TABLE OF CONTENTS

August 2021

1. INTRODUCTION

The primary federal statute in the US regulating the privacy and security of health information is the Health Insurance Portability and Accountability Act of 1996 ('HIPAA'). HIPAA, as amended in 2009 by the Health Information Technology for Economic and Clinical Health Act of 2009 ('HITECH Act'), and their implementing regulations, govern 'covered entities' and 'business associates.' The law governing business associates can be confusing: they are entities covered by HIPAA but they are not HIPAA Covered Entities, they have multiple and overlapping reporting requirements to covered entities in the event of a privacy or security incident, and they have a multitude of privacy and security obligations - some only contractual and some regulatory. To understand why this is the case, a little history is helpful.

As its full name suggests, HIPAA was focused on issues such as the portability of health insurance from one job to another, rather than privacy or security of health information. The statute included an 'Administrative Simplification' subtitle which focused on the lack of standards for electronic ad-

ministrative transactions between health care providers and health plans.

Back in 1996, a US healthcare provider who sought to electronically bill Medicare, a state Medicaid programme, and private payers may have had to use different formats for each claim. The healthcare provider and health plan may have been assisted by a 'healthcare clearinghouse' to help facilitate electronic claims, converting healthcare claims from one format to another. This lack of standardisation resulted in significant costs to the healthcare industry, so the U.S. Congress included the Administrative Simplification subtitle in HIPAA, requiring the development of standard formats for a number of electronic administrative transactions. The statute only governed the following three types of entities involved in such electronic transactions:

- healthcare providers (but only if they electronically conducted one or more of the covered transactions);
- healthcare clearinghouses (who would convert transactions into and out of the standard formats); and
- health plans.

The issue of privacy was a last minute addition to the legislation, with Congress authorising the U.S. Department of Health & Human Services ('HHS') to promulgate privacy and security standards governing health information.[1] The HHS recognised a significant gap in the statute, namely that healthcare providers and health plans relied heavily on a variety of service providers, yet the statute only provided authority to regulate the providers, plans, and their healthcare clearinghouses. The HHS addressed this in the privacy regulations by defining service providers as 'business associates' and requiring covered entities to enter into contracts with business associates that provided for the safeguarding of protected health information (45 C.F.R. Parts 160 and 164).

Under the HIPAA Privacy Rule, these contracts, commonly known as 'business associate agreements,' created contractual obligations on business associates to limit their use and disclosure of protected health information, put in place appropriate safeguards, help covered entities facilitate patient rights, report impermissible uses and disclosures of protected health information to the covered entity, and provide records to the HHS upon request, among other things (45 C.F.R. § 164.504(e) (2020).

The subsequent HIPAA Security Rule added a few requirements for business associate agreements involving electronic protected health information, such as reporting security incidents.

As a result, between the HIPAA Privacy Rule's initial compliance date in 2003 and the HITECH Act in 2009, HIPAA only indirectly regulated business associates, requiring covered entities to enter into business associate agreements with contractual obligations and restrictions that only the covered

entities could enforce.

In the HITECH Act, Congress made business associates directly subject to certain parts of HIPAA (HITECH Act and §§ 17931, 17932(b), and 17934 of Chapter 156 of Title 42 on Health Information Technology of the U.S. Code). The HITECH Act required business associates to comply with the HIPAA Security Rule, implement notification obligations when an impermissible use or disclosure rose to the level of a 'breach of unsecured protected health information,' and comply with certain HIPAA Privacy Rule requirements. Still, as is detailed in greater depth below, the HIPAA Privacy Rule required business associate agreements to include certain provisions that the HITECH Act did not address, resulting in those provisions remaining only contractual obligations on business associates. For example, the requirement to safeguard a hard copy of protected health information remains only a contractual requirement; a business associate is not subject to penalties under HIPAA for failing to do so. All of this has led to the current regulatory state for business associates: they are subject to different requirements than covered entities; they have three different reporting requirements to covered entities that date back to the HIPAA Privacy Rule, the HIPAA Security Rule, and then the HITECH Act and subsequent Breach Notification Rule; and the HHS can only enforce some of the requirements of a business associate agreement.

2. BUSINESS ASSOCIATE

A business associate generally is a person or entity (45 C.F.R. § 160.103 (2020)):

- that creates, receives, maintains, or transmits protected health information on behalf of a covered entity (or another business associate) for a function or activity that HIPAA regulates; or
- that performs certain specifically identified services (e.g. legal, actuarial, accounting) where the provision of the service involves the receipt of protected health information from the covered entity (or from one of its other business associates).

There are a few exceptions in regulation and guidance. If a covered entity discloses protected health information to a healthcare provider for treatment purposes, then the receiving healthcare provider is not a business associate of the covered entity (even if it is providing the treatment on the covered entity's behalf, such as a hospital that hires a company to provide treatment in its emergency department (45 C.F.R. § 160.103 (2020)). The regulation also includes exceptions for group health plans and their plan sponsors, for certain relationships between government entities, and for covered enti-

ties that participate in an 'organized healthcare arrangement' - certain types of arrangements involving clinically integrated healthcare providers or healthcare providers participating in certain public joint arrangements.

Guidance also indicates that a 'conduit' is not a business associate if it only transports protected health information (with any temporary storage only incidental to the transmission) and does not access the information other than on a random or infrequent basis as necessary to provide the transport service or as required by law.[2] Examples of conduits include the U.S. Postal Service, private couriers, and their electronic equivalents, such as internet service providers. If a conduit also provides services in which it maintains protected health information (other than temporary storage that is incident to the transmission), then it will be a business associate with respect to those storage services (e.g. an internet service provider that also maintains protected health information by offering email and data backup services).

To understand who is a business associate, it is also important to understand exactly what is 'protected health information.' Protected health information includes 'individually identifiable health information' other than information in a covered entity's employment records, certain education records and related treatment records of students, and records of individuals deceased for more than fifty years (45 C.F.R. § 160.103 (2020)). Information generally is 'health information' if it relates to an individual's past, present, or future physical or mental health or condition, the provision of healthcare to the individual, or past, present, or future payment for the provision of healthcare to an individual (45 C.F.R. § 160.103 (definition of 'health information') (2020)). The HHS broadly interprets protected health information to include information that merely identifies someone as a patient of a healthcare provider or member of a health plan, without specific treatment or payment information, or information about participation in a health plan.[3]

The HIPAA Privacy Rule treats health information as individually identifiable unless it has been de-identified through one of two methods:

- an expert in de-identification has determined in writing that there is a very small risk of identification; or
- 18 categories of identifiers have been removed (including dates more specific than a year and most geographic information more specific than the state, including zip codes) and the covered entity or business associate does not have actual knowledge that the remaining information identifies an individual (45 C.F.R. § 164.514(b) (2020)). In practice, this means that seemingly anonymous information, such as a spreadsheet that does not have patient names but has patient zip codes, could qualify as protected health information and make

its holder a business associate (if maintaining the information on behalf of a covered entity).

3. BUSINESS ASSOCIATE AGREEMENTS

As referenced above, the HHS attempted to ensure that certain privacy and security protections follow protected health information to business associates by requiring covered entities to enter into business associate agreements with certain requirements. Business associate agreements must include the following requirements (45 C.F.R. §§ 164.314(a) and 164.504(e) (2020)):

- establish the business associate's permitted and required uses and disclosures of protected health information, which generally cannot include uses or disclosures that the HIPAA Privacy Rule would not allow the covered entity itself to make;
- prohibit any other uses and disclosures of protected health information unless required by law;
- use appropriate safeguards to prevent impermissible uses and disclosures of protected health information (a contractual requirement only with respect to hard copy and verbal protected health information);
- report any impermissible use or disclosure of protected health information to the covered entity (a contractual requirement only if the use or disclosure does not qualify as a 'breach of unsecured protected health information');
- report any security incident involving electronic protected health information (a contractual requirement only, unless the security incident gives rise to a 'breach of unsecured protected health information');
- report a breach of unsecured protected health information as required by the Breach Notification Rule;
- ensure that any subcontractor that creates, receives, maintains, or transmits protected health information agrees to the same restrictions;
- make available protected health information to the covered entity or individual, as set forth in the business associate agreement, for purposes of the individual accessing the protected health information (a contractual requirement only with respect to hard copy protected health information);
- incorporate certain individual-requested amendments to the protected health information (a contractual requirement only);
- provide an accounting of certain disclosures of protected health information upon request;

- if the business associate is to carry out a covered entity's HIPAA Privacy Rule obligation (such as distributing the covered entity's notice of privacy practices), then the business associate should comply with the HIPAA Privacy Rule requirements applicable to the covered entity (a contractual requirement only);
- make the business associate's internal records related to protected health information available to the HHS for purposes of the HHS investigating the covered entity's HIPAA compliance;
- at termination of the business associate agreement, return or destroy protected health information to the extent feasible, and, for information in which return or destruction is infeasible, only further use and disclosure of the information for the purpose that makes return or destruction infeasible and continue to safeguard the information consistent with the business associate agreement; and
- comply with the applicable requirements of the HIPAA Security Rule.

As indicated above, some of the provisions are only contractual; meaning that the HHS cannot impose penalties for a business associate's noncompliance. Other requirements are both contractual and regulatory, meaning that the HHS can directly impose penalties for non-compliance (HHS Guidance on Direct Liability of Business Associates).

HIPAA does not clearly require a covered entity to perform any due diligence or monitoring of a business associate beyond obtaining a compliant business associate agreement. In fact, the HHS initially rejected an ongoing monitoring requirement (HIPAA Privacy Rule, 65 Fed. Reg. at p. 82461). Rather, a covered entity's responsibilities with respect to a business associate's compliance with its business associate agreement is that if a covered entity learns of a pattern of activity or practice of the business associate that materially breaches the business associate agreement, then the covered entity must take reasonable steps to have the business associate cure the breach or end the violation. If such steps are unsuccessful, the covered entity must terminate the relationship with the business associate, if feasible (45 C.F.R. § 164.504(e)(1)(ii) (2020)).

4. SUBCONTRACTOR BUSINESS ASSOCIATES

The HIPAA Privacy Rule has always required business associate agreements to require a business associate to pass on the same restrictions to its subcontractors (HIPAA Privacy Rule, 65 Fed. Reg. at 82,809, codified at 45 C.F.R. § 164.504(e)(2)(ii)(D) (2000)). The result is a chain of business associate

agreements that travel 'downstream' from business associate to subcontractor, subcontractor to its subcontractor, and so on. However, under the original HIPAA regulations, only the entity that had a direct relationship with the covered entity was considered a 'business associate.'

The 45 C.F.R Parts 160 and 164 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule of 25 January 2013 ('2013 HIPAA Omnibus Rule') (codified at 45 C.F.R. § 160.103)) amendments to the various HIPAA regulations implementing the HITECH Act, the Genetic Information Nondiscrimination Act of 2008, and other changes, revised the definition of 'business associate' to include subcontractors that create, receive, maintain, or transmit protected health information on behalf of a business associate. As the HITECH Act made business associates directly subject to certain HIPAA requirements, the result of the 2013 HIPAA Omnibus Rule's change was to also make subcontractors directly subject to such requirements. Accordingly, subcontractor business associates are essentially treated the same as any other business associate.

The HIPAA Privacy Rule requires that a business associate require the subcontractor to agree to the same restrictions and conditions that apply to the business associate (45 C.F.R. § 164.504(e)(2)(ii)(D) (2020)). A business associate agreement between a covered entity and business associate, however, may include provisions that are not required by HIPAA, such as indemnification clauses. The 2013 HIPAA Omnibus Rule's preamble commentary clarifies that such voluntarily negotiated provisions are outside the HIPAA Privacy and Security Rules' governance, suggesting that these need not be part of the same restrictions and conditions that a business associate must pass on to a subcontractor (2013 HIPAA Omnibus Rule, 78 Fed. Reg. at 5601). However, 'each agreement in the business associate chain must be as stringent or more stringent as the agreement above with respect to the permissible uses and disclosures' (2013 HIPAA Omnibus Rule, 78 Fed. Reg. at 5601). Accordingly, if a business associate agrees to a restriction on use or disclosure (such as agreeing to not disclose protected health information outside of the US), then it arguably must ensure that its subcontractors agree to the same restriction. This can create difficult contractual situations, with business associates trapped in an untenable situation when a covered entity insists on a restriction on use or disclosure of protected health information that a subcontractor will not likewise agree to.

Like a covered entity with respect to a business associate, a business associate must take action upon learning of a subcontractor's pattern of activity or practice that violates the business associate agreement with the subcontractor (45 C.F.R. § 164.504(e)(1)(iii) (2020)).

5. PRIVACY RULE

The HIPAA Privacy Rule includes (45 C.F.R. part 164 subpart E):

- limits on uses and disclosures of protected health information;
- rights for individuals with respect to their protected health information (e.g. rights to access and amend such information, the right to receive a notice of privacy practices); and
- administrative requirements (such as written policies and procedures and designation of a privacy officer).

A business associate generally is subject to the same limits on uses and disclosures of protected health information, as it generally may not use or disclose protected health information in a manner that the covered entity could not, except for uses and disclosures for data aggregation involving multiple covered entities, and for the business associate's proper management and administration (45 C.F.R. §§ 164.502(a)(3) and 164.504(e)(2)(i)(2020)). Additionally, the business associate may not use or disclose protected health information other than as the business associate agreement permits or requires. For example, while a covered entity may disclose protected health information to a public health authority for public health purposes, a business associate may not do so unless permitted by its business associate agreement or required by law.

With respect to the rights that the HIPAA Privacy Rule provides to individuals, a business associate's role generally is limited to assisting the covered entity with facilitating such rights. For example, if an individual requests access to or amendment of certain protected health information, it primarily falls to the covered entity to accept or deny the request or make the amendment. But if the business associate maintains the protected health information at issue, then the business associate must provide access (either to the covered entity or directly to the individual, as specified in its business associate agreement) and incorporate any amendments at the covered entity's direction (45 C.F.R. § 164.504(e)(2)(ii)(E) and (F) (2020)). In 2016, the 21st Century Cures Act granted business associates authority to provide individuals with access to their protected health information (seemingly without regard to whether the business associate agreement authorises the business associate to provide access directly to the individual) (21st Century Cures Act, 42 U.S.C. § 17935(e)(2)), although HHS had not yet promulgated regulatory changes to implement this statutory provision. A business associate also must account for certain non-routine disclosures (such as impermissible disclosures or disclosures required by law), and provide this accounting of disclosures to the covered entity (or, at the covered entity's direction, to the individual) upon request (45 C.F.R. § 164.504(e)(2)(ii)(G) (2020)). The HIPAA Privacy Rule does not require a business associate to maintain a notice of privacy practices, nor to facilitate a covered entity's provision of its notice to individuals.

The HIPAA Privacy Rule administrative requirements do not apply to business associates, such as the requirement to maintain privacy policies and procedures, designate a privacy officer, or sanction workforce members who violate the HIPAA Privacy Rule. An exception is that a business associate agreement must require the business associate to maintain appropriate safeguards around protected health information, which is analogous to a covered entity's requirement to implement reasonable and appropriate safeguards. This safeguards requirement, however, is only a contractual obligation for business associates. While not required, a business associate may find it helpful to implement privacy policies and procedures to ensure compliance with its business associate agreements and applicable HIPAA Privacy Rule provisions.

6. SECURITY RULE

In contrast to the HIPAA Privacy Rule, the HIPAA Security Rule applies to business associates in the same manner as covered entities (45 C.F.R. part 164 subpart C (2020)). While the HITECH Act only requires business associates to comply with certain provisions of the HIPAA Security Rule governing administrative, physical, and technical safeguards and policies and procedures, the HHS interprets the remainder of the HIPAA Security Rule's provisions, such as its 'general rules,' to implicitly also apply to business associates (as these were incorporated by reference into the provisions that the HITECH Act makes applicable) (2013 HIPAA Omnibus Rule, 78 Fed. Reg. 5590).

The HIPAA Security Rule includes dozens of standards and implementation specifications. In short, the provisions require a variety of administrative, physical and technical safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information (45 C.F.R. §§ 164.308 to 164.312 (2020)). While the HIPAA Privacy Rule applies to all forms of protected health information, the HIPAA Security Rule only applies to electronic protected health information (45 C.F.R. § 164.302 (2020)). The HIPAA Security Rule is flexible and scalable, allowing a business associate to address standards and implementation specifications by determining what combination of controls is reasonable for the business associate's unique organisation (organisation (45 C.F.R. § 164.306 (2020)). For example, while the HIPAA Security Rule requires reasonable and appropriate authentication of users who have access to electronic protected health information, it provides a business associate discretion to determine a reasonable authentication scheme, rather than requiring a particular level of password strength or limit on failed login attempts.

While all of the HIPAA Security Rule's standards are required, some of its implementation specifications are 'addressable.' Where an implementation specification is addressable, a business associate must implement it where reasonable and appropriate (45 C.F.R. § 164.306(d)(3)(i) (2020)). If a busi-

ness associate determines that it is not reasonable to implement an addressable implementation specification, then it must document this determination and implement any equivalent alternative measures if reasonable and appropriate (45 C.F.R. § 164.306(d)(3)(ii) (2020)).

The HHS generally treats the requirement to conduct an accurate and thorough enterprise-wide risk analysis as the most important of the HIPAA Security Rule's requirements. This requirement has been the leading cause of the HHS entering into formal financial settlement agreements with covered entities and business associates, and the HHS has audited business associates on this requirement[4]. The HHS has issued Guidance on Risk Analysis where it outlines the elements it expects a risk analysis to include.

7. BREACH NOTIFICATION RULE

A business associate is contractually required to report all impermissible uses and disclosures and security incidents to a covered entity (or, in the case of a subcontractor, to the upstream business associate) (45 C.F.R. §§ 164.314(a)(2)(i)(C) and 164.504(e)(2)(ii)(C) (2020). If an impermissible use or disclosure qualifies as a 'breach of unsecured protected health information,' then the business associate is required by regulation to report the breach upstream without unreasonable delay and no later than 60 days after discovery of the breach (45 C.F.R. § 164.410 (2020)). The business associate must, to the extent possible, include in its notice the identity of all affected individuals and the same content that the covered entity must include in its notifications to affected individuals and the media (45 C.F.R. §§ 164.404(c) and 164.410(c) (2020)):

- a brief description of what happened (including dates of the breach and discovery);
- a description of the affected protected health information (such as whether social security numbers are impacted);
- any steps individuals should take to protect themselves from potential harm;
- a brief description of what the business associate is doing to investigate the breach, mitigate harm, and protected against further breaches; and
- contact procedures for individuals to ask questions or learn additional information.

It is common for the business associate to interpret the last content requirement as only requiring contact information for the covered entity to contact the business associate, rather than for affected individuals to contact the business associate.

A covered entity or business associate may determine that an impermissible use or disclosure is not a 'breach of unsecured protected health information' because (45 C.F.R. § 164.402 (2020)):

- the information is secured through an appropriate level of encryption or destruction;
- one of three statutory exceptions apply (e.g., an unintentional internal use in good faith, a disclosure to someone at the same business associate who was authorised to access the information, or a good faith belief that the unauthorised recipient could not retain the information); or
- a breach risk assessment demonstrates a low probability of compromise of the protected health information. The breach risk assessment must consider at least four factors:
    - the nature of the protected health information (such as its identifiability and sensitivity);
    - the nature of the recipient (such as whether the recipient has legal obligations to protect the information);
    - whether the recipient actually accessed or viewed the protected health information; and
    - the extent the risk to the protected health information has been mitigated (such as through destruction and/or a confidentiality agreement).

A covered entity may rely on a business associate's breach risk assessment, or may conduct its own and reach a different conclusion.

While the business associate's only legal obligation is to notify the upstream entity, a covered entity must notify affected individuals, the HHS (through a web reporting portal), and the media (if more than 500 individuals in a state or jurisdiction are affected) (45 C.F.R. §§ 164.404(c) to 164.408 (2020)). While not required by HIPAA, the parties to a business associate agreement can include an indemnification provision requiring a business associate to indemnify the covered entity for some or all of its breach costs. Additionally, a covered entity can delegate its breach notification obligations to a business associate, which may be useful in a breach affecting a large number of covered entities in order to avoid duplicate notices to affected individuals.

8. PENALTIES

A covered entity can contractually hold a business associate liable for a violation of the business associate agreement by the latter. Likewise, a business associate can hold a subcontractor contractually liable.

If a business associate (including a subcontractor business associate) violates a direct regulatory requirement, then it is subject to civil penalties and, in some cases, criminal penalties. The HHS Office for Civil Rights ('OCR') may impose civil monetary penalties, with minimum and maximum amounts

varying based on the level of knowledge and culpability (45 C.F.R. § 160.404(b)(2) (2020)):

- $119 to $59,522 - the business associate did not know and by exercising reasonable diligence, would not have known of the violation ('no knowledge');
- $1,191 to $59,522 - the violation was due to reasonable cause and not to willful neglect ('reasonable cause');
- $11,904 to $59,522 - the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the entity knew, or, by exercising reasonable diligence, would have known that the violation occurred ('wilful neglect – corrected'); or
- $59,522 to $1,785,651 - the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity or business associate knew, or by exercising reasonable diligence, would have known that the violation occurred ('wilful neglect – not corrected').

The value of these fines is adjusted, annually in accordance with the Federal Civil Penalties Inflation Adjustment Act of 1990 (as amended in 2015) (section 701 of Pub. L. 114-74). The updated amounts are published annually at 45 CFR part 102 (Annual Civil Monetary Penalties Inflation Adjustment, 85 Fed. Reg. 2869 (Jan. 17, 2020)).

The OCR can treat each separate day that there is a violation, or each separate individual where there is a violation involving protected health information of multiple individuals, as a separate violation (45 C.F.R. § 160.406 (2020)). For multiple violations of an identical provision (e.g. the prohibition on impermissible disclosures), HIPAA includes penalty caps per calendar year. There is currently some confusion regarding the amount of such caps because the HITECH Act includes minimum caps and maximum caps for each level of culpability, leaving ambiguity as to whether to apply the minimum cap or the maximum cap. For example, for a violation in which there is no knowledge, the HITECH Act set forth minimum and maximum penalties per violation, and minimum ($25,000) and maximum ($1,500,000) caps on penalties for multiple violations of the same provision during the same calendar year. When implementing the HITECH Act under President Obama, the HHS interpreted the maximum caps of $1,500,000 to apply for each level of culpability, which is reflected in the regulations (adjusted for inflation to $1,785,651). Under President Trump, however, the HHS interpreted the statute differently, issuing a notice of enforcement discretion taking the position that the minimum caps should apply

. Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties, 84 Fed. Reg. 18,151 (Apr. 30, 2019). The HHS interpretation under President Trump did not result in a change in the regulations, however, and so the current administration may choose to follow the regulations, applying the maximum cap of $1,785,651 at each level of culpability. Where there are multiple HIPAA provi-

sions violated (e.g. a failure to implement policies and procedures, a failure to impose sanctions on workforce members who violate the HIPAA Privacy Rule, a failure to reasonably safeguard against impermissible uses or disclosures), the cap is applied separately for each provision (meaning that total penalties can significantly exceed $1.8 million).

State Attorneys General ('AGs') can bring an action on behalf of their affected residents seeking lower penalties of up to $100 per violation, with the calendar year caps of $25,000 for multiple violations of an identical provision (42 U.S.C. § 1320d-5(d) (2019)).

The U.S. Department of Justice ('DOJ') can bring criminal penalties against any person who knowingly obtains or discloses protected health information in violation of HIPAA (42 U.S.C. § 1320d-6(a) (2019)). The criminal penalties are up to $50,000 and/or up to one year imprisonment, up to $100,000 and/or up to five years imprisonment if the offence is committed under false pretences, and up to $250,000 and/or up to ten years imprisonment if the offence is committed with intent to sell, transfer, or use protected health information for commercial advantage, personal gain, or malicious harm (42 U.S.C. § 1320d-6(b) (2019)).

While the potential penalties are very high, in practice the OCR historically has resolved the vast majority of investigations (approximately 99%) in which it finds indications of non-compliance through voluntary corrective action or technical assistance, rather than financial penalty or settlement. Additionally, AGs in a number of states have brought actions under HIPAA, with a record number in 2018, mostly arising from security breaches. Further, US attorneys within the DOJ have focused their criminal actions on cases that generally involve financial fraud, such as identity theft, or the occasional high profile case involving snooping or sale of medical records.

---

1. Joseph Conn, Kassebaum Baker on HIPAA, health IT and a changed lawmaking environment, Modern Healthcare, 29 August 2011; HIPAA § 264, 42 U.S.C. § 1320d note.

2. Frequently Asked Questions #245, U.S. Department of Health and Human Services Office for Civil Rights (19 December 2002).

3. Health Services Research and the HIPAA Privacy Rule, HHS, (20 May 2005); 45 C.F.R § 164.504(f)(1)(iii) (applying the HIPAA Privacy Rule to information that merely identifies whether an individual was a patient of a health care provider).

4. Resolution Agreements and Civil Money Penalties, HHS, (accessed 2 August 2020).