106TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 106–773
Part 1

MEDICAL FINANCIAL PRIVACY PROTECTION ACT

JULY 20, 2000.—Ordered to be printed

Mr. LEACH, from the Committee on Banking and Financial Services, submitted the following

R E P O R T

together with

DISSENTING VIEWS

[To accompany H.R. 4585]

[Including cost estimate of the Congressional Budget Office]

The Committee on Banking and Financial Services, to whom was referred the bill (H.R. 4585) to strengthen consumers' control over the use and disclosure of their health information by financial institutions, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Medical Financial Privacy Protection Act".

SEC. 2. USE AND DISCLOSURE OF HEALTH INFORMATION BY FINANCIAL INSTITUTIONS.

(a) IN GENERAL.—Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) is amended by inserting after section 502 the following:

"SEC. 502A. SPECIAL RULES FOR HEALTH INFORMATION.

"(a) RULES FOR DISCLOSURE.—

"(1) GENERAL RULE REQUIRING AFFIRMATIVE CONSENT FOR DISCLOSURE.—

"(A) IN GENERAL.—A financial institution may not disclose any individually identifiable health information pertaining to a consumer to an affiliate or a nonaffiliated third party unless the financial institution—

"(i) has provided to the consumer a clear and conspicuous notice in writing, in electronic form, or in another form permitted by the regulations implementing this subtitle, of the categories of such information that may be disclosed and the categories of affiliates or nonaffiliated third parties to whom the financial institution discloses such information;

"(ii) has clearly and conspicuously requested in writing, in electronic form, or in another form permitted by the regulations implementing this subtitle, that the consumer affirmatively consent to such disclosure; and

"(iii) has obtained from the consumer such affirmative consent and such consent has not been withdrawn.

"(B) WITHDRAWAL OF CONSENT.—A consumer may withdraw a consent to use or disclose individually identifiable health information at any time, except that any such withdrawal of consent is subject to the authorized uses made by the financial institution in reliance on the consent prior to its withdrawal.

"(2) DISCLOSURE OF INFORMATION ABOUT PERSONAL SPENDING HABITS.—

"(A) IN GENERAL.—If a financial institution provides a service to a consumer through which the consumer makes or receives payments or transfers by check, debit card, credit card, or other similar instrument, the financial institution may not disclose any information described in subparagraph (B) pertaining to the consumer to an affiliate or a nonaffiliated third party unless the financial institution has satisfied the requirements of clauses (i), (ii), and (iii) of paragraph (1)(A) with respect to the disclosure.

"(B) INFORMATION DESCRIBED.—The information described in this paragraph is—

"(i) an individualized list of a consumer's transactions or an individualized description of a consumer's interests, preferences, or other characteristics; or

"(ii) any such list or description constructed in response to an inquiry about a specific, named individual;

if the list or description is derived from individually identifiable health information collected in the course of providing a service described in subparagraph (A) to the consumer.

"(3) DISCLOSURE OF AGGREGATE LISTS.—A financial institution may not disclose any aggregate list of consumers containing or derived from individually identifiable health information to an affiliate or a nonaffiliated third party unless the financial institution has satisfied, for each consumer on the list, the requirements of clauses (i), (ii), and (iii) of paragraph (1)(A) with respect to the disclosure.

"(4) DISCLOSURE OF COVERAGE DENIAL OR MEDICAL EXAMINATION TEST RESULTS.—A financial institution may not disclose to an affiliate or a nonaffiliated third party whether or not a consumer has been denied life or health insurance coverage, or any medical examination test results, unless the financial institution has satisfied the requirements of clauses (i), (ii), and (iii) of paragraph (1)(A) with respect to the disclosure.

"(5) DISCLOSURE OF CONSENT INFORMATION.—A financial institution may not disclose to an affiliate or a nonaffiliated third party that a consumer has not provided consent under paragraph (1), (2), (3), or (4) unless the institution is authorized to disclose this information under another provision of this section.

"(6) EXCEPTIONS TO DISCLOSURE LIMITATIONS.—This section shall not restrict a financial institution from disclosing individually identifiable health information, or any other information described in paragraph (2)(B), (3), or (4)—

"(A) for a purpose described in paragraph (1), (2), (3), (5), (7), or (8) of section 502(e);

"(B) for purposes of maintaining and operating consolidated customer call centers, or providing consolidated customer account statements or other related services to customers;

"(C) to the institution's attorneys, accountants, and auditors, a State guaranty fund in connection with the resolution of an insolvent or impaired insurer, or an insurance rate advisory organization in connection with the establishment of rates for particular lines of insurance;

"(D) in connection with performing services for or functions solely on behalf of the financial institution with respect to the financial institution's own customers, including marketing of the financial institution's own products or services to the financial institution's customers; or

"(E) for purposes of underwriting, premium rating, reinsurance, or replacement of a group health plan (as defined in section 733 of the Employee Retirement Income Security Act of 1974 (29 U.S.C. 1191b)) or workers' compensation policy.

"(7) VOLUNTARY CONSENT.—A financial institution shall not condition provision of a financial product or service, or the terms of a financial product or service, on a consumer's affirmative consent to disclosure of individually identifiable

health information to an affiliate or a nonaffiliated third party for a purpose other than a purpose necessary for provision of the financial product or service.

"(8) LIMITS ON REDISCLOSURE AND REUSE OF INFORMATION.—

"(A) IN GENERAL.—Except as provided in subparagraph (B), an affiliate or a nonaffiliated third party that receives individually identifiable health information from a financial institution under this section shall not disclose such information to any other person, unless such disclosure would be lawful if made directly to such other person by the financial institution.

"(B) DISCLOSURE UNDER AN EXCEPTION.—Notwithstanding subparagraph (A), any person that receives individually identifiable health information from a financial institution in accordance with one of the exceptions in paragraph (6) may use or disclose such information only—

"(i) as permitted under that exception; or

"(ii) under another exception in such paragraph to carry out the purpose for which the information was disclosed by the financial institution.

"(9) CONSTRUCTION.—Except as provided in paragraph (6)(A), this section applies in lieu of subsections (b), (c), and (e) of section 502 to a disclosure by a financial institution of individually identifiable health information.

"(b) RULES FOR RECEIPT AND USE.—

"(1) IN GENERAL.—In deciding whether, or on what terms, to offer, provide, or continue to provide a financial product or service, other than insurance, to a consumer, a financial institution shall not request to receive individually identifiable health information about the consumer from an affiliate or nonaffiliated third party, or use, evaluate, or otherwise consider any such information, unless the financial institution—

"(A) has clearly and conspicuously requested in writing, in electronic form, or in another form permitted by the regulations implementing this subtitle, that the consumer affirmatively consent to such receipt and use; and

"(B) has obtained from the consumer such affirmative consent and such consent has not been withdrawn.

"(2) RESTRAINT ON INFORMATION REQUESTS.—In deciding whether, or on what terms, to offer, provide, or continue to provide a financial product or service, other than insurance, to a consumer, a financial institution shall not request the consent described in paragraph (1)(A) to receive individually identifiable health information available from an affiliate, unless the financial institution otherwise in the ordinary course of rendering the decision would, if that information were not available from an affiliate, request consent to receive the same or substantially similar information from a nonaffiliated third party.

"(c) CONSUMER RIGHTS TO ACCESS AND CORRECT INFORMATION.—

"(1) ACCESS.—

"(A) IN GENERAL.—Upon the request of a consumer, a financial institution shall make available to the consumer individually identifiable health information about the consumer that is within the possession of the financial institution.

"(B) EXCEPTIONS.—Notwithstanding subparagraph (A), a financial institution—

"(i) shall not be required to disclose to a consumer any confidential commercial information, such as an algorithm used to derive credit scores or other risk scores or predictors;

"(ii) shall not be required to create new records in order to comply with the consumer's request;

"(iii) shall not be required to disclose to a consumer any information assembled by the financial institution, in a particular matter, as part of the financial institution's efforts to comply with laws preventing fraud, money laundering, or other unlawful conduct, or otherwise to identify or investigate such conduct;

"(iv) shall not disclose any information required to be kept confidential by any other Federal law; and

"(v) shall not be required to disclose information (as specified in regulations promulgated by the Federal agencies referred to in section 504(a) in consultation with the Department of Health and Human Services) if the disclosure would endanger the life or physical safety of any individual or if the information was obtained under a promise of confidentiality from someone other than a health care provider and the disclosure would be likely to reveal that source.

"(C) ACCESS BY EXAMINED INDIVIDUAL TO RESULTS OF MEDICAL EXAMINATIONS.—

"(i) IN GENERAL.—A financial institution shall take such actions as are necessary to ensure that, in any case in which—

"(I) a medical examination of an individual is required for initial or continued enrollment under an insurance policy issued by the financial institution; and

"(II) the medical examination is conducted by a person who is in the employ of the institution or whose services are procured otherwise by the institution;

the individual (or the individual's legal guardian) is provided all medical information obtained from the examination at the same time that the information is made available to the financial institution and the individual is encouraged to make the information available to the individual's own physician.

"(ii) PROVISION TO PHYSICIAN.—Upon the request of an individual (or a legal guardian) described in clause (i), the information required to be provided to the individual or guardian under such clause shall be provided to the individual's physician instead of, or in addition to, the individual or guardian.

"(2) CORRECTION.—

"(A) OPPORTUNITY TO DISPUTE.—A financial institution shall provide a consumer the opportunity to dispute the accuracy of any individually identifiable health information disclosed to the consumer pursuant to paragraph (1), and to present evidence thereon.

"(B) AMENDMENT, CORRECTION, OR DELETION.—A financial institution—

"(i) shall amend, correct, or delete material information identified by a consumer that is materially incomplete or inaccurate; or

"(ii) shall notify the consumer of—

"(I) its refusal to make such amendment, correction, deletion;

"(II) the reasons for the refusal; and

"(III) the identity of the person who created the information and shall refer the consumer to that person for purposes of amending or correcting the information or filing with it a concise statement of what the consumer believes to be the correct information.

"(3) RULE OF CONSTRUCTION.—For purposes of this subsection, the term 'consumer', when used with respect to a financial institution, means a customer of the institution, or a person who has applied for and been denied a financial product or service by the institution.

"(4) COORDINATION AND CONSULTATION.—In prescribing regulations implementing this subsection, the Federal agencies specified in section 504(a) shall consult with one another to ensure that the regulations—

"(A) impose consistent requirements on the financial institutions under their respective jurisdictions;

"(B) take into account conditions under which financial institutions do business both in the United States and in other countries; and

"(C) are consistent with the principle of technology neutrality.

"(5) CHARGES FOR DISCLOSURES.—A financial institution may impose a reasonable, cost-based charge for making a disclosure under this subsection, which charge shall be disclosed to the consumer before making the disclosure.

"(6) NOTICE OF RIGHTS TO ACCESS AND CORRECT.—The disclosures required by section 503 shall include a statement of the consumer's right to access and correct individually identifiable health information in accordance with this subsection.

"(d) SPECIAL REQUIREMENTS TO PROTECT ESPECIALLY SENSITIVE HEALTH INFORMATION.—

"(1) SEPARATE CONSENT.—In any case in which this section requires a person to obtain a consumer's affirmative consent to the receipt, use, or disclosure of individually identifiable health information, the person shall obtain a separate and specific consent with respect to any information pertaining to—

"(A) mental health services requested or received by an individual;

"(B) human immunodeficiency virus (commonly known as HIV), acquired immune deficiency syndrome, or any other sexually transmitted disease;

"(C) genetic information;

"(D) reproductive health services requested or received by an individual; or

"(E) substance abuse treatment requested or received by an individual.

"(2) NO EXCEPTION TO DISCLOSURE LIMITATIONS FOR MARKETING PURPOSES.—Notwithstanding subsection (a)(6)(D), a financial institution may not disclose individually identifiable health information, or any other information described in paragraph (2)(B), (3), or (4) of subsection (a), for purposes of marketing the fi-

nancial institution's own products or services to the financial institution's customers, if the information pertains to a subject described in any of subparagraphs (A) through (E) of paragraph (1) of this subsection.

"(e) RELATIONSHIP TO OTHER LAWS.—Nothing in this section shall be construed as—

"(1) modifying, limiting, or superseding standards promulgated by the Secretary of Health and Human Services under—

"(A) part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.); or

"(B) section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191; 110 Stat. 2033);

"(2) applying to an activity, to the extent that the activity is subject to regulation under any of the provisions of law referred to in subparagraph (A) or (B) of paragraph (1); or

"(3) authorizing the use or disclosure of individually identifiable health information in a manner other than as permitted by other applicable law.

"(f) CIVIL LIABILITY.—

"(1) IN GENERAL.—Any financial institution which fails to comply with any provision of this section with respect to any disclosure or use of individually identifiable health information pertaining to any consumer shall be liable to the consumer in an amount equal to the sum of the amounts determined under each of the following subparagraphs:

"(A) COMPENSATORY DAMAGES.—The greater of—

"(i) the amount of any actual damage sustained by the consumer as a result of such failure; or

"(ii) any amount paid by the consumer to the financial institution.

"(B) GENERAL DAMAGES.—

"(i) INDIVIDUAL ACTIONS.—In the case of any action by an individual, such additional amount as the court may allow.

"(ii) CLASS ACTIONS.—In the case of a class action, the sum of—

"(I) the aggregate of the amount which the court may allow for each named plaintiff; and

"(II) the aggregate of the amount which the court may allow for each other class member, without regard to any minimum individual recovery.

"(C) ATTORNEYS' FEES.—In the case of any successful action to enforce any liability under subparagraph (A) or (B), the costs of the action, together with reasonable attorneys' fees.

"(2) FACTORS TO BE CONSIDERED IN AWARDING GENERAL DAMAGES.—In determining the amount of any liability of any person under paragraph (1)(B), the court shall consider, among other relevant factors—

"(A) the frequency and persistence of noncompliance by such person;

"(B) the nature of the noncompliance;

"(C) the extent to which such noncompliance was intentional; and

"(D) in the case of any class action, the number of consumers adversely affected.".

(b) DEFINITIONS.—Section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809) is amended by adding at the end the following:

"(12) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.—The term 'individually identifiable health information' means any information, including demographic information obtained from or about an individual, that is described in section 1171(6)(B) of the Social Security Act (42 U.S.C. 1320d(6)(B)).

"(13) GENETIC INFORMATION.—The term 'genetic information' means individually identifiable health information about genes, gene products, or inherited characteristics that may derive from an individual or a family member of an individual (including information about a request for or receipt of genetic services by an individual or a family member of an individual).".

(c) CLERICAL AMENDMENT.—The table of contents for the Gramm-Leach-Bliley Act is amended by inserting after the item relating to section 502 the following:

"Sec. 502A. Special rules for health information.".

SEC. 3. REGULATIONS; EFFECTIVE DATE.

(a) REGULATIONS.—

(1) REGULATORY AUTHORITY.—Section 504(a) of the Gramm-Leach-Bliley Act (15 U.S.C. 6804(a)) shall apply to the issuance of regulations to carry out the amendments made by this Act in the same manner as such section applies to the issuance of other regulations to carry out subtitle A of title V of the Gramm-Leach-Bliley Act, except as provided in paragraph (4).

(2) AUTHORITY TO GRANT EXCEPTIONS.—The regulations issued to carry out the amendments made by this Act may include such additional exceptions to the provisions of section 502A of the Gramm-Leach-Bliley Act, as inserted by section 2, as are deemed consistent with the purposes of subtitle A of title V of such Act, except as provided in paragraph (3)(B).

(3) SPECIAL PROTECTIONS FOR ESPECIALLY SENSITIVE HEALTH INFORMATION.—

(A) IN GENERAL.—The regulations issued to carry out the amendments made by this Act shall, where appropriate, include special policies and procedures to protect the confidentiality of individually identifiable health information pertaining to—

(i) mental health services requested or received by an individual;

(ii) human immunodeficiency virus (commonly known as HIV), acquired immune deficiency syndrome, and any other sexually transmitted disease;

(iii) genetic information;

(iv) reproductive health services requested or received by an individual; and

(v) substance abuse treatment requested or received by an individual.

(B) AUTHORITY TO GRANT EXCEPTIONS.—The regulations issued to carry out the amendments made by this Act may not include any exception to the provisions of section 502A of the Gramm-Leach-Bliley Act, as inserted by section 2, that diminishes the protection afforded by such section to the confidentiality of individually identifiable health information pertaining to—

(i) mental health services requested or received by an individual;

(ii) human immunodeficiency virus (commonly known as HIV), acquired immune deficiency syndrome, or any other sexually transmitted disease;

(iii) genetic information;

(iv) reproductive health services requested or received by an individual; or

(v) substance abuse treatment requested or received by an individual.

(4) DEADLINE.—Regulations to carry out the amendments made by this Act shall be issued in final form not later than 6 months after the date of the enactment of this Act.

(b) EFFECTIVE DATE.—The amendments made by this Act shall take effect 6 months after the date on which regulations are required to be issued under subsection (a)(4), except to the extent that a later date is specified in such regulations.

PURPOSE AND SUMMARY

The purpose of H.R. 4585, the Medical Financial Privacy Protection Act, is to strengthen consumers' control over the use and disclosure of their health information by financial institutions. The legislation requires financial institutions to obtain a consumer's affirmative consent before disclosing any individually identifiable health information about that consumer to an affiliate or non-affiliated third party, and prohibits financial institutions from obtaining such information from an affiliate or non-affiliated third party or using such information in deciding whether or on what terms to offer a consumer a financial product or service (other than insurance), unless the consumer consents to such receipt or use.

In addition to the general prohibition on sharing individually identifiable health information stated above, consent is specifically required for the following disclosures to affiliates or non-affiliated third parties: (1) a list or description of a consumer's personal spending habits derived from individually identifiable health information; (2) an aggregate list of consumers derived from individually identifiable health information; (3) whether a consumer has been denied life or health insurance coverage; and (4) medical examination test results. The legislation prohibits financial institutions from disclosing to an affiliate or non-affiliated third party that a consumer has refused to consent to the disclosure of individually identifiable health information.

The legislation outlines certain circumstances in which individually identifiable health information may be disclosed without consumer consent, including for insurance underwriting purposes, to service a financial product or service requested or authorized by a consumer, to protect against or prevent fraud, to comply with Federal, State, or local laws or regulations, or in connection with performing services for or functions solely on behalf of a financial institution with respect to that institution's own customers.

The legislation prohibits a financial institution from conditioning the availability of a product or service on a consumer's affirmative consent to disclosure of individually identifiable health information to an affiliate or a non-affiliated third party for a purpose other than that which is necessary to provide the product or service.

A party that receives individually identifiable health information from a financial institution is prohibited from disclosing the information to any other person, unless the financial institution itself could have legally made the disclosure directly to the person. If a person receives individually identifiable health information from a financial institution pursuant to one of the specified exceptions, the person can only use the information as permitted under that exception, or under another exception to carry out the purpose for which the information was initially disclosed.

The recently enacted Gramm-Leach-Bliley Act permits mergers between insurance companies and depository institutions, giving rise to concerns that banks could obtain individually identifiable health information from an affiliated insurer and use the information to make lending or other financial decisions. To address this concern, the legislation prohibits a financial institution from even requesting a consumer's consent to receive health information from an affiliate, unless the institution would ordinarily request consent to receive the same or substantially similar information from a non-affiliated third party, were the information not available from its affiliate.

The legislation gives consumers the right to inspect, copy, and seek corrections to individually identifiable health information that is in the possession of a financial institution. This right of access and correction can be asserted by customers of the financial institution, as well as by consumers who are not customers but who have applied for and been denied a financial product or service by the institution. The materials that a financial institution must make available for a consumer's inspection need not include certain categories of information, including confidential commercial information, information assembled by the institution as part of its efforts to comply with laws preventing fraud, money laundering or other unlawful conduct, or information the disclosure of which would endanger the life or physical safety of any individual. Financial institutions are authorized to impose a reasonable, cost-based charge for gathering, producing and copying individually identifiable health information pursuant to a consumer's request, which charge must be disclosed in advance to the consumer.

In cases where a financial institution requires an applicant for initial or continued insurance coverage to undergo a medical examination administered by a health care provider employed or retained by the financial institution, the legislation requires that the results of such examination be provided to the consumer (and/or

the consumer's physician if the consumer so directs) at the same time that the information is made available to the financial institution.

The legislation contains the following special protections for individually identifiable health information pertaining to mental health services, HIV/AIDS or other sexually transmitted diseases, genetic information, reproductive health services, or substance abuse treatment: (1) financial institutions are required to obtain separate and specific consent from the consumer prior to the receipt, use or disclosure of such information; (2) financial institutions are prohibited from sharing such information under the exception permitting disclosure for the purposes of marketing their own products to their own customers; and (3) the relevant regulatory agencies are directed to adopt, where appropriate, special policies and procedures to protect the confidentiality of such information, and are explicitly precluded from granting exceptions to the consent requirements established by the legislation that would diminish the protections afforded such information.

The legislation imposes civil liability on financial institutions that fail to comply with its provisions governing the use or disclosure of individually identifiable health information. Consumers harmed by a financial institution's failure to comply may recover compensatory and other damages, as well as the costs of the litigation, including reasonable attorneys' fees.

The legislation does nothing to modify, limit or supersede medical privacy standards promulgated by the Secretary of Health and Human Services (HHS) pursuant to authority granted under the Health Insurance Portability and Accountability Act, and specifically exempts activities already subject to HHS regulations.

BACKGROUND AND NEED FOR LEGISLATION

The Gramm-Leach-Bliley Act, signed into law on November 12, 1999, contained far-reaching privacy protections for financial information, including provisions enabling customers of financial institutions, for the first time, to "opt out" of having their personal financial information shared with unaffiliated third parties; requiring all financial institutions to disclose annually to all customers, in clear and conspicuous terms, their policies and procedures for protecting customers' nonpublic personal information; and barring financial institutions from disclosing customer account numbers or access codes to unaffiliated third parties for telemarketing or other direct marketing purposes.

Public opinion polling data and other evidence suggest that Americans' strong interest in preserving their personal privacy in an era of staggering technological change applies with particular force to information relating to the health and medical condition of an individual or a family member. Health care providers and the insurance industry plainly need access to health information in order to provide the medical care an individual needs and to perform basic business functions related to the underwriting and claims processes. But with the potential for mergers between insurance companies and other financial firms increasing in today's marketplace—and with technological advances facilitating broader dissemination of information—concerns have been raised about the

sharing of medical information among financial affiliates and with non-affiliated third parties.

Lack of confidence in the financial services industry's ability to protect the confidentiality of personal health information has potentially devastating consequences for the health care delivery system. Individuals who come to believe that their medical privacy is not being adequately protected by those institutions that have access to their health records are less likely to be candid with medical professionals about their health. A recent survey by the California Health Care Foundation found that one in six patients engages in some form of "privacy-protective behavior," defined to include providing inaccurate information to their doctors, "doctor-hopping" to avoid a consolidated medical record, paying out of pocket for care that is insured, and even avoiding care completely.

Although there is no conclusive evidence of widespread industry abuses or unauthorized disclosures of personal health information, potential for misuse of such information exists, especially now with scientific advances that allow so much more to be known and predicted about individuals based upon medical and genetic testing. H.R. 4585 addresses consumers' fundamental concerns about threats to their medical privacy, while at the same time permitting legitimate uses of medical information for insurance and other business purposes that benefit these same customers.

HEARINGS

H.R. 4585, the Medical Financial Privacy Protection Act, was introduced on June 6, 2000, by Chairman Leach. On June 14, 2000, the Committee held a hearing on the legislation. Testifying at the hearing were Gary Gensler, Under Secretary for Domestic Finance, Department of the Treasury; Kathleen Sebelius, Commissioner of Insurance for Kansas, Vice President, National Association of Insurance Commissioners; Richard K. Harding, President-elect, American Psychiatric Association, Vice Chair, Clinical Affairs and Professor of Psychiatrics and Pediatrics, University of South Carolina School of Medicine; Steve Bartlett, President, Financial Services Roundtable; Don Brain, President of Lockton Benefit Company, Kansas City, Missouri on behalf of the Independent Insurance Agents of America; Robert H. Rheel, Senior Vice President, Fireman's Fund, on behalf of the American Insurance Association; Edward L. Yingling, Deputy Executive Vice President, American Banker's Association; Robbie Meyer, Senior Counsel, American Council of Life Insurance; Nicole Beason, Esther Peterson Fellow, Consumers Union; A.G. Breitenstein, Chief Privacy Officer, ChoosingHealth.com; Evan Hendricks, Editor and Publisher, Privacy Times; Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group; Joy L. Pritts, Senior Counsel, Health Privacy Group, Georgetown University; and Ronald Weich, Attorney, Zuckerman, Spaeder, Goldstein, Taylor and Kolker, LLP on behalf of the American Civil Liberties Union.

COMMITTEE CONSIDERATION AND VOTES

On June 29, 2000, the Committee met in open session to mark up H.R. 4585, the Medical Financial Privacy Protection Act. The

Committee called up a Committee print as original text for purposes of amendment.

During consideration of the bill, the Committee approved a Manager's Amendment by voice vote that:

• Clarifies that consumers have a right to withdraw their consent to the disclosure of individually identifiable health information, except to the extent that the financial institution has taken action in reliance thereon.

• Clarifies that customer consent need not be obtained for disclosures of individually identifiable health information for purposes of maintaining and operating consolidated customer call centers, or providing consolidated customer account statements or other related services to customers.

• Clarifies that the provision permitting disclosure without consumer consent of individually identifiable health information to state guaranty funds in connection with the resolution of an insolvent insurer also applies to impaired insurance companies.

• Clarifies that the provision permitting disclosure without consumer consent of individually identifiable health information for purposes of a group health plan or workers compensation policy is limited to underwriting, premium rating, reinsurance or replacement purposes.

• Provides that the information that must be made available to a consumer who has requested access to individually identifiable health information in the possession of a financial institution need not include information assembled by a financial institution in investigating or identifying fraud, money laundering, or other unlawful conduct.

• Gives Federal regulators authority, in consultation with the Department of Health and Human Services, to prescribe regulations limiting a financial institution's obligation to make available for a consumer's inspection and correction information which would endanger the life or physical safety of any individual, or was obtained under a promise of confidentiality from someone other than a health care provider whose identity would likely be revealed by the disclosure to the consumer.

• Provides that the right to access and correct individually identifiable health information in the possession of a financial institution can be exercised by customers of the institution, as well as by consumers who are not customers but who have applied for and been denied a financial product or service by the institution.

• Requires that a financial institution's privacy policy disclosure under Title V of Gramm-Leach-Bliley include a statement of the consumer's right to access and correct individually identifiable health information.

The following additional actions were taken by voice vote unless roll call vote is noted:

AMENDMENTS APPROVED

• An amendment, as amended, offered by Mr. Bentsen, expanding the prohibition on a financial institution obtaining or using individually identifiable health information from an affiliate or nonaffiliated third party in deciding whether to provide a loan or credit to include any financial product or service, other than insurance.

• An amendment, as amended, offered by Mrs. Maloney, prohibiting financial institutions from disclosing the fact that a consumer has withheld consent to disclosure of individually identifiable health information.

• An amendment offered by Mrs. Kelly and Mr. Watt, clarifying language of the manager's amendment regarding withdrawal by a customer of consent to disclosure of individually identifiable health information.

• An amendment, as amended, offered by Mrs. Biggert, clarifying that the bill does not reach activity governed by proposed Department of Health and Human Services regulations.

• An amendment offered by Mr. Bentsen and others, adding "genetic information" to the category of information subject to disclosure only with the customer's separate and specific consent.

• An amendment, as amended, offered by Ms. Schakowsky and Mrs. Maloney, adding reproductive health and substance abuse treatment to the category of especially sensitive information as to which separate and specific consumer consent must be obtained, and not allowing such information to be shared for marketing purposes without such consent. The amendment was approved 24 to 5.

YEAS	NAYS	PASS
Mr. Leach	Mr. Metcalf	Mr. Lucas
Mrs. Roukema	Mr. Barr	
Mr. Baker	Mr. Ryun of Kansas	
Mr. Campbell	Mr. Terry	
Mr. Hill	Mr. Green	
Mr. LaFalce		
Mr. Frank		
Ms. Waters		
Mrs. Maloney		
Mr. Gutierrez		
Mr. Watt		
Mr. Ackerman		
Mr. Bentsen		
Mr. Maloney		
Ms. Hooley		
Mr. Sandlin		
Mr. Meeks, G.		
Ms. Lee		
Mr. Mascara		
Mr. Inslee		
Ms. Schakowsky		
Mr. Moore		
Mrs. Jones		
Mr. Capuano		

• An amendment offered by Mr. Watt, clarifying that fees charged by financial institutions for retrieving individually identifiable health information for consumers should be cost based.

• An amendment offered by Mr. Watt clarifying the scope of the special treatment afforded certain kinds of sensitive health information.

• An amendment, as amended, offered by Mr. Ackerman, requiring the disclosure of medical examination results to consumers by insurance companies in certain circumstances, and prohibiting disclosure of whether a consumer has been denied life or health insurance coverage and of medical examination test results.

• An amendment offered by Mr. LaFalce, to provide that a financial institution shall not condition provision of a financial product or service on a consumer's affirmative consent to release of health information.

• An amendment offered by Mr. LaFalce to provide for a private right of action by consumers if individually identifiable health information is misused.

AMENDMENTS DEFEATED

• The Committee defeated an amendment by Mr. LaFalce making two changes to the Committee Print. First, the LaFalce amendment would have struck the exception in the Committee Print allowing a financial institution to share information in connection with performing services for or functions solely on behalf of the financial institution without consumer consent. Second, the LaFalce amendment would have added a provision prohibiting a financial institution from denying a financial product or service to a consumer because the consumer refuses to consent to the disclosure of individually identifiable health information. The amendment, as amended, was defeated by a vote of 16–16.

YEAS	NAYS
Dr. Weldon	Mr. Leach
Mr. LaFalce	Mrs. Roukema
Mr. Frank	Mr. Bereuter
Mr. Sanders	Mr. Baker
Mrs. Maloney	Mr. Castle
Mr. Watt	Mr. Campbell
Mr. Ackerman	Mr. Barr
Mr. Bentsen	Mr. Ryun of Kansas
Mr. Maloney	Mr. Hill
Ms. Carson	Mr. Ryan of Wisconsin
Mr. Meeks, G.	Mr. Ose
Ms. Lee	Mr. Sweeney
Mr. Inslee	Mrs. Biggert
Ms. Schakowsky	Mr. Terry
Mr. Moore	Mr. Green
Mr. Capuano	Mr. Toomey

The Committee tabled, on a vote of 20 to 15, a motion appealing the ruling of the chair that an amendment offered by Mr. Inslee was not germane to the bill. The amendment would have applied the opt-in provisions applicable to individually identifiable health information to all forms of non-public personal information. The motion to table was offered by Mrs. Roukema.

YEAS	NAYS
Mr. Leach	Mr. LaFalce
Mrs. Roukema	Ms. Waters
Mr. Bereuter	Mrs. Maloney
Mr. Baker	Ms. Velazquez
Mr. Castle	Mr. Watt
Mr. Campbell	Mr. Ackerman
Mr. Lucas	Mr. Meeks, G.
Mr. Metcalf	Ms. Lee
Mr. Barr	Mr. Mascara
Dr. Paul	Mr. Inslee
Mr. Ryun of Kansas	Ms. Schakowsky
Mr. Hill	Mr. Moore
Mr. Terry	Mr. Gonzalez
Mr. Green	Mrs. Jones
Mr. Toomey	Mr. Capuano
Mr. Frank	
Mr. Bentsen	
Mr. Maloney	
Ms. Hooley	
Mr. Sherman	

The Committee Print, as amended, was adopted by voice vote. Subsequently, H.R. 4585, as amended, was adopted and ordered favorably reported to the House by a vote of 26–14–1.

YEAS	NAYS	PASS
Mr. Leach	Mr. Bereuter	Dr. Weldon
Mrs. Roukema	Mr. Baker	
Mr. Castle	Mr. Metcalf	
Mr. Royce	Mr. Ney	
Mr. LaFalce	Mr. Barr	
Mr. Frank	Mrs. Kelly	
Mr. Kanjorski	Dr. Paul	
Ms. Waters	Mr. Ryun of Kansas	
Mrs. Maloney	Mr. Hill	
Mr. Gutierrez	Mr. Manzullo	
Ms. Velazquez	Mr. Ryan of Wisconsin	
Mr. Watt	Mrs. Biggert	
Mr. Ackerman	Mr. Terry	
Mr. Bentsen	Mr. Green	
Ms. Carson		
Mr. Weygand		
Mr. Sherman		
Mr. Meeks, G.		
Ms. Lee		
Mr. Mascara		
Mr. Inslee		
Ms. Schakowsky		
Mr. Moore		
Mrs. Jones		
Mr. Capuano		
Mr. Forbes		

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee reports that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT FINDINGS

As provided for in clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, no oversight findings have been submitted to the Committee by the Committee on Government Reform.

CONSTITUTIONAL AUTHORITY

In compliance with clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Constitutional Authority of Congress to enact this legislation is derived from Article I, section 8, clause 1 (relating to the general welfare of the United States); Article I, section 8, clause 3 (relating to Congressional power to regulate commerce); Article 1, section 8, clause 5 (relating to the power "to coin money" and "regulate the value thereof"); and Article I, section 8, clause 18 (relating to making all laws necessary and proper for carrying into execution powers vested by the Constitution in the government of the United States).

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

Clause 3(c)(2) of rule XIII of the Rules of the House of Representatives is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

CONGRESSIONAL ACCOUNTABILITY ACT

The reporting requirement under section 102(b)(3) of the Congressional Accountability Act (P.L. 104–1) is inapplicable because this legislation does not relate to terms and conditions of employment or access to public services or accommodations.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE AND UNFUNDED MANDATES ANALYSIS

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 14, 2000.

Hon. JAMES A. LEACH,
Chairman, Committee on Banking and Financial Services, House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 4585, the Medical Financial Privacy Protection Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Mark Hadley (for federal costs) and Stuart Hagen (for the private-sector impact).

Sincerely,

BARRY B. ANDERSON
(For Dan L. Crippen, Director).

Enclosure.

H.R. 4585—Medical Financial Privacy Protection Act

Summary: H.R. 4585 would establish rules for financial institutions concerning the confidentiality of customers' medical information. The bill would prohibit financial institutions from disclosing a customer's health information without his or her affirmative consent. The Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), and the National Credit Union Administration (NCUA) would enforce the provisions of H.R. 4585 as it applies to the financial institutions that those agencies now regulate.

CBO estimates that implementing this legislation would not result in any significant cost to the federal government. Because enactment of H.R. 4585 would affect direct spending and receipts, pay-as-you-go procedures would apply to the bill. However, CBO estimates that any impact on direct spending and receipts would not be significant.

H.R. 4585 contains no intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would not affect the budgets of state, local, or tribal governments.

The bill would impose several new private-sector mandates on financial institutions that hold or handle health information about individuals. However, CBO cannot determine whether the direct cost of those requirements would exceed the statutory threshold for private-sector mandates specified in UMRA ($109 million in 2000, adjusted annually for inflation). How regulators would implement certain provisions in the bill is very uncertain, and little information is available as to how some of the mandates would affect the operation of financial institutions.

Estimated cost to the Federal Government: Based on information from the NCUA, CBO estimates that implementing H.R. 4585 would increase administrative costs at the agency, but any such costs would be negligible.

Both the OTS and the OCC charge fees to cover all their administrative costs; therefore, any additional spending by those agencies to implement the bill would have no net budgetary effect. That is not the case with the FDIC, however, which uses deposit insurance premiums paid by all banks to cover the expenses it incurs to supervise state-chartered banks. The bill would cause a small increase in FDIC spending, but would not affect its premium income. Overall, CBO estimates that H.R. 4585 would increase direct spending and offsetting receipts for the OTS, OCC, and FDIC by less than $500,000 a year over the 2001–2005 period.

Budgetary effects on the Federal Reserve are recorded as changes in revenues (governmental receipts). Based on information from the Federal Reserve, CBO estimates that enacting H.R. 4585

would reduce such revenues by less than $500,000 a year over the 2001–2005 period.

Pay-as-you-go considerations: The Balanced Budget and Emergency Deficit Control Act sets up pay-as-you-go procedures for legislation affecting direct spending or receipts. Enacting H.R. 4585 would affect both direct spending and receipts, but CBO estimates that any such effects would be negligible.

Estimated impact on state, local, and tribal governments: H.R. 4584 contains no intergovernmental mandates as defined in UMRA and would not affect the budgets of state, local, or tribal governments.

Estimated impact on the private sector: H.R. 4585 would require financial institutions that hold or handle individually identifiable health information (IIHI) to abide by several new mandates. The bill would require financial institutions to:

- Obtain affirmative consent from customers whose IIHI the financial institution intends to share with an affiliate or nonaffiliated third party;
- Allow customers the right to review, inspect, and correct IIHI held by the financial institution; and
- Obtain separate, affirmative consent from customers to share IIHI that is especially sensitive, such as information pertaining to mental health services and genetic information.

For reasons described below, CBO cannot determine whether the direct cost of those mandates would exceed the threshold specified in UMRA for private-sector costs ($109 million in 2000, adjusted annually for inflation).

Affirmative Consent. While the bill would require financial institutions to obtain the customers' consent to share IIHI with affiliates or nonaffiliated third parties, it would exempt many uses of that information from the mandate. In general, those exceptions would enable financial institutions to use IIHI without consent for the purposes for which the information was collected, such as in calculating premium rates for insurance products, or to provide consolidated products and services to their customers, such as customer call centers or consolidated billing. According to industry sources, few current practices of financial institutions would require affirmative consent under the bill. However, CBO is uncertain as to whether changes in the financial services industry permitted by the recently enacted Gramm-Leach-Bliley Act (such as allowing financial institutions to affiliate with securities and insurance companies) will lead institutions to expand their uses of personal health information.

Consumers' Right to Review. The cost of the mandate to allow consumers to review information held by financial institutions would depend on how it would be interpreted by regulatory agencies. A broad interpretation of the type of information a consumer could be granted access to might include any IIHI located anywhere in the financial institution, including, for example, canceled checks or credit card slips payable to health care providers. A request for information of that kind could require potentially time-consuming and expensive searches. On the other hand, if the access to information was limited to IIHI contained in a consolidated record created for the purpose of storing IIHI or that was used to

make a business decision directly affecting the consumer, then the cost could be relatively low.

A provision in the bill allowing institutions to charge a "reasonable, cost-based" fee to consumers for providing this information would reduce the net cost of the mandate. The extent of that reduction would depend on the breadth of consumers' access to their IIHI and on what costs would be offset by the fee. If the broader definition of the type of information to be made available were applicable, then institutions might have to develop new systems for collecting all forms of IIHI. If the fee provision applied only to the marginal costs of collection the information for the requesting consumer, then the institution might not be able to recover the fixed costs of developing the new systems. This could significantly raise the costs of complying with the bill. Once new systems are in place, the marginal costs of allowing the consumer to review and correct IIHI might be fully offset by the fee.

Consent to Share Sensitive Information. The cost to financial institutions of requiring separate consent to share sensitive information would depend in part on how regulatory agencies interpret the categories of information for which separate consent is required. Specifically, the term "genetic information" might be interpreted more or less expansively by regulators, potentially affecting the scope of information included in this category.

Estimate prepared by: Federal Costs: Mark Hadley. Revenues: Carolyn Lynch. Impact on State, Local, and Tribal Governments: Shelley Finlayson. Impact on the Private Sector: Stuart Hagen.

Estimate approved by: Robert A. Sunshine, Assistant Director for Budget Analysis.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title

The short title of the bill is the "Medical Financial Privacy Protection Act."

Section 2. Use and disclosure of health information by financial institutions

Section 2(a) amends the Gramm-Leach-Bliley Act by adding a new section 502A. Section 502A(a)(1) prohibits financial institutions from disclosing any individually identifiable health information to an affiliate or non-affiliated third party unless (1) the consumer has been provided with a clear and conspicuous notice of the categories of information that may be disclosed and the categories of parties to whom it is disclosed; (2) the financial institution has clearly and conspicuously requested that the consumer affirmatively consent to such disclosure; and (3) the consumer has consented to such disclosure and that consent has not been withdrawn.

Section 502A(a)(2)–(4) outlines specific categories of information as to which a consumer's consent must be received before the information is disclosed to an affiliate or non-affiliated third party:

> (1) a list or description of a consumer's personal spending habits derived from individually identifiable health information collected by a financial institution in the course of providing a service to a consumer through which the consumer makes or

receives payments or transfers by check, debit card, credit card, or other similar instrument;

(2) an aggregate list of consumers containing or derived from individually identifiable health information;

(3) whether a consumer has been denied life or health insurance coverage; and

(4) medical examination test results.

Section 502A(a)(5) prohibits a financial institution from disclosing to an affiliate or non-affiliated third party the fact that a consumer has refused to consent to the disclosure of individually identifiable health information.

Section 502A(a)(6) outlines certain exceptions pursuant to which individually identifiable health information may be disclosed by a financial institution to an affiliate or non-affiliated third party without first obtaining customer consent. The section incorporates certain exceptions enumerated in section 502(e) of the Gramm-Leach-Bliley Act, as well as the following additional exceptions:

(1) for purposes of maintaining and operating consolidated customer call centers, or providing consolidated customer account statements or other related services to customers who request information about their accounts with a financial institution;

(2) to a financial institution's attorneys, accountants, and auditors, a State insurance guaranty fund in connection with an insolvent or impaired insurer, or an insurance rate advisory organization in connection with the establishment of rates for particular lines of insurance;

(3) in connection with performing services for or functions solely on behalf of a financial institution with respect to the institution's own customers, including marketing of the institution's own products or services to its customers; and

(4) for purposes of underwriting, premium rating, reinsurance, or replacement of a group health plan (as defined in section 733 of the Employee Retirement Income Security Act of 1974 (29 U.S.C. §1191(b)) or workers' compensation policy.

With regard to the last exception, aggregated data, in lieu of individually identifiable information, should be used to the maximum extent possible to achieve the purposes provided for in section 502A(a)(6)(E).

Section 502A(a)(7) prohibits a financial institution from conditioning the availability of a product or service, or its terms, on a consumer's affirmative consent to disclosure of individually identifiable health information to an affiliate or a non-affiliated third party for a purpose other than that which is necessary to provide the product or service.

Section 502A(a)(8) places strict limitations on the redisclosure and reuse of individually identifiable health information. It prohibits an affiliate or non-affiliated third party that receives individually identifiable health information from a financial institution from disclosing the information to any other person, unless the disclosure would be lawful if made directly to such other person by the financial institution. It further provides that where a person receives individually identifiable health information from a financial institution pursuant to one of the exceptions contained in section 502A(a)(6), the person can only use the information as permitted

under that exception, or under another exception specified in section 502A(a)(6) to carry out the purpose for which the information was initially disclosed by the financial institution.

Section 502A(a)(9) clarifies that disclosures of individually identifiable health information by financial institutions are governed by this section in lieu of sections (b), (c), and (e) of section 502 of the Gramm-Leach-Bliley Act, except to the extent that certain exceptions contained in section 502(e) are incorporated by reference.

Section 502A(b) sets forth the rules governing receipt and use of individually identifiable health information. Section 502A(b)(1) provides that in deciding whether, or on what terms, to offer, provide, or continue to provide a financial product or service, other than insurance, to a consumer, a financial institution shall not request to receive individually identifiable health information about the consumer from an affiliate or non-affiliated third party, or use, evaluate, or otherwise consider any such information, without first obtaining the consumer's affirmative consent. Section 502A(b)(2) prohibits a financial institution from even requesting a consumer's consent to receive health information from an affiliate, unless the institution would ordinarily request consent to receive the same or substantially similar information from a non-affiliated third party, were the information not available from its affiliate.

Section 502A(c) requires that, upon a consumer's request, a financial institution must provide the consumer with access to, and the opportunity to correct, their individually identifiable health information in the possession of the financial institution, subject to the following exceptions:

(1) A financial institution shall not be required to disclose to a consumer any confidential commercial information;

(2) A financial institution shall not be required to create new records in order to comply with a consumer's request;

(3) A financial institution shall not be required to disclose to a consumer any information assembled by the financial institution, in a particular matter, in an effort to comply with laws preventing fraud, money laundering, or other unlawful conduct, or otherwise to identify or investigate such conduct;

(4) A financial institution shall not disclose any information required to be kept confidential by any other Federal law; and

(5) A financial institution shall not be required to disclose information if the disclosure would endanger the life or physical safety of any individual or if the information was obtained under a promise of confidentiality from someone other than a health care provider and the disclosure would be likely to reveal that source.

Section 502A(c)(1)(C) provides that in instances where a financial institution requires an individual who is seeking initial or continued enrollment under an insurance policy to undergo a medical examination administered by a person employed or retained by the financial institution, the results of such examination must be provided to the individual or the individual's legal guardian (and/or the consumer's physician if the consumer so directs) at the same time that the information is made available to the financial institution.

Section 502A(c)(2) affords consumers the right to dispute the accuracy of any individually identifiable health information disclosed

by a financial institution pursuant to this section, and requires the financial institution to amend, correct, or delete material information that is materially incomplete or inaccurate, or notify the consumer of its refusal to make such amendment, correction, or deletion. In the latter scenario, the financial institution is required to state its reasons for refusing to take the action requested by the consumer, and to identify the person who created the information and refer the consumer to that person for purposes of amending or correcting the information or filing with it a concise statement of what the consumer believes to be the correct information.

Section 502A(c)(3) limits the class of individuals who can assert the right to access and correct individually identifiable health information to customers of the financial institution that possesses the information, and consumers who are not customers but who have applied for and been denied a financial product or service by the institution.

Section 502A(c)(4) directs the Federal agencies responsible for implementing the access and correction rights afforded consumers by this section to consult with one another to ensure that the regulations each prescribes impose consistent requirements on financial institutions; take into account conditions under which financial institutions do business in the United States and in other countries; and are consistent with the principle of technology neutrality.

Section 502A(c)(5) authorizes financial institutions to charge consumers a reasonable, cost-based fee for making disclosures of individually identifiable health information pursuant to this subsection, which charge must be disclosed to the consumer in advance. Given the potentially expansive reach of the bill's definition of "individually identifiable health information," a financial institution's search for information needed to comply with a request made pursuant to this subsection might have the effect of imposing significant costs on the consumer, thereby discouraging such requests and thwarting the intent of this provision. Accordingly, in prescribing regulations implementing this section, the Federal agencies identified in section 504(a) of the Gramm-Leach-Bliley Act should develop reasonable classifications of the types of information required to be made available for review and correction by the consumer.

For example, a financial institution's obligation under this section would clearly extend to individually identifiable health information specific to the consumer, such as medical records or files, information relating to medical test results, or aggregated data describing a consumer's purchases of medical products or services. By the same token, the provision is not intended to require financial institutions to search for individually identifiable health information that may appear in uncollected, unaggregated records reflecting a consumer's expenditures, such as checks, or credit or debit card receipts or statements.

Section 502A(c)(6) provides that in disclosing their privacy policies pursuant to section 503 of the Gramm-Leach-Bliley Act, financial institutions must include a statement of the consumer's right to access and correct individually identifiable health information pursuant to this subsection. The Committee recognizes that imposing this disclosure obligation on financial institutions that do not collect, use or have access to individually identifiable health infor-

mation potentially could have a disruptive effect on the financial institutions' relationships with customers. For example, an institution required to make such disclosure even though it had no individually identifiable health information in its possession could create suspicion and unwarranted concerns among its customers. The Federal agencies specified in section 504(a) of the Gramm-Leach-Bliley Act should take this potential for consumer misunderstanding into account when prescribing regulations implementing this provision.

Section 502A(d) requires that in those instances in which a consumer's affirmative consent is a prerequisite to the receipt, use, or disclosure of individually identifiable health information, a separate and specific consent must be obtained with respect to any information pertaining to (1) mental health services requested or received by an individual; (2) HIV/AIDS or any other sexually transmitted disease; (3) genetic information; (4) reproductive health services requested or received by an individual; or (5) substance abuse treatment requested or received by an individual. The subsection also prohibits financial institutions from disclosing individually identifiable health information relating to these five subjects for purposes of marketing their own products or services to their customers.

Section 502A(e) clarifies the new section's relationship to other laws. Nothing in the new section is to be construed as (1) modifying, limiting, or superseding standards promulgated by the Secretary of Health and Human Services under part C of title XI of the Social Security Act or section 264(c) of the Health Insurance Portability and Accountability Act; (2) applying to an activity that is subject to regulation by the Secretary of Health and Human Services under those statutory directives; or (3) authorizing the use or disclosure of health information in a manner other than as permitted by applicable law.

Section 502A(f) authorizes the imposition of civil liability against institutions that fail to comply with any provision of the section with respect to disclosure or use of individually identifiable health information. A consumer harmed by a financial institution's noncompliance may recover compensatory damages, general damages, and litigation costs, including reasonable attorneys' fees. In awarding general damages pursuant to this subsection, courts are required to consider, among other relevant factors, the frequency, persistence, and nature of the noncompliance; the extent to which the noncompliance was intentional; and, in class actions, the number of consumers adversely affected.

Section 2(b) amends Section 509 of the Gramm-Leach-Bliley Act by adding definitions of the terms "individually identifiable health information" and "genetic information." The term "individually identifiable health information" is defined as any information, including demographic information obtained from or about an individual, that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual, and identifies the individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. The term "genetic information" is defined as individually identifiable health

information about genes, gene products, or inherited characteristics that may derive from an individual or family member of an individual (including information about a request for or receipt of genetic services by an individual or family member of an individual). To avoid unintended overlap with the definition of "individually identifiable health information," the term "genetic information" is not intended to include information about the sex or age of an individual; information about chemical, blood, or urine analyses of the individual, unless these analyses are genetic tests; or information about physical examinations of an individual, and other information relevant to determining the current health status of the individual.

Section 3. Regulations; effective date

This section clarifies that the regulatory authority granted by section 504(a) of the Gramm-Leach-Bliley Act extends to the amendments made by this legislation, and that the regulations issued to implement those amendments may include such additional exceptions to new section 502A as are deemed consistent with the purposes of subtitle A of title V of the Gramm-Leach-Bliley Act.

This section also contains additional protections for the especially sensitive health information identified in new section 502A. Specifically, the section requires that where appropriate, the regulations implementing the amendments made by the legislation must include special policies and procedures for protecting the confidentiality of individually identifiable health information pertaining to (1) mental health services requested or received by an individual; (2) HIV/AIDS or any other sexually transmitted disease; (3) genetic information; (4) reproductive health services requested or received by an individual; or (5) substance abuse treatment requested or received by an individual. In addition, the implementing regulations may not include any exception to the provisions of section 502A that has the effect of diminishing the protection afforded these five categories of particularly sensitive information.

Finally, this section requires regulations to carry out the amendments of the new section to be issued not later than six months after the date of enactment. The amendments made by the new section shall take effect six months after the date on which the regulations are required to be issued, unless a later date is specified in the regulations.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

GRAMM-LEACH-BLILEY ACT

* * * * * * *

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) * * *

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

TITLE V—PRIVACY

Subtitle A—Disclosure of Nonpublic Personal Information

* * * * * * *

SEC. 502A. SPECIAL RULES FOR HEALTH INFORMATION.

(a) RULES FOR DISCLOSURE.—

(1) GENERAL RULE REQUIRING AFFIRMATIVE CONSENT FOR DISCLOSURE.—

(A) IN GENERAL.—A financial institution may not disclose any individually identifiable health information pertaining to a consumer to an affiliate or a nonaffiliated third party unless the financial institution—

(i) has provided to the consumer a clear and conspicuous notice in writing, in electronic form, or in another form permitted by the regulations implementing this subtitle, of the categories of such information that may be disclosed and the categories of affiliates or nonaffiliated third parties to whom the financial institution discloses such information;

(ii) has clearly and conspicuously requested in writing, in electronic form, or in another form permitted by the regulations implementing this subtitle, that the consumer affirmatively consent to such disclosure; and

(iii) has obtained from the consumer such affirmative consent and such consent has not been withdrawn.

(B) WITHDRAWAL OF CONSENT.—A consumer may withdraw a consent to use or disclose individually identifiable health information at any time, except that any such withdrawal of consent is subject to the authorized uses made by the financial institution in reliance on the consent prior to its withdrawal.

(2) DISCLOSURE OF INFORMATION ABOUT PERSONAL SPENDING HABITS.—

(A) IN GENERAL.—If a financial institution provides a service to a consumer through which the consumer makes or receives payments or transfers by check, debit card, credit card, or other similar instrument, the financial institution may not disclose any information described in subparagraph (B) pertaining to the consumer to an affiliate or a nonaffiliated third party unless the financial institution has satisfied the requirements of clauses (i), (ii), and (iii) of paragraph (1)(A) with respect to the disclosure.

(B) INFORMATION DESCRIBED.—The information described in this paragraph is—

(i) an individualized list of a consumer's transactions or an individualized description of a consumer's interests, preferences, or other characteristics; or

(ii) any such list or description constructed in response to an inquiry about a specific, named individual;

if the list or description is derived from individually identifiable health information collected in the course of providing a service described in subparagraph (A) to the consumer.

(3) DISCLOSURE OF AGGREGATE LISTS.—A financial institution may not disclose any aggregate list of consumers containing or derived from individually identifiable health information to an affiliate or a nonaffiliated third party unless the financial institution has satisfied, for each consumer on the list, the requirements of clauses (i), (ii), and (iii) of paragraph (1)(A) with respect to the disclosure.

(4) DISCLOSURE OF COVERAGE DENIAL OR MEDICAL EXAMINATION TEST RESULTS.—A financial institution may not disclose to an affiliate or a nonaffiliated third party whether or not a consumer has been denied life or health insurance coverage, or any medical examination test results, unless the financial institution has satisfied the requirements of clauses (i), (ii), and (iii) of paragraph (1)(A) with respect to the disclosure.

(5) DISCLOSURE OF CONSENT INFORMATION.—A financial institution may not disclose to an affiliate or a nonaffiliated third party that a consumer has not provided consent under paragraph (1), (2), (3), or (4) unless the institution is authorized to disclose this information under another provision of this section.

(6) EXCEPTIONS TO DISCLOSURE LIMITATIONS.—This section shall not restrict a financial institution from disclosing individually identifiable health information, or any other information described in paragraph (2)(B), (3), or (4)—

(A) for a purpose described in paragraph (1), (2), (3), (5), (7), or (8) of section 502(e);

(B) for purposes of maintaining and operating consolidated customer call centers, or providing consolidated customer account statements or other related services to customers;

(C) to the institution's attorneys, accountants, and auditors, a State guaranty fund in connection with the resolution of an insolvent or impaired insurer, or an insurance

rate advisory organization in connection with the establishment of rates for particular lines of insurance;

(D) in connection with performing services for or functions solely on behalf of the financial institution with respect to the financial institution's own customers, including marketing of the financial institution's own products or services to the financial institution's customers; or

(E) for purposes of underwriting, premium rating, reinsurance, or replacement of a group health plan (as defined in section 733 of the Employee Retirement Income Security Act of 1974 (29 U.S.C. 1191b)) or workers' compensation policy.

(7) VOLUNTARY CONSENT.—A financial institution shall not condition provision of a financial product or service, or the terms of a financial product or service, on a consumer's affirmative consent to disclosure of individually identifiable health information to an affiliate or a nonaffiliated third party for a purpose other than a purpose necessary for provision of the financial product or service.

(8) LIMITS ON REDISCLOSURE AND REUSE OF INFORMATION.—

(A) IN GENERAL.—Except as provided in subparagraph (B), an affiliate or a nonaffiliated third party that receives individually identifiable health information from a financial institution under this section shall not disclose such information to any other person, unless such disclosure would be lawful if made directly to such other person by the financial institution.

(B) DISCLOSURE UNDER AN EXCEPTION.—Notwithstanding subparagraph (A), any person that receives individually identifiable health information from a financial institution in accordance with one of the exceptions in paragraph (6) may use or disclose such information only—

(i) as permitted under that exception; or

(ii) under another exception in such paragraph to carry out the purpose for which the information was disclosed by the financial institution.

(9) CONSTRUCTION.—Except as provided in paragraph (6)(A), this section applies in lieu of subsections (b), (c), and (e) of section 502 to a disclosure by a financial institution of individually identifiable health information.

(b) RULES FOR RECEIPT AND USE.—

(1) IN GENERAL.—In deciding whether, or on what terms, to offer, provide, or continue to provide a financial product or service, other than insurance, to a consumer, a financial institution shall not request to receive individually identifiable health information about the consumer from an affiliate or nonaffiliated third party, or use, evaluate, or otherwise consider any such information, unless the financial institution—

(A) has clearly and conspicuously requested in writing, in electronic form, or in another form permitted by the regulations implementing this subtitle, that the consumer affirmatively consent to such receipt and use; and

(B) has obtained from the consumer such affirmative consent and such consent has not been withdrawn.

(2) RESTRAINT ON INFORMATION REQUESTS.—In deciding whether, or on what terms, to offer, provide, or continue to provide a financial product or service, other than insurance, to a consumer, a financial institution shall not request the consent described in paragraph (1)(A) to receive individually identifiable health information available from an affiliate, unless the financial institution otherwise in the ordinary course of rendering the decision would, if that information were not available from an affiliate, request consent to receive the same or substantially similar information from a nonaffiliated third party.

(c) CONSUMER RIGHTS TO ACCESS AND CORRECT INFORMATION.—

(1) ACCESS.—

(A) IN GENERAL.—Upon the request of a consumer, a financial institution shall make available to the consumer individually identifiable health information about the consumer that is within the possession of the financial institution.

(B) EXCEPTIONS.—Notwithstanding subparagraph (A), a financial institution—

(i) shall not be required to disclose to a consumer any confidential commercial information, such as an algorithm used to derive credit scores or other risk scores or predictors;

(ii) shall not be required to create new records in order to comply with the consumer's request;

(iii) shall not be required to disclose to a consumer any information assembled by the financial institution, in a particular matter, as part of the financial institution's efforts to comply with laws preventing fraud, money laundering, or other unlawful conduct, or otherwise to identify or investigate such conduct;

(iv) shall not disclose any information required to be kept confidential by any other Federal law; and

(v) shall not be required to disclose information (as specified in regulations promulgated by the Federal agencies referred to in section 504(a) in consultation with the Department of Health and Human Services) if the disclosure would endanger the life or physical safety of any individual or if the information was obtained under a promise of confidentiality from someone other than a health care provider and the disclosure would be likely to reveal that source.

(C) ACCESS BY EXAMINED INDIVIDUAL TO RESULTS OF MEDICAL EXAMINATIONS.—

(i) IN GENERAL.—A financial institution shall take such actions as are necessary to ensure that, in any case in which—

(I) a medical examination of an individual is required for initial or continued enrollment under an insurance policy issued by the financial institution; and

(II) the medical examination is conducted by a person who is in the employ of the institution or

whose services are procured otherwise by the institution;

the individual (or the individual's legal guardian) is provided all medical information obtained from the examination at the same time that the information is made available to the financial institution and the individual is encouraged to make the information available to the individual's own physician.

(ii) PROVISION TO PHYSICIAN.—Upon the request of an individual (or a legal guardian) described in clause (i), the information required to be provided to the individual or guardian under such clause shall be provided to the individual's physician instead of, or in addition to, the individual or guardian.

(2) CORRECTION.—

(A) OPPORTUNITY TO DISPUTE.—A financial institution shall provide a consumer the opportunity to dispute the accuracy of any individually identifiable health information disclosed to the consumer pursuant to paragraph (1), and to present evidence thereon.

(B) AMENDMENT, CORRECTION, OR DELETION.—A financial institution—

(i) shall amend, correct, or delete material information identified by a consumer that is materially incomplete or inaccurate; or

(ii) shall notify the consumer of—

(I) its refusal to make such amendment, correction, deletion;

(II) the reasons for the refusal; and

(III) the identity of the person who created the information and shall refer the consumer to that person for purposes of amending or correcting the information or filing with it a concise statement of what the consumer believes to be the correct information.

(3) RULE OF CONSTRUCTION.—For purposes of this subsection, the term "consumer", when used with respect to a financial institution, means a customer of the institution, or a person who has applied for and been denied a financial product or service by the institution.

(4) COORDINATION AND CONSULTATION.—In prescribing regulations implementing this subsection, the Federal agencies specified in section 504(a) shall consult with one another to ensure that the regulations—

(A) impose consistent requirements on the financial institutions under their respective jurisdictions;

(B) take into account conditions under which financial institutions do business both in the United States and in other countries; and

(C) are consistent with the principle of technology neutrality.

(5) CHARGES FOR DISCLOSURES.—A financial institution may impose a reasonable, cost-based charge for making a disclosure under this subsection, which charge shall be disclosed to the consumer before making the disclosure.

(6) NOTICE OF RIGHTS TO ACCESS AND CORRECT.—The disclosures required by section 503 shall include a statement of the consumer's right to access and correct individually identifiable health information in accordance with this subsection.

(d) SPECIAL REQUIREMENTS TO PROTECT ESPECIALLY SENSITIVE HEALTH INFORMATION.—

(1) SEPARATE CONSENT.—In any case in which this section requires a person to obtain a consumer's affirmative consent to the receipt, use, or disclosure of individually identifiable health information, the person shall obtain a separate and specific consent with respect to any information pertaining to—

(A) mental health services requested or received by an individual;

(B) human immunodeficiency virus (commonly known as HIV), acquired immune deficiency syndrome, or any other sexually transmitted disease;

(C) genetic information;

(D) reproductive health services requested or received by an individual; or

(E) substance abuse treatment requested or received by an individual.

(2) NO EXCEPTION TO DISCLOSURE LIMITATIONS FOR MARKETING PURPOSES.—Notwithstanding subsection (a)(6)(D), a financial institution may not disclose individually identifiable health information, or any other information described in paragraph (2)(B), (3), or (4) of subsection (a), for purposes of marketing the financial institution's own products or services to the financial institution's customers, if the information pertains to a subject described in any of subparagraphs (A) through (E) of paragraph (1) of this subsection.

(e) RELATIONSHIP TO OTHER LAWS.—Nothing in this section shall be construed as—

(1) modifying, limiting, or superseding standards promulgated by the Secretary of Health and Human Services under—

(A) part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.); or

(B) section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191; 110 Stat. 2033);

(2) applying to an activity, to the extent that the activity is subject to regulation under any of the provisions of law referred to in subparagraph (A) or (B) of paragraph (1); or

(3) authorizing the use or disclosure of individually identifiable health information in a manner other than as permitted by other applicable law.

(f) CIVIL LIABILITY.—

(1) IN GENERAL.—Any financial institution which fails to comply with any provision of this section with respect to any disclosure or use of individually identifiable health information pertaining to any consumer shall be liable to the consumer in an amount equal to the sum of the amounts determined under each of the following subparagraphs:

(A) COMPENSATORY DAMAGES.—The greater of—

(i) the amount of any actual damage sustained by the consumer as a result of such failure; or

(ii) any amount paid by the consumer to the financial institution.

(B) GENERAL DAMAGES.—

(i) INDIVIDUAL ACTIONS.—In the case of any action by an individual, such additional amount as the court may allow.

(ii) CLASS ACTIONS.—In the case of a class action, the sum of—

(I) the aggregate of the amount which the court may allow for each named plaintiff; and

(II) the aggregate of the amount which the court may allow for each other class member, without regard to any minimum individual recovery.

(C) ATTORNEYS' FEES.—In the case of any successful action to enforce any liability under subparagraph (A) or (B), the costs of the action, together with reasonable attorneys' fees.

(2) FACTORS TO BE CONSIDERED IN AWARDING GENERAL DAMAGES.—In determining the amount of any liability of any person under paragraph (1)(B), the court shall consider, among other relevant factors—

(A) the frequency and persistence of noncompliance by such person;

(B) the nature of the noncompliance;

(C) the extent to which such noncompliance was intentional; and

(D) in the case of any class action, the number of consumers adversely affected.

* * * * * * *

SEC. 509. DEFINITIONS.

As used in this subtitle:

(1) * * *

* * * * * * *

(12) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.—The term "individually identifiable health information" means any information, including demographic information obtained from or about an individual, that is described in section 1171(6)(B) of the Social Security Act (42 U.S.C. 1320d(6)(B)).

(13) GENETIC INFORMATION.—The term "genetic information" means individually identifiable health information about genes, gene products, or inherited characteristics that may derive from an individual or a family member of an individual (including information about a request for or receipt of genetic services by an individual or a family member of an individual).

* * * * * * *

DISSENTING VIEWS

These views dissent from the Banking Committee Report on the Medical Financial Privacy Protection Act, H.R. 4585.

H.R. 4585 is intended to strengthen consumers' control over the use and disclosure of their health information by financial institutions. Although this is an admirable goal, this legislation is, at best premature. Further, during the markup of this bill, several unnecessary amendments were added to this bill which simply added to the overbearing nature of the regulations the legislation seeks to impose.

In the Fall of 1999, the House of Representatives passed the Financial Services Modernization Act of 1999, (P.L. 106–102). This bill included the first adoption of far-reaching privacy protections for financial information ever passed by Congress. The Financial Services Modernization Act included several privacy provisions, such as a requirement that all financial institutions have an obligation to respect the privacy of customers and protect the security and confidentiality of customer financial records; and a prohibition on the disclosure of credit card, savings and transaction account numbers or other forms of account access information to a third party for use in marketing.

During the markup of H.R. 4585, I cautioned the Committee on Banking and Financial Services not move too quickly to pass new regulations on the financial services industry so soon after such a sweeping overhaul of current regulations. Rather, we should wait to see the results of our most recent efforts before embarking on new reforms. Such action is premature considering federal regulators have not yet decided how they will interpret the provisions included in the Financial Services Modernization Act.

The Department of Health and Human Services is also currently finalizing regulations that relate to the privacy of health information, which incidentally, they have been working on for over two years. In addition, industry leaders have made it very clear to me, they have no intention of using their customers' personal health information in providing financial services. In fact, the nation's major insurance trade groups and banking trade associations have both adopted voluntary guidelines with regard to this matter. These self-imposed rules call for banking and insurance organizations to obtain the affirmative consent of a customer before sharing health information.

Further, H.R. 4585 included several "opt-in" requirements which require banks to obtain specific consent from customers if they wish to share specific types of health information. Originally, the bill included requirements for mental illness and sexually transmitted diseases. However, during the course of debate, this bill became a christmas tree of sorts for a number of marginal liberal interests. It now includes language mandating banks receive special

permission before sharing information about abortions or drug abuse by their customers. These overly-specific mandates simply create more excessive regulation for the financial services industry, and they are not at all needed to ensure the privacy of bank customers in light of the regulations passed as part of the Financial Services Modernization Act.

For these reasons, I respectfully, dissent from the report on H.R. 4585.

BOB BARR.

○