Media coverage

August 2018

1. INTRODUCTION

HIPAA, short for the Health Insurance Portability and Accountability Act of 1996, is a familiar term to most people, but when and how it applies often confounds healthcare professionals, business executives and attorneys alike, let alone the general public. Over the course of the more than 20 years of HIPAA's existence, this confusion persists and has even intensified in an age in which there is instantaneous and continuous global reporting of the struggle of large retail companies, sophisticated financial institutions, healthcare providers large and small and government agencies to deal with data security breaches. Recent news stories about unexpected data mining practices and the proliferation of multiple laws governing data collection, use, and disclosure raise questions as to when and whether HIPAA protects health information.

A HIPAA misstep can have serious legal, financial and reputational consequences, so understanding what HIPAA protects and requires is critical for any person or business that touches health information. This article is not intended to detail each and every HIPAA requirement and nuance, but rather to list a sequence of basic questions whose answers can be used as fundamental building blocks for HIPAA compliance[1].

2. DOES HIPAA APPLY?

HIPAA does not protect all information[2]. HIPAA does not even protect all health information. To be HIPAA-protected, the information must fit within very specific definitions set forth under §160.103 of the HIPAA Privacy and Security Rules, Part 160 and 164 of Title 45 of the Code of Federal Regulations ('CFR') ('the HIPAA Privacy and Security Rules') before it qualifies for HIPAA protection and subjects those that use or disclose it to HIPAA's requirements. Only protected health information qualifies for HIPAA protection, so understanding the components of this definition is critical to understanding whether HIPAA applies in the first place. Notably, HIPAA only applies to health information that is individually identifiable and that is created, received, maintained, or transmitted by covered entities or business associates, and their subcontractors (as such terms are defined under HIPAA).

2.1. Key definitions

Protected health information ('PHI'): is defined as 'individually identifiable health information' (defined below) that is transmitted or maintained in electronic media or in any other form or medium, but does not include information:

1. in education records covered by the federal Family Educational Rights and Privacy Act of 1974 ('FERPA');
2. in certain secondary school records held by health care providers[3];
3. in employment records held by a 'covered entity' (defined below) in its role as employer; and
4. regarding a person who has been deceased for more than 50 years.

Individually identifiable health information ('IIHI'): is information that is a subset of 'health information' (defined below), including demographic information such as an address, Social Security Number and birth date, collected from an individual, that:

1. is created or received by a 'health care provider,' 'health plan,' 'employer,' or 'health care clearinghouse' (as each of these terms is defined in §160.103 of the HIPAA Privacy and Security Rules); and
2. 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
3. that identifies the individual; or
4. with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Health information: is any information, including 'genetic information' (a term also specifically defined at §160.103 of the HIPAA Privacy and Security Rules), whether oral or recorded in any form or medium, that:

1. 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
2. relates to the past, present, or future physical or mental health 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.

Covered entity: is a 'health plan,' a 'health care clearinghouse,' and/or a 'health care provider' who transmits any 'health information' in electronic form in connection with a 'transaction.' A transaction is the transmission of information between two parties to carry out financial or administrative activities related to health care, and specifically includes transmissions involving eligibility for a health plan and health plan premium payments, in addition to transmissions involving health care claims, coordination of benefits, referrals and authorisations for health care, and other types of transmissions associated with health care provider activities. The definition of 'health plan' excludes, among other things, plans that provide coverage for accident or disability income; coverage issued as a supplement to liability insurance; liability insurance, including general liability insurance and automobile liability insurance; workers' compensation insurance; automobile medical payment insurance; and other insurance coverage specified in the HIPAA Privacy and Security Rules under which benefits for medical care are secondary or incidental to other insurance benefits.

Business associate: the HIPAA Privacy and Security Rules make it clear that a 'business associate' is subject to many of the same HIPAA responsibilities as a 'covered entity.' A business associate is a person who, on behalf of a covered entity, but other than in the capacity of a member of the workforce of such covered entity, creates, receives, maintains or transmits PHI for a function or activity regulated by HIPAA. A business associate that subcontracts with another person to provide services to the business associate that require the creation, receipt, maintenance or transmission of PHI ('a subcontractor') is subject to the same HIPAA responsibilities as the business associate. Accordingly, covered entities, business associates and subcontractors are each individually responsible for HIPAA compliance and risk both contract and federal government sanctions for failures to adequately protect the privacy and security of PHI as required by HIPAA.

2.2. Non-HIPAA data

When the definitions set forth above are put together, it becomes clear that certain information that is 'health information,' even when it is IIHI, is not protected by HIPAA ('non-HIPAA data'). Similarly, those using and disclosing this non-HIPAA data are not subject to HIPAA's requirements with respect to such non-PHI.

Examples of non-PHI include:

> IIHI disclosed by individuals about themselves on websites and health apps (other than those developed and/or used by a covered entity, business associate, or subcontractor[4] on behalf of a covered entity or business associate), to friends or family, or to anyone *other than* a health care provider, health plan, employer, or health care clearinghouse. Such IIHI can be redisclosed by the recipient without violating HIPAA.
> information that would be IIHI, but does not fall within the definition of 'health information' because it is not created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse.

Examples of information that is technically PHI, but which may be mistaken as non-HIPAA data, include:

> IIHI held in employment records by an employer that is not a covered entity (i.e. a health care provider, health plan, or health care clearinghouse).
> health information that does not include a patient's name or other identifiers, but that can be combined with other information to identify the individual, such as 'redacted' medical records that include a date of service, or de-identified health information that can be re-identified when combined with aggregated data from another source.

2.3. When does HIPAA apply?

However, for HIPAA to apply and actually 'protect' the PHI under HIPAA's privacy and security requirements, it must be created, received, maintained or transmitted by a covered entity, business associate, or subcontractor. In this sense, the term 'protected health information' is, itself, misleading, since an employer can create PHI, but that PHI will not be subject to HIPAA protections unless a covered entity, business associate, or subcontractor is involved.

Examples of IIHI generally subject to HIPAA protection:

IIHI that has been:

1. created, received, maintained or transmitted by a hospital, physician, nurse, technician or other health care provider that is treating a patient;
2. created, received, maintained or transmitted by a health app or medical device worn by an individual to a health care provider or treating facility[5];
3. created, received, maintained or transmitted by a health app to a health plan by a health plan member;

4. created, received, maintained or transmitted by a quality management company in connection with analysis of health outcomes for a health care provider or health plan;
5. obtained from patient records by a 'snooping' employee in the workforce of a treating health care facility;
6. created, received, or maintained by an electronic health records company and sold to a data aggregator;
7. collected from an employee wellness programme about an employee and maintained by the employer (unless the employer is a covered entity and maintains the information in employment records held in its role as an employer); and
8. maintained by a cloud service provider, even if the IIHI has been encrypted and the cloud service provider has no access to the decryption key[6].

Examples of IIHI that are not generally subject to HIPAA protection:

1. information disclosed by an individual about his or her own identity, address, diagnosis, health condition or prognosis by way of a health app or wearable device not made available to the individual or recommended by the individual's health care provider or health plan;
2. information disclosed by an individual on social media about his or her health status or condition;
3. information disclosed by a health care provider to family members, friends or neighbours of a patient about the patient's identity, address, diagnosis, or health conditions[7];
4. publication by a newspaper, television news program or other internet or media outlet about the identity, address, diagnosis, health condition or prognosis of an individual being treated for a health condition;
5. confirmation by family members, friends or neighbours of a patient about such patient's identity, address, diagnosis, health condition or prognosis; and
6. discussion by a healthcare professional, who has not treated or consulted with a patient, on television or through other media about the identity, location, diagnosis, health condition or prognosis of such patient.

3. WHAT ARE THE PERMITTED USES AND DISCLOSURES OF PHI?

Covered entities, business associates and subcontractors may only use or disclose PHI as permitted under §164.502 of the HIPAA Privacy and Security Rules.

There are differences between the PHI uses and disclosures permitted for covered entities, on one hand, and business associates and subcontractors, on the other. Whereas a covered entity may use or disclose PHI to the individual for 'treatment,' 'payment,' or 'health care operations' (as these terms are defined at §164.501 of the HIPAA Privacy and Security Rules); pursuant to a valid authorisation; and for specified other purposes[8] a business associate and/or subcontractor may only use or disclose PHI as permitted or required under its business associate agreement or subcontractor agreement, as required by law, and (but only if expressly permitted under its business associate agreement or subcontractor agreement) for its own management and administration or to provide data aggregation services relating to the health care operations of the covered entity (§164.502(a)(3) and (a)(4) of the HIPAA Privacy and Security Rules). In other words, a business associate or subcontractor's rights to use and

disclose PHI are generated by and limited to the rights set forth in the contract that gives it access to the PHI in the first place (though the business associate's and subcontractor's obligations to meet applicable HIPAA privacy and security obligations is independent of and may exceed express contractual obligations). In addition, a covered entity that is required under the HIPAA Privacy and Security Rules to have a notice of privacy practices ('NPP') may only use or disclose PHI as described in its NPP.

Detailing each and every permitted use or disclosure of PHI is beyond the scope of this article, but certain uses and disclosures are more likely than others to trip up covered entities, business associates and subcontractors, either because the use or disclosure seems as though it should be permitted under HIPAA (but is not, or is only permitted under limited and specific circumstances), or because the parties using or disclosing the PHI misunderstand their HIPAA-defined roles. In some cases, a party who is acting as a business associate under HIPAA refuses to sign a business associate agreement under the mistaken belief that its services do not involve creation, receipt, maintenance or transmission of PHI. In other cases, a covered entity may require every third party with which it contracts and that receives or accesses (or might receive or access) PHI to sign a business associate agreement, regardless of whether the third party is providing or is likely to provide a service on behalf of the covered entity. In some of these instances (where, for example, a hospital system seeks a business associate agreement from a physician group that will be accessing its electronic health records in connection with the treatment of mutual patients), a data use agreement would be the appropriate contract.

3.1. Examples of impermissible use or disclosure of PHI

1. Covered entity, business associate or subcontractor contracts with a software vendor that refuses to sign a business associate or subcontractor agreement, despite the fact the software vendor may access PHI when performing software updates or remediation of computer glitches.
2. More PHI than that which is minimally necessary to accomplish the intended purpose of the use or disclosure is used or disclosed.
3. PHI is used or disclosed in a manner not consistent with and described in the covered entity's NPP.
4. A business associate de-identifies PHI, not on behalf of the covered entity or for its own management and administration, but in order to sell it to a data aggregator.
5. PHI is disclosed pursuant to a subpoena, discovery request, or other 'lawful process', but the individual whose PHI is disclosed has not authorised the disclosure and no reasonable efforts (as described in §164.512(e) of the HIPAA Privacy and Security Rules) have been made to ensure the individual has been given notice of the request and/or to secure a qualified protective order.

3.2. Examples of permissible use or disclosure of PHI

1. Provision of PHI by a hospital to a health care provider involved in treatment of the patient even though such health care provider has not signed a business associate agreement with the hospital.
2. Release of PHI to a law enforcement official by a covered entity without the individual's consent where the individual is or is suspected to be a victim of a crime, under specified circumstances (§164.512(f)(3) of the HIPAA Privacy and Security Rules).

3. Release of PHI by a physician to avert a serious threat to health or safety when the use or disclosure is consistent with applicable law and standards of ethical conduct, and the physician, in good faith, believes the use or disclosure is necessary to prevent or lessen an imminent threat to the health or safety of a person or the public and is made to a person reasonably able to prevent or lessen the threat (§164.512(j) of the HIPAA Privacy and Security Rules).

4. WHAT ARE THE CONSEQUENCES OF NON-COMPLIANCE?

An acquisition, access, use or disclosure of PHI in a manner not permitted under §164.500 et seq of the HIPAA Privacy and Security Rules protecting the privacy of the PHI is generally deemed to be a breach, triggering various notification and reporting requirements[9] and potentially leading to federal and/or state government enforcement actions and civil monetary or criminal penalties. The covered entity, business associate or subcontractor, as applicable, may determine that an impermissible disclosure of PHI is not a breach if it demonstrates there is a low probability the PHI was compromised, based on a risk assessment of at least the following four factors:

1. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. the unauthorised person who used the PHI or to whom the disclosure was made;
3. whether the PHI was actually acquired or viewed; and
4. the extent to which the risk to the PHI has been mitigated (§164.402 of the HIPAA Privacy and Security Rules).

As discussed above, a business associate or subcontractor is only permitted to use or disclose PHI as set forth in its business associate or subcontractor agreement (or as is required by law), so a use or disclosure that might be permitted by a covered entity, but that is not expressly granted in the business associate or subcontractor agreement would likely constitute a breach. By way of example, imagine a business associate that provides data analysis for a covered entity health care provider or health plan and is prohibited under its business associate agreement from using or disclosing the covered entity's PHI outside the US. The business associate hires a subcontractor to analyse a subset of the data, but fails to include a contractual provision prohibiting the subcontractor from using or disclosing the data outside the US. The subcontractor has an office in Dubai, and individuals working in that office access the data for purposes of performing the necessary data analysis. The business associate would be directly liable for a HIPAA breach (and potentially subject to government action and contractual damages), even if there was no access to the PHI by third parties as a result of the work performed by the Dubai office.

The trend toward criminal prosecution of covered entities for HIPAA violations[10] and multi-million dollar civil monetary penalty awards[11] should trigger renewed focus on HIPAA compliance by a wide array of businesses in the coming years.

5. CONCLUSION

Of necessity, this article can only graze the surface of even the relatively limited scope of the three questions regarding HIPAA that have been addressed. It can serve to give an introduction to the terminology and structure of HIPAA and its regulatory scheme. However, the challenges and deepening complexity of issues confronting businesses affected by HIPAA as it approaches its 22nd birthday and the broader global data privacy and security universe suggests that assistance of competent professionals should be sought, even for matters that may at first blush appear to be relatively simple or routine.

---

1. This Guidance Note addresses the requirements of HIPAA, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 ('HITECH'), and the HIPAA Privacy and Security Rules, Part 160 and 164 of Title 45 of the Code of Federal Regulations ('CFR') as amended by the 'Omnibus Rule' (Subparts A, B, C and D of Part 160 of Title 45 of the CFR and Subparts A and C of Part 164 of the CFR).

2. Note that HIPAA standards, requirements or implementation specifications that are 'contrary to' state law generally preempt state law (§160.203 of Title 45 of the CFR), but state laws that relate to the privacy of individually identifiable health information and are determined by the Secretary of the U.S. Department of Health & Human Services ('HHS') to be 'more stringent' (as described at §160.202 of Title 45 of the CFR) than HIPAA are among those not preempted by HIPAA. This Guidance Note does not address specific state laws that are not preempted by HIPAA, and a separate review of state laws pertaining to privacy and security of individually identifiable health information is necessary to ensure compliance with applicable state laws.

3. See §1232g(a)(4)(B)(iv) of Title 20 of the United States Code for a complete description.

4. HHS' Office for Civil Rights, Health App Use Scenarios & HIPAA (2016).

5. Ibid.

6. HHS' Office for Civil Rights, Guidance on HIPAA & Cloud Computing (2016).

7. HHS' Office for Civil Rights, How HIPAA Allows Doctors to Respond to the Opioid Crisis (2017).

8. §164.502(a)(1) of the HIPAA Privacy and Security Rules.

9. §164.404, 164.406, 164.408, 164.410 of the HIPAA Privacy and Security Rules.

10. See, e.g., U.S. Attorney's Office District of Massachusetts, Springfield Doctor Convicted by Jury of Illegally Sharing Patient Medical Files (2018).

11. See, e.g., *Director of the Office for Civil Rights v. The University of Texas MD Anderson Cancer Center* (2018).