Montgomery County Council Public Hearing
Expedited Bill 5-23, Personnel and Human Resources –
Prospective Employees – Health Care Privacy
February 14, 2023
Testimony of Melissa McKenna

Good afternoon. My name is Melissa McKenna.

Thank you Councilmember Luedtke for calling attention to this arcane county practice and introducing this expedited legislation, to take effect immediately upon passage. And thank you all for supporting Bill 5-23 ending the County's collection of protected health information.

That the Montgomery County Government Medical History Review Form was updated less than a year ago and is still being required for employment is beyond words. Frankly, I'm shocked it hasn't been legally challenged by now. The potential for bias against hiring based on the answers to these questions is vast.

Make no mistake about it, protected health information **IS** being collected. The County government is **NOT** a health care provider and has no business asking for this information. I wholly agree that prospective employees only have to answer "business-related" questions as to whether they are able to meet published minimum job qualifications.

Judging anyone's fitness for a job should be made by an outside entity and only the results, meaning yes or no that the person can perform the job, be reported to the County Office of Human Resources. It is vital that protected health information be shared only with a health care entity that has the correct and necessary HIPAA policies and protections in place.

It's not just a matter of reproductive health information, this is a matter of disability rights. The disclosure of any disability is voluntary! People with disabilities, especially those with invisible disabilities, by their answers, are forced to disclose their condition.

The potential for misuse/abuse or bias of the provided information ‘to evaluate an individual’s future eligibility for disability or disability retirement benefits’ is enormous and the determination should be made by a third party.

In addition to this legislation, please change county practices to outsource determinations regarding physical fitness to meet essential job requirements and short- and long-term disability.

If health information is used with any of 18 identifiers (listed in my written testimony), it is considered identifiable and therefore protected health information. The County Medical History Form requests/contains 6 of the 18 identifiers. As part of a personnel file, protected health information becomes ‘individually identifiable health information’ that is accessible by many others and is absolutely subject to HIPAA privacy protections.

I would go a step further and request that this bill also mandate the purging of this information of current and past employees from all personnel files and County electronic records immediately upon passage.

Finally, the bill should specifically include the Health Insurance Portability and Accountability Act of 1996, PUBLIC LAW 104–191—AUG. 21, 1996 and that terms such as ‘protected health information,’ ‘individually identifiable health information,’ and ‘health information’ conform to those in HIPAA, 42 USC 1320d (pages 87-89).

I hope you include the following friendly amendments to Bill 5-23:

1. Immediately destroy all physical files and purge electronic files of the medical history form for all current and past employees.
2. Amend the definitions and language throughout to conform to the definitions in HIPAA.

Thank you.
Melissa McKenna

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

Public Law 104–191
104th Congress

An Act

To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Aug. 21, 1996
[H.R. 3103]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Health Insurance Portability and Accountability Act of 1996.
42 USC 201 note.

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Health Insurance Portability and Accountability Act of 1996".

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

the validity of any such lien or mortgage and the amount of payment to be made, and the employment of attorneys and other personnel skilled in State real estate law as necessary;

(D) payment authorized in connection with remission or mitigation procedures relating to property forfeited; and

(E) the payment of State and local property taxes on forfeited real property that accrued between the date of the violation giving rise to the forfeiture and the date of the forfeiture order.

(3) RESTORATION PAYMENT.—Notwithstanding any other provision of law, if the Federal health care offense referred to in paragraph (1) resulted in a loss to an employee welfare benefit plan within the meaning of section 3(1) of the Employee Retirement Income Security Act of 1974, the Secretary of the Treasury shall transfer to such employee welfare benefit plan, from the amount realized from the forfeiture of property referred to in paragraph (1), an amount equal to such loss. For purposes of paragraph (1), the term "restoration payment" means the amount transferred to an employee welfare benefit plan pursuant to this paragraph.

SEC. 250. RELATION TO ERISA AUTHORITY.

29 USC 1136 note.

Nothing in this subtitle shall be construed as affecting the authority of the Secretary of Labor under section 506(b) of the Employee Retirement Income Security Act of 1974, including the Secretary's authority with respect to violations of title 18, United States Code (as amended by this subtitle).

Subtitle F—Administrative Simplification

SEC. 261. PURPOSE.

42 USC 1320d note.

It is the purpose of this subtitle to improve the Medicare program under title XVIII of the Social Security Act, the medicaid program under title XIX of such Act, and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information.

SEC. 262. ADMINISTRATIVE SIMPLIFICATION.

(a) IN GENERAL.—Title XI (42 U.S.C. 1301 et seq.) is amended by adding at the end the following:

"PART C—ADMINISTRATIVE SIMPLIFICATION

"DEFINITIONS

"SEC. 1171. For purposes of this part:

42 USC 1320d.

"(1) CODE SET.—The term 'code set' means any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.

"(2) HEALTH CARE CLEARINGHOUSE.—The term 'health care clearinghouse' means a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements.

"(3) HEALTH CARE PROVIDER.—The term 'health care provider' includes a provider of services (as defined in section 1861(u)), a provider of medical or other health services (as defined in section 1861(s)), and any other person furnishing health care services or supplies.

"(4) HEALTH INFORMATION.—The term 'health information' means any information, whether oral or recorded in any form or medium, that—

"(A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

"(B) 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.

"(5) HEALTH PLAN.—The term 'health plan' means an individual or group plan that provides, or pays the cost of, medical care (as such term is defined in section 2791 of the Public Health Service Act). Such term includes the following, and any combination thereof:

"(A) A group health plan (as defined in section 2791(a) of the Public Health Service Act), but only if the plan—

"(i) has 50 or more participants (as defined in section 3(7) of the Employee Retirement Income Security Act of 1974); or

"(ii) is administered by an entity other than the employer who established and maintains the plan.

"(B) A health insurance issuer (as defined in section 2791(b) of the Public Health Service Act).

"(C) A health maintenance organization (as defined in section 2791(b) of the Public Health Service Act).

"(D) Part A or part B of the Medicare program under title XVIII.

"(E) The medicaid program under title XIX.

"(F) A Medicare supplemental policy (as defined in section 1882(g)(1)).

"(G) A long-term care policy, including a nursing home fixed indemnity policy (unless the Secretary determines that such a policy does not provide sufficiently comprehensive coverage of a benefit so that the policy should be treated as a health plan).

"(H) An employee welfare benefit plan or any other arrangement which is established or maintained for the purpose of offering or providing health benefits to the employees of 2 or more employers.

"(I) The health care program for active military personnel under title 10, United States Code.

"(J) The veterans health care program under chapter 17 of title 38, United States Code.

"(K) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), as defined in section 1072(4) of title 10, United States Code.

"(L) The Indian health service program under the Indian Health Care Improvement Act (25 U.S.C. 1601 et seq.).

"(M) The Federal Employees Health Benefit Plan under chapter 89 of title 5, United States Code.

"(6) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.—The term 'individually identifiable health information' means any information, including demographic information collected from an individual, that—

"(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

"(B) 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—

"(i) identifies the individual; or

"(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

"(7) STANDARD.—The term 'standard', when used with reference to a data element of health information or a transaction referred to in section 1173(a)(1), means any such data element or transaction that meets each of the standards and implementation specifications adopted or established by the Secretary with respect to the data element or transaction under sections 1172 through 1174.

"(8) STANDARD SETTING ORGANIZATION.—The term 'standard setting organization' means a standard setting organization accredited by the American National Standards Institute, including the National Council for Prescription Drug Programs, that develops standards for information transactions, data elements, or any other standard that is necessary to, or will facilitate, the implementation of this part.

"GENERAL REQUIREMENTS FOR ADOPTION OF STANDARDS

"SEC. 1172. (a) APPLICABILITY.—Any standard adopted under this part shall apply, in whole or in part, to the following persons: 42 USC 1320d–1.

"(1) A health plan.

"(2) A health care clearinghouse.

"(3) A health care provider who transmits any health information in electronic form in connection with a transaction referred to in section 1173(a)(1).

"(b) REDUCTION OF COSTS.—Any standard adopted under this part shall be consistent with the objective of reducing the administrative costs of providing and paying for health care.

"(c) ROLE OF STANDARD SETTING ORGANIZATIONS.—

"(1) IN GENERAL.—Except as provided in paragraph (2), any standard adopted under this part shall be a standard that has been developed, adopted, or modified by a standard setting organization.

"(2) SPECIAL RULES.—

"(A) DIFFERENT STANDARDS.—The Secretary may adopt a standard that is different from any standard developed, adopted, or modified by a standard setting organization, if—

"(i) the different standard will substantially reduce administrative costs to health care providers and health plans compared to the alternatives; and

What is Protected Health Information?

Posted By HIPAA Journal on Jan 1, 2023

The latest article in our HIPAA basics series answers the question what is protected health information?

The Health Insurance Portability and Accountability Act (HIPAA) requires covered entities to implement safeguards to ensure the confidentiality, integrity, and availability of protected health information, but what is protected health information?

First, it is worthwhile explaining two other important terms detailed in HIPAA compliance regulations: A covered entity and a business associate. A covered entity is a healthcare provider, health plan, or healthcare clearinghouse which transmits health data electronically for transactions that the U.S. Department of Health and Human Services has adopted standards. A business associate is an organization or individual who performs services on behalf of a HIPAA-covered entity that requires access to, or the use of, protected health information.

What is Protected Health Information?

Protected health information is the term given to health data created, received, stored, or transmitted by HIPAA-covered entities and their business associates in relation to the provision of healthcare, healthcare operations and payment for healthcare services. Protected health information is often shortened to PHI, or in the case of electronic health information, ePHI.

Get The HIPAA Compliance Checklist

Free and Immediate Download

Work Email *

First Nam Last Nam

Work Number *

Company *

Download Checklist

Delivered via email so please ensure you enter your email address correctly.

Your Privacy Respected
HIPAA Journal Privacy Policy

County Council Public Hearing Bill 5-23 testimony of Melissa McKenna. attachment page 6 of 10

HIPAA Protected Health Information Definition

Protected health information "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" that is:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

Protected Health Information Includes…

Protected health information includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or healthcare coverage. 'Protected' means the information is protected under the HIPAA Privacy Rule.

Protected health information is defined in the Code of Federal Regulations and applies to health records, but not education records which are covered by other federal regulations, and neither records held by a HIPAA-covered entity related to its role as an employer. In the case of an employee-patient, protected health information does not include information held on the employee by a covered entity in its role as an employer, only in its role as a healthcare provider.

PHI does not include individually identifiable health information of persons who have been deceased for more than 50 years.

What is Individually Identifiable Health Information?

When individually identifiable information is used by a HIPAA covered entity or business associate in relation to healthcare services or payment it is classed as protected health information.

There are 18 identifiers that can be used to identify, contact, or locate a person. If health information is used with any of these identifiers it is considered identifiable. If PHI has all of these identifiers removed, it is no longer considered to be protected health information. (see de-identification of protected health information)

1. Names (Full or last name and initial)
2. All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the U.S. Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. Dates (other than year) directly related to an individual
4. Phone Numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers (including serial numbers and license plate numbers)
13. Device identifiers and serial numbers;
14. Web Uniform Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal and voice prints

17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

PHI Health Apps

There is some confusion around PHI and health apps as they often collect information that is classed as PHI when it is recorded or used by a healthcare provider. Health apps record information such as heart rate data and the data include personal identifiers. However, the data collected by these apps and trackers is not always covered by HIPAA Rules. App developers can be business associates, but in the most part they are not.

If a HIPAA covered entity develops a health app for use by patients or plan members and it collects, uses, stores, or transmits protected health information, the information must be protected in line with HIPAA Rules.

If a physician recommends a PHI health app be used by a patient, such as for tracking BMI or heart rate data, the information is not subject to HIPAA Rules as the app was not created for the physician.

A third-party health app developer would be classed as a business associate, and required to comply with HIPAA, if the app has been created for a HIPAA-covered entity and it collects, uses, stores, or transmits identifiable health information or if the developer is contracted with a HIPAA-covered entity to provide health monitoring services via the app.

PHI health app guidance was issued by OCR in 2016 and can be viewed on this link (PDF).

PHI Information Technology

The HIPAA Security Rule requires safeguards to be implemented by HIPAA-covered entities and their business associates to protect PHI that is created, used, received, stored, or transmitted in electronic format. Administrative, physical, and technical controls must be implemented to ensure the confidentiality, integrity, and availability of ePHI.

Failures to protect ePHI and subsequent privacy violations can result in significant fines, although since there is no private cause of action in HIPAA, patients affected by data breaches cannot sue HIPAA covered entities for the exposure, theft, or impermissible disclosure of their PHI.

The HIPAA Privacy Rules stipulates allowable uses and disclosures of PHI and gives patients the right to obtain a copy of the PHI that is held by their healthcare providers. HealthIT can be used to help patients access their PHI. Many healthcare providers now allow patients to access some or all of their health information via patient portals. If only partial information is available through a patient portal, patients can still exercise their right to obtain all PHI in a designated record set held by their healthcare providers by submitting a request in writing.

FAQs

Would patient information such as “Mrs. Green from Miami” be considered PHI?

Although there could be thousands of Mrs. Greens in Miami, there is likely to be fewer Mrs. Kawtowskis in Maryland. As it would be impractical for HIPAA to stipulate there has to be fewer than so many “Mrs. As” in a population of “B” before the two identifiers combined are considered to be PHI, all combinations of identifiers are consider PHI under HIPAA – even “Mrs. Green from Miami”.

What are allowable uses and disclosures of PHI?

Without an authorization from the patient, a covered entity is only allowed to use and disclose a patient´s PHI for its own treatment, payment, and health care operations. A covered entity can also disclose the patient´s PHI to a business associate provided both the covered entity and the business associated have signed a HIPAA-compliant business associate agreement.

What are incidental uses and disclosures of PHI?

Incidental uses and disclosures of PHI are those that occur accidentally as a by-product of another allowable use or disclosure. Provided the covered entity or business associate has applied reasonable safeguards and implemented the minimum necessary standard with respect to the primary use or disclosure, there is no violation of HIPAA.

Can you provide an example of an incidental disclosure?

An example of an incidental disclosure is when an employee of a business associate walks into a covered entity's facility and recognizes a patient in the waiting room. Although the business associate does not need to know the identity of any patients at the covered entity's facility, the business associate has a compliant business associate agreement in place and is visiting the facility to carry out work described in the agreement. Therefore the disclosure of PHI is incidental to the compliant work being done.

Would a personal wearable device such as a step counter be considered a PHI health app?

Unless the personal wearable device collects, uses, and/or stores data, and that data is transmitted to – or downloaded at – a physician's office or healthcare facility, the device is not a PHI health app. So, in most cases, a wearable step counter would not be considered a PHI health app provided it is used for personal use only.

County Council Public Hearing Bill 5-23 testimony of Melissa McKenna. attachment page 9 of 10

Author: Steve Alder is the editor-in-chief of HIPAA Journal. Steve is responsible for editorial policy regarding the topics covered on HIPAA Journal. He is a specialist on healthcare industry legal and regulatory affairs, and has several years of experience writing about HIPAA and other related legal topics. Steve has developed a deep understanding of regulatory issues surrounding the use of information technology in the healthcare industry and has written hundreds of articles on HIPAA-related topics.

County Council Public Hearing Bill 5-23 testimony of Melissa McKenna. attachment page 10 of 10

Melissa Mdenna
8.15-23

HIPAA Protected Health Information Definition

Protected health information "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" that is:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

Protected Health Information Includes...

Protected health information includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or healthcare coverage. 'Protected' means the information is protected under the HIPAA Privacy Rule.

Protected health information is defined in the Code of Federal Regulations and applies to health records, but not education records which are covered by other federal regulations, and neither records held by a HIPAA-covered entity related to its role as an employer. In the case of an employee-patient, protected health information does not include information held on the employee by a covered entity in its role as an employer, only in its role as a healthcare provider.

PHI does not include individually identifiable health information of persons who have been deceased for more than 50 years.

What is Individually Identifiable Health Information?

When individually identifiable information is used by a HIPAA covered entity or business associate in relation to healthcare services or payment it is classed as protected health information.

There are 18 identifiers that can be used to identify, contact, or locate a person. If health information is used with any of these identifiers it is considered identifiable. If PHI has all of these identifiers removed, it is no longer considered to be protected health information. (see de-identification of protected health information)

1. Names (Full or last name and initial)
2. All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the U.S. Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. Dates (other than year) directly related to an individual
4. Phone Numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers (including serial numbers and license plate numbers)
13. Device identifiers and serial numbers;
14. Web Uniform Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal and voice prints