did not have written policies in place regarding ONC certification prior to its CIA with the OIG.

SQOO also identified systemic issues in eCW's quality assurance processes, including gaps in traceability between certification criteria and test cases, which meant that eCW's software might not meet certification requirements in practice. Docs. 218-59 at 7-11; 270-1 at 2. Consequently, SQOO could not "ascertain whether [eCW's] EHR comprehensively [met] all of the certification requirements ... because eCW ha[d] done only the minimum amount of QA required to pass certification testing, ...which itself [wa]s not comprehensive."⁵¹ Doc. 270-1 at 2. Later, "SQOO found that eCW [still] was not running 'all testing scripts designed to confirm full compliance with the M.U. certification criteria ... against every build of the EHR that was intended for release to customers.'"⁵² Docs. 266-2 ¶ 23; 270-5 at 10; 300-9 ¶ 23 (second alteration in original).

eCW ultimately failed to implement a traceability matrix—a key SQOO recommendation meant to ensure compliance with certification criteria—until years after it was first proposed. Docs. 216-2 ¶¶ 249-254; 266-1 ¶¶ 249-54. In fact, SQOO frequently and repeatedly identified inconsistencies in eCW's implementation of the traceability matrix and other quality assurance processes.⁵³ See, e.g., Docs. 218-60 at 165-66, 168-70; 218-67 at 126-129; 270-6 at 4.

⁵¹ SQOO issued its baseline assessment on December 12, 2017. Doc. 218-59. On November 14, 2017, eCW certified in writing to its ONC-ACB that all required testing for §170.315(d)(1-3, 5-7) had been successfully completed, that there was no limitation on the validity of its declaration of conformity, and that its product was able to meet the respective ONC 2015 Edition certification criteria requirements and maintain the Product's conformance to the full scope of the criteria. Doc. 266-48 at 5-6.

⁵² There is evidence, which eCW disputes, that eCW employees were also concerned that eCW's limited testing could "[leave] open the possibility that the software might contain other bugs that the certification test cases won't uncover." Doc. 266-2 ¶ 38 (citing Docs. 266-43; 266-44; 266-45).

⁵³ "As of November 20, 2019," for instance, "eCW had not yet completed the Traceability Matrix for EHR certification criteria that was originally recommended in June 2018. During an onsite meeting in September 2019 with the eCW Staff responsible for the Traceability Matrix, the SQOO learned that ongoing delays in completing this recommendation were due primarily to insufficient Staff resources dedicated to the EHR Traceability Matrix project." Doc. 270-2 at 5. The SQOO subsequently wrote that "eCW's largest gap relate[d] to their internal organizational structure, a lack of a proactive mindset, and

On April 11, 2019, SQOO reported that “eCW’s software ha[d] numerous security vulnerabilities which ha[d] been identified by the SQOO, outside security experts, and automated software,” which eCW had failed to adequately address and/or acknowledge. Doc. 266-25 at 1-2. Because of this issue and many others, SQOO concluded that “[t]hese problems [were] sufficiently widespread and frequent that they significantly hamper[ed] eCW’s ability to prevent, detect, and remediate [not only] Patient Safety Issues [but also] Certification Issues in eCW’s EHR.” *Id.* at 4. Eventually, OIG sought \$2,717,500 in stipulated penalties due to eCW’s failure to comply with its obligations under the CIA to install oversight processes and to create policies and procedures to address certification issues.⁵⁴ Docs. 216-2 ¶¶ 277-79; 266-1 ¶¶ 277-79.

Further, there is evidence that eCW had little interest in improving its compliance structure. SQOO repeatedly expressed “concerns about eCW’s ability to both create and self-assess its own plans and performance required to address known safety issues in its software.”⁵⁵ Doc. 270-7 at 2. SQOO noted that eCW had an extremely flat management structure; that eCW lacked clinicians with information technology training or experience to conduct risk analyses and adequately test its software; that eCW’s compliance officer had limited knowledge of the inner workings of the company and little or no experience in implementing or managing a quality management or risk

lack of a well-formed, qualified Team of [AppSec] Engineers that are empowered to proactively research and strengthen the defenses within eCW’s application codebase.” *Id.* at 2.

⁵⁴ It is undisputed that OIG’s October 2019 demand letter did not seek stipulated penalties based on any specific security vulnerabilities alleged in this case. Docs. 216-2 ¶ 279; 266-1 ¶ 279.

⁵⁵ “These concerns [were] magnified by the enormous reach of eCW’s product into the heart of the United States ... healthcare system.” Doc. 270-7 at 2; see also Doc. 218-42 at 5-7 (“An overarching and primary risk ... observed [by the SQOO] was that eCW lack[ed] a formal and well-documented risk management process, which fail[ed] to fully identify and measure risk and oversee plans to mitigate them.”).

management standards-based process; and that eCW's leadership was consistently unable to answer what SQOO considered fundamental questions about eCW's AppSec security posture. Docs. 266-34 at 1-4; 270-7 at 14. According to SQOO, AppSec leadership could not answer who monitored eCW's "database monitoring and alerting system(s)," could not sufficiently define a "secure" Wi-Fi connection, did not seem to understand basic principles of the client/server model, including what constitutes a server, and did not know if eCW utilized any security monitoring tools on its databases nor whether data from those tools were fed into any other relevant systems. Doc. 270-7 at 14. As a result, SQOO concluded (1) that eCW's existing policies and procedures for reviewing security vulnerabilities, controls, events, and incidents were broadly insufficient and (2) that eCW's AppSec leadership did "not have sufficient clarity into their purview, mandate, domain, or responsibilities to effectively execute the duties of their office."⁵⁶ *Id.* at 8-9, 13; *see* Doc. 270-2 at 2.

On this record, the Court cannot say as a matter of law that eCW's claimed "robust compliance procedures" negate scienter.

3. *Materiality*

Relators must prove that eCW's misrepresentations were material to the government's decision to pay claims. *Escobar*, 579 U.S. at 192. Materiality is defined as having a natural tendency to influence, or being capable of influencing, the payment or receipt of money or property. 31 U.S.C. § 3729(b)(4); *see also Escobar*, 579 U.S. at 187. The test for materiality is holistic and does not turn on a single fact or occurrence.

⁵⁶ Relators claim that eCW's AppSec director, did not "even know what the ONC user authentication requirements were until October 2019." Doc. 266-2 ¶ 34 (citing Doc. 266-36).

Bibby, 987 F.3d at 1343 (quoting *Escobar*, 579 U.S. at 191; and *United States ex rel. Escobar v. Universal Health Servs., Inc.*, 842 F.3d 103, 109 (1st Cir. 2016) (*Escobar II*)). Rather, courts consider several factors, including “(1) whether the requirement is a condition of the government's payment, (2) whether the misrepresentations went to the essence of the bargain with the government, and (3) to the extent the government had actual knowledge of the misrepresentations, the effect on the government's behavior.” *Bibby*, 987 F.3d at 1347.

Condition of Payment. Fraudulent conduct in obtaining ONC certification is material because the payment of MIPS incentives is conditioned on providers’ certifications that they use CEHRT. 42 C.F.R. §§ 414.1305, 414.1375; see Docs. 216-2 ¶¶ 116, 124-27; 218-22 at 13; 266-1 ¶¶ 116, 124-27. False representations made to obtain CEHRT certification are therefore directly tied to the government’s decision to pay incentives under the MIPS program. This factor favors Relators.

Essence of the Bargain. Compliance with ONC criteria goes to the essence of the government’s bargain. *Bibby*, 987 F.3d at 1347. This factor, according to eCW, “focuses on the substantiality of the noncompliance and *its impact* on the goals of the contract.” Doc. 216-1 at 30 (citing *United States ex rel. Bonzani v. United Techs. Corp.*, 662 F. Supp. 3d 217, 232-33, 235 (D. Conn. 2023)) (emphasis in original). This means, eCW argues, that nonconformities with ONC criteria are not material unless there is evidence of a “real-world impact,” such as hacking incidents or breaches of healthcare providers’ records. Docs. 216-1 at 30; 300 at 7, 13. However, the absence of a security breach does not automatically negate the materiality of compliance with ONC certification criteria—there is substantial evidence that compliance itself is essential to

the core requirements of CMS's Meaningful Use and Promoting Interoperability programs. See, e.g., Doc. 218-22; 42 C.F.R. §§ 495.4, 414.1305. Again, CMS pays incentives to providers who adopt CEHRT, which CMS defines as software satisfying certain certification criteria established by ONC, including specific privacy and security criteria.⁵⁷ Docs. 216-2 ¶¶ 116, 124-27; 218-22 at 13; 266-1 ¶¶ 116, 124-27; see 42 C.F.R. §§ 495.4 and 414.1305.

A reasonable jury could find that eCW's allegedly false certifications that Version 11 met certain security-related certification criteria goes to the essence of the government's bargain.

Government Response. Analysis of this *Escobar* factor is generally fact-intensive and that is particularly true here. *Bibby*, 987 F.3d at 1347 (collecting cases). As noted, that analysis includes what the government did or did not do as evidence of alleged flaws in eCW's software surfaced.

eCW claims that it fully disclosed Relators' allegations to the government and that the absence of a decision to decertify its software or the failure to stop payments means that any alleged misrepresentations were not material. Doc. 216-1 at 27-30. Of course, it's never that simple. *Escobar*, 579 U.S. at 194. The failure to decertify eCW's software does not necessarily negate materiality. Materiality turns on whether misrepresentations had a natural tendency to influence payment—not whether the

⁵⁷ ONC-certified products must demonstrate appropriate privacy and security capabilities whenever a certified capability involves access, exchange, or use of electronic health information—this means specific privacy and security criteria under § 170.315(d) are conditionally necessary for certification to other functional criteria. Doc. 218-14 at 15 (“The framework puts every criterion from §170.315(a), §170.315(b), §170.315(c), §170.315(e), §170.315(f), §170.315(g), and §170.315(h) with the expected privacy and security criteria from the §170.315(d) category that must support the respective criteria functionality.”).

government eventually took formal or the most severe enforcement action available. *Bibby*, 987 F.3d at 1351-52; see *United States ex rel. Fahn v. GardaWorld Fed. Servs. LLC*, 2024 WL 1605313, at *12 n.8 (M.D. Ga. Apr. 12, 2024) (“[A] ‘finding’ of materiality by the ‘factfinder’ does not require the government to have taken ‘the strongest possible action,’ only that some enforcement action is taken.”) (quoting *Bibby*, 987 F.3d at 1352). Courts have also rejected attempts to use regulatory inaction as a shield to liability where the alleged fraud was concealed or the consequences were misrepresented. See, e.g., *United States ex rel. Wallace v. Exactech, Inc.*, 2020 WL 4500493, at *16 n.16 (N.D. Ala. Aug. 5, 2020). Here, there is evidence that eCW “repeatedly reported inaccurate information ... to the SQOO ... [throughout its] entire ... CIA[]], which directly caused the SQOO to report inaccurate information” to OIG and ONC. Doc. 218-72 at 268; see *Bibby*, 987 F.3d at 1349 (quoting *Escobar II*, 842 F.3d at 112 (“[M]ere awareness of allegations concerning noncompliance with regulations is different from knowledge of actual noncompliance.”)) (alteration in original). As for the continued payment of claims, courts have held that continued payment does not necessarily negate materiality, especially when, as here, payments are made to innocent third parties. See, e.g., *United States v. Corp. Mgmt., Inc.*, 78 F.4th 727, 737-38 (5th Cir. 2023) (“While *Escobar* articulated that continued payment despite knowledge of fraud often indicates lack of materiality, ‘often’ does not mean ‘always.’”); see *Fahn*, 2024 WL 1605313, at *12 n.9 (“The continued payment factor may carry less weight due to the unique circumstances of th[e] case.”). According to DOJ, “CMS was arguably required to make payments as long as the software remained certified.” Doc. 292 at 11.

In any event, the government took significant action when it learned of Relators' allegations to ensure that eCW addressed alleged flaws. Shortly after Relators filed their initial complaint, DOJ disclosed to eCW the security flaws identified by Relators and directed eCW to "immediately address any such security vulnerabilities" and confirm that it was "acting with all due speed to investigate and address such issues." Docs. 69-3 at 4-6; 218-110. This prompted eCW to address some issues within 12 hours. Doc. 316-1 at 4; see Docs. 216-2 ¶¶ 322-29; 266-1 ¶¶ 322-29. DOJ presented eCW with additional details in January 2019 through a PowerPoint presentation provided by Relators and directed eCW to fix them. Docs. 216-2 ¶¶ 330-332; 266-1 ¶¶ 330-32; see Docs. 266-2 ¶¶ 243-44; 300-9 ¶¶ 243-44. DOJ also had multiple meetings with ONC and OIG to discuss the security concerns raised by Relators. *See, e.g.*, Docs. 216-2 ¶¶ 344, 346-49, 354-59; 266-1 ¶¶ 344, 346-49, 354-59. For instance, Relators provided DOJ with updates regarding vulnerabilities still present in eCW's software in May 2021. Docs. 216-2 ¶ 353; 266-1 ¶ 353; 266-2 ¶ 245; 300-9 ¶ 245. After, DOJ and ONC conferred and, on May 27, 2021, ONC directed SQOO to investigate. Docs. 216-2 ¶¶ 354-55; 266-1 ¶¶ 354-55. SQOO conducted a detailed investigation and issued a "Security Assessment" on July 14, 2021, which was shared with ONC, OIG, and DOJ. Docs. 216-2 ¶¶ 358-60; 266-1 ¶¶ 358-60; 266-2 ¶ 248; 300-9 ¶ 248. DOJ later sent eCW a letter on October 26, 2021, identifying specific security vulnerabilities requiring further attention. Docs. 216-2 ¶ 368; 266-1 ¶ 368. In short, the government repeatedly pushed eCW to address alleged flaws. eCW might have avoided the ultimate sanction, but it certainly was not exonerated.

In sum, the Court cannot say as matter of law that eCW's alleged misrepresentations were not material.

4. Causation

To establish liability under the FCA, a relator must show that the false statement or fraudulent conduct “caused the government to pay out money or forfeit moneys due.” Doc. 216-1 at 20; see 31 U.S.C. § 3729(a)(1)(B); see also *Ruckh v. Salus Rehab., LLC*, 963 F.3d 1089, 1097 & n.3, 1107 (11th Cir. 2020). As eCW frames the issue, that means Relators must adduce evidence that eCW's misrepresentations caused ONC to certify its software. Doc. 216-1 at 22. As framed, the answer seems obvious—it is undisputed that ONC certification is largely attestation-based. *E.g.*, Docs. 266-2 ¶¶ 70-71; 300-9 ¶¶ 70-71 (“[ONC-]ACBs must accept developer ‘self-attestations.’”). But eCW then advances a counter-factual argument: because ONC did not decertify or suspend its certification when it learned of the flaws in eCW's software, Relators cannot prove that eCW's misrepresentations caused the ONC to certify the software. Doc. 216-1 at 23-24. If that sounds like eCW's inherently factual materiality argument, that's because it effectively is, and the Court has rejected that argument. As discussed, ONC played a key role in the government's investigation of alleged flaws in eCW's software and that investigation did not exonerate eCW.

However, the Court elaborates on eCW's statement of the issue. Causation turns on the relationship between eCW's conduct and a provider's eligibility to receive MIPS incentives. To earn MIPS incentives, providers must use CEHRT. Docs. 216-2 ¶¶ 116, 124-27; 218-22 at 13; 266-1 ¶¶ 116, 124-27. Thus, when developers misrepresent the capabilities of their software to get CEHRT certification, they cause

providers using their software to report, falsely, that they qualify for MIPS incentive payments.

As discussed above at some length, there is evidence that eCW falsely represented that its software met ONC requirements for CEHRT. But for those representations, eCW's software would not have been certified. And a jury could find ineligible providers received MIPS incentive payments as a result. See, e.g., Doc. 218-22 at 13; see also *Ruckh*, 963 F.3d at 1105, 1107. That ONC did not decertify Version 11 does not as a matter of law break that causation chain.

In short, there is evidence that eCW's fraudulent conduct caused the government to pay false claims. Accordingly, the Court cannot say as a matter of law that Relators cannot establish the element of causation.

5. Damages

Based on their false ONC certification theory,⁵⁸ Relators seek to recover the MIPS incentive payments paid because of providers' CEHRT attestations. Docs. 266 at 39; 266-2 § XIII ¶ 311. In perfunctory fashion, eCW advances three reasons why the "court should grant summary judgment as to damages."⁵⁹ Doc. 216-1 at 54-56.

⁵⁸ Perhaps understandably, Relators have no evidence of actual damages arising from providers' allegedly false certification of HIPAA compliance. According to the amended complaint, those damages would include every reimbursement claim submitted by providers using eCW software, a staggering toll, the proof of which would face likely insurmountable evidentiary obstacles. For example, when CMS reimburses a provider, it pays for a substantial benefit CMS received—medical services rendered to a beneficiary. Figuring out what part of that reimbursement was paid for a provider's certification of HIPAA compliance would likely be impossible. Relators' theory of recovery for false attestations to secure CEHRT certification, on the other hand, is straightforward. When CMS pays MIPS incentives, that payment is, absent an exception, conditioned on providers' use of CEHRT. If the CEHRT certification was fraudulently obtained, there is evidence that CMS did not get what it paid for.

⁵⁹ eCW abandoned a fourth reason that apparently was based on its misunderstanding of the Relators' damages model. Compare Doc. 216-1 at 56 with Doc. 300 at 23-24.

First, eCW argues that the MIPS program is “budget neutral” and thus there are no damages. Doc. 216-1 at 54-56. In concept, MIPS is designed to be budget neutral because the financial penalties imposed on low-performing providers fund the financial rewards for high-performing providers. Docs. 216-2 ¶ 122; 266-1 ¶ 122. The reality is that the MIPS program is not budget neutral. From 2019 to 2024, CMS allocated an additional \$500 million annually to award exceptional performers, a sum not subject to budget neutrality requirements. Doc. 218-107 ¶ 40. Accordingly, Relators argue that the MIPS program is not budget neutral for every year in their damages model (i.e., 2019 to 2024) because Congress appropriated additional funds for exceptional performance bonuses (\$2.5 billion total). Docs. 266 at 40; 266-2 § XIII ¶¶ 317-320.

In any event, the Court rejects the logic underlying eCW’s budget neutral argument. The government suffers harm when it pays money because of fraudulent conduct, even if it would have paid as much or more to other parties absent the fraud. *See, e.g., United States v. Anghaie*, 633 F. App’x 514, 518-19 (11th Cir. 2015) (“A defendant may ... be liable ... even if the defendants may have won the contracts anyway as the lowest bidder.”) (citing *United States v. Killough*, 848 F.2d 1523, 1532 (11th Cir.1988)); *see also United States ex rel. Grubbs v. Kanneganti*, 565 F.3d 180, 188-89 (5th Cir. 2009). Put simply, enriched fraudsters cannot escape liability by arguing that the government has not been injured because the government paid less to someone else.

Second, eCW argues that Relators' damages expert⁶⁰ failed to consider that "if eCW's EHR software had been decertified ..., eCW's customers would have been eligible for hardship exceptions ... and/or to claim exemptions from reporting due to their small-practice status." Doc. 216-1 at 55. In other words, if the government had discovered the fraud and pulled Version 11's CEHRT certification, some providers still might have been able to receive MIPS incentives. The Court fails to see the relevance of that fanciful thought experiment to eCW's motion for "judgment as to damages." Of course, eCW can present relevant evidence to mitigate Relators' claimed damages.

Third, eCW argues that "a full refund is. . . the wrong measure of damages, because Relators have not proven that eCW's EHR software had no value."⁶¹ Doc. 216-1 at 55. eCW does not attempt to quantify the value of uncertified software. If eCW had, it might have realized that it again misses the point. This case is not about the value of software purchased by providers, it is about MIPS incentives that were improperly paid. The government bargained for CEHRT certification for which it paid MIPS incentives. See, e.g., Doc. 218-22 at 13. If Relators can prove eCW fraudulently obtained CEHRT certification for its software, Relators may attempt to recover damages based on the amount of MIPS incentive payments the government improperly paid eCW customers.

⁶⁰ Relators' damages expert recalculated MIPS scores by reducing the promoting interoperability category to zero, determining the difference between what the government actually paid and what it would have paid if eCW had not fraudulently obtained certification. See Doc. 218-106.

⁶¹ *Accord Yates*, 21 F.4th at 1304 ("[I]n the context of Medicare claims, where no product or service is provided to the United States, courts have measured damages as the difference between what the government paid and what it would have paid had the defendant's claim been truthful and accurate The rationale is that, had the defendant truthfully admitted that it was non-compliant, the United States would not have paid.") (emphasis in original); *Id.* at 1305 ("[W]e [have] rejected an argument similar to [Defendant's]—that outside of the context of the delivery of a product or service to the United States, damages can be determined based on the value purportedly provided to the United States.").

Accordingly, eCW is not entitled to “judgment on damages.”

6. *Government action and public-disclosure bars*

The FCA bars claims based on allegations or transactions that are the subject of a civil suit or administrative civil money penalty proceeding in which the government is already a party as well as claims based on allegations or transactions that have been publicly disclosed unless the relators are original sources of the information. 31 U.S.C. § 3730(e)(3)-(4)(A). eCW argues that both bars apply here because the allegations made by the Relators were publicly disclosed through various public channels, such as websites, and in *Delaney*, which the government has already addressed through previous settlements and proceedings. Doc. 216-1 at 46-54.

On this record, the Court cannot say as a matter of law that Relators’ claims in their entirety are barred.⁶² The Relators’ allegations are arguably distinct from those in *Delaney*, which involved different software versions, different flaws, and different claims and damages. *Compare* Doc. 17 with Doc. 218-38; *see* Docs. 216-2 ¶¶ 197-205; 266-1 ¶¶ 197-205; 266-2 ¶¶ 96, 336; 300-9 ¶¶ 96, 336. *Delaney* focused on requirements under CMS’s Meaningful Use Program, which was replaced by MIPS in 2017, and involved an earlier version of eCW’s EHR software that was certified under the 2011 and 2014 ONC standards. Docs. 218-38; 266-2 ¶ 96; 300-9 ¶ 96. Moreover, *Delaney* involved allegations that eCW hardcoded its software to pass certification testing, without mentioning specific security vulnerabilities under § 170.315(d). *Compare* Doc. 218-38 with Docs. 266 at 12; 266-2 §§ III, IV. As one eCW attorney put it, “[t]his isn’t the same case at all. The allegation in the *Delaney* case was that the company

⁶² eCW does not seek a ruling that particular aspects of the Relators’ claims are barred.

designed the software intentionally to cheat a testing protocol that they knew about in advance. That is, I think it should be very clear, a very different case from this one.” Doc. 85 at 50:14-17. Finally, the websites that eCW cites as public disclosures only disclosed some vulnerabilities identified in earlier versions of the software and did not reveal any fraudulent conduct by eCW related to the certification of Version 11. Docs. 216-2 ¶¶ 293-96; 266-1 ¶¶ 293-96; see Docs. 218-5 at 240:12-19; 218-110; 316-1 at 4.

In short, the Court cannot say as a matter of law that Relators’ false CEHRT attestation allegations are barred in their entirety.

In sum, there exist genuine issues of material fact as to whether eCW knowingly caused the government to pay false claims for MIPS incentive payments by fraudulently obtaining CEHRT certification of its software. Accordingly, eCW’s motion for summary judgment on Relators’ false ONC certification theory is **DENIED**.

C. False HIPAA Compliance Theory

Relators tersely allege that eCW has “violated and is violating the FCA by causing healthcare providers to falsely certify compliance with ... [HIPAA security] regulations.” Doc. 17 ¶ 107. Without question, as it acknowledged, eCW must comply with HIPAA Privacy and Security Rules. See, e.g., Doc. 218-30 at 4. The question here, however, is whether eCW *by some fraudulent means*⁶³ caused providers to make misrepresentations of HIPAA compliance when submitting claims to CMS. According to eCW, Relators’ HIPAA compliance theory appears to be premised on 31 U.S.C. §

⁶³ This element of a fraudulent inducement theory has been called the “original fraud.” *Marsteller*, 880 F.3d at 1314 (“[S]ubsequent claims are false ‘because of an *original fraud*.’”). Typically, and here, the actual “false” claims are not independently fraudulent because the party submitting the claim has been duped by that original fraud and thus has not knowingly submitted a false claim. *Gose v. Native Am. Servs. Corp.*, 109 F.4th 1297, 1315 (11th Cir. 2024); see Doc. 17 ¶ 114.

3729(a)(1)(A) which requires them to prove “(1) a [materially] false or fraudulent claim; (2) which was presented, or caused to be presented, by [eCW] to [CMS] for payment or approval, (3) with the knowledge that the claim was false.” Doc. 216-1 at 21 (alteration in original).

The Relators have struggled to find footing for their HIPAA theory. The reason is that their theory does not fit in the regulatory framework for ONC certification and it is only within that framework that the Relators identify some specific evidence of fraud. As discussed, and as Relators adroitly exploit, ONC has sufficiently precise certification criteria for EHR software. 45 C.F.R. § 170.315; *see also* Doc. 266-31. Although those criteria address some concerns covered by HIPAA, they do not incorporate wholesale HIPAA, or more to the point, the HIPAA Security Rule. Docs. 216-2 ¶¶ 136-138; 266-1 ¶¶ 136-138. Quite clearly, eCW did not attest that its software complied with HIPAA security regulations to obtain CEHRT certification. Further, neither ONC nor CMS monitor or enforce compliance with the HIPAA Privacy or Security Rules. Docs. 216-2 ¶ 140; 266-1 ¶ 140; *see* 81 Fed. Reg. 72404 (Oct. 19, 2016). A different body—the Department of Health and Human Services’ Office of Civil Rights—administers and enforces the HIPPA Privacy and Security Rules. Docs. 216-2 ¶¶ 129,133; 266-1 ¶¶ 129, 133. In fact, as Relators admit, both “ONC and CMS advise clinicians that ‘EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules.’” Docs. 216-2 ¶ 136; 266-1 ¶ 136. In short, Relators present no evidence that eCW represented that its software complied fully with HIPAA security regulations to obtain CEHRT status.

In their amended complaint, Relators base their HIPAA compliance theory on an electronic data interchange (“EDI”) form that providers must execute before submitting claims for payment electronically to CMS. Docs. 17 ¶ 108; 17-3; *compare* Docs. 266 at 29-30; 266-2 ¶¶ 113-14. Relators claim they find on that form an express certification that *providers* will comply with the HIPAA Security Rule in this sentence: “The provider agrees ... [to] use sufficient security procedures (including compliance with all provisions of the HIPAA security regulations) to ensure that *all transmissions of documents are authorized and protect all beneficiary-specific data from improper access.*”⁶⁴ Docs. 17-3; 266-2 ¶¶ 113-14 (emphasis added). In a feat of grammatical gymnastics, Relators rearrange that sentence to read, providers will ensure (1) that their transmissions are authorized and (2) much more broadly, that their practices protect all beneficiary-specific data from improper access. Doc. 266 at 30. Rearranged that way, Relators argue the EDI form requires providers to certify compliance with transmission protocols *and* to certify compliance with the HIPAA Security Rule, that is, that their EHR protects all beneficiary-specific data from improper access.

There are two problems with this theory. First, Relators skip the critical first step—by what original fraud did eCW cause providers to unwittingly make a false certification of HIPAA compliance for each bill they submitted to CMS? Relators don’t say.⁶⁵ Second, the Relators’ rearrangement of the EDI certification makes neither common nor grammatical sense. Plainly, the EDI certification covers the security of

⁶⁴ According to eCW, “relators do not identify the basis for their implied-certification argument, which is not the EDI Enrollment Agreement.” Doc. 300-9 ¶ 113.

⁶⁵ Relators vaguely assert that eCW “did not tell the customers the software was insecure.” Doc. 266 at 32. But the evidence Relators cite for that assertion is even more vague. They claim eCW did not tell customers about some of its internal testing. Docs. 266 at 32; 266-2 ¶ 117.

transmissions to CMS.⁶⁶ As for common sense, the purpose of EDI is to facilitate the *transmission* of data for coverage and payment determinations. Docs. 216-2 ¶¶ 145-149; 266-1 ¶¶ 145-149. Consistent with that, CMS enforces HIPAA's Transaction Rule,⁶⁷ not the HIPPA Security Rule. Docs. 216-2 ¶¶ 140-142; 266-1 ¶¶ 140-142. In short, the EDI form simply, and logically, addresses transmission of data to CMS; it does not extract from providers a promise that their practices comply with the HIPAA Security Rule.⁶⁸

More fundamentally, Relators' HIPAA theory is detached from practical reality. Compliance with HIPAA's Security Rule impacts the entirety of providers' practices, not just their EHR software. Thus, compliance is necessarily provider-specific. Docs. 216-2 ¶¶ 130-32; 266-1 ¶¶ 130-32. And Relators' HIPAA theory is time-specific—it turns on whether a provider's practice complied with HIPAA when the provider submits a bill. Consequently, even if eCW could cause a provider to violate HIPAA, it does not follow that all providers violated HIPAA, much less that all providers' practices were not HIPAA-compliant each and every time when they submitted claims to CMS. In fact,

⁶⁶ Here is the Court's effort at a grammatical breakdown of the EDI attestation. The requirement "to ensure ... and protect" forms a single, continuous infinitive phrase modifying "use." This indicates a unified objective: to ensure authorized transmissions and protect data in the course of those transmissions. The second verb, "protect," lacks an independent subject or clause, which suggests it is grammatically tied to and dependent on the context of "transmissions of documents." This language does not establish a free-standing obligation to protect data generally but rather describes the dual goals of a single security process—ensuring the authorization and protection of transmitted data.

⁶⁷ CMS administers HIPAA Administrative Simplification requirements, which require standard formats and code sets for electronic health care transactions, e.g., claims and payment. Docs. 216-2 ¶¶ 141-44; 266-1 ¶¶ 141-44. Transactions that fail to comply with these requirements are automatically rejected by Medicare's EDI system. Docs. 216-2 ¶ 147; 266-1 ¶ 147.

⁶⁸ Late in the day, and certainly not in any pleading, Relators threw out the "concern" that eCW's software might have led providers to erroneously complete HIPAA "security risk assessments." Docs. 218-7 ¶¶ 34-35; 266 at 28-29. If this undeveloped concern has any relevance, it is covered by Relators' false ONC certification theory.

Relators have not identified any provider's practice that failed to comply with the HIPAA Security Rule at the time a bill was transmitted to CMS.⁶⁹ Finally, and logically enough, providers, not EHR software developers, are responsible for ensuring that their practices comply with HIPAA. Docs. 216-2 ¶¶ 136-38; 266-1 ¶¶ 136-38.

So back to original fraud, or rather the absence of clear material misrepresentations by eCW of broad HIPAA compliance that caused providers to submit false claims to CMS. Simply put, Relators cannot establish the elements of an FCA claim based on their HIPAA compliance theory. *See, e.g., Ruckh*, 963 F.3d at 1109. They point to no fraudulent conduct by eCW that caused providers to falsely certify compliance with the HIPAA Security Rule when submitting claims to CMS. The EDI form does not certify such compliance, and even if it did, the Relators point to no fraudulent acts or omissions by eCW that caused providers to falsely certify broad HIPAA compliance. And even if they had, Relators have not identified any provider that was not HIPAA-compliant when that provider submitted a claim for reimbursement. *See* Doc. 218-105 at 239:13-240:20. In other words, they have not shown the presentment⁷⁰ of a false claim; they do not address presentment at all. Nor have Relators shown that eCW knew that it, somehow, was inducing all providers to certify

⁶⁹ While Relators' claim that eCW's software does not properly enforce access controls and thus cannot ensure that transmissions of documents to CMS are authorized, they have failed to identify any unauthorized transmissions to CMS or show that eCW's alleged lack of access controls was material to the providers' ability to certify compliance with HIPAA's transmission security requirements. Docs. 266 at 30; 266-2 ¶ 115; *see* Doc. 218-105 at 239:13-240:20 ("Q: I can comply with my EDI obligations even though I'm using eCW's EHR software? Those two things are possible? A: It depends ...").

⁷⁰ *See Corsello v. Lincare*, 428 F.3d 1008, 1014 (11th Cir. 2005) ("Underlying improper practices alone are insufficient to state a claim under the False Claims Act absent allegations that a specific fraudulent claim was in fact submitted to the government.") (citing *United States ex rel. Clausen v. Lab. Corp. of Am., Inc.*, 290 F.3d 1301, 1311 (11th Cir. 2002)).

that their practices complied with the HIPAA Security Rule. Nor is there evidence that compliance with the HIPAA Security Rule in its entirety is material to CMS payments to providers. While compliance may be important generally, when CMS pays a provider's claim, it is paying for services rendered to patients, not HIPAA compliance.

Accordingly, eCW is entitled to summary judgment on Relators' HIPAA compliance theory.

IV. CONCLUSION

For the foregoing reasons, eCW's motion for summary judgment (Doc. 215) based on Relators' fraudulent inducement theory is **DENIED**. eCW is **GRANTED** summary judgment on Relators' HIPAA compliance theory.⁷¹

SO ORDERED, this 25th day of June, 2025.

S/ Marc T. Treadwell
MARC T. TREADWELL, JUDGE
UNITED STATES DISTRICT COURT

⁷¹ On December 4, 2024, eCW moved to strike Relators' October 1, 2024 Supplemental Discovery Response, arguing the disclosure was untimely, prejudicial, and obtained through improper conduct. Doc. 297. Alternatively, eCW requested additional discovery and permission to file supplemental briefs on pending motions. Docs. 317 at 2; 344 at 1 &n.1.

Federal Rule of Civil Procedure 37(c)(1) allows courts to exclude evidence if a party fails to disclose it timely, unless the failure was substantially justified or harmless. Here, eCW claims that the Supplemental Response is not material to the case. Doc. 344 at 2 n.3; *compare* Doc. 338 at 4 ("eCW expressly stated in its summary judgment filings that the supplement was 'not material' or was 'irrelevant' to its summary judgment arguments.") (citing Doc. 300-9 ¶¶ 336-341). That concern can be addressed before trial. As for timeliness, Relators have sufficiently demonstrated that their Supplemental Response was submitted at eCW's request, and any delay was caused by eCW's withholding of relevant JIRA tickets and delayed access to the Contrast server. To address possible prejudice, the Court allowed eCW to reconvene Mr. Wheeler's deposition, which it did on January 29, 2025. Finally, at the June 4, 2025 motions hearing, eCW did not request additional discovery or ask to submit supplemental briefing, and the Court ruled on those motions. The Court finds that Relators' Supplemental Response was timely and that further briefing is not necessary. Accordingly, eCW's Motion to Exclude Relators' Second Supplemental Response (Doc. 297) is **DENIED**.