Chapter 5

PATIENT INFORMATION AND PRIVACY

I. HIPAA Basics for Arbitrators

Briar A. Andresen, Esq.[1]

The privacy provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[2] have been around for well over a decade now. Health care consumers generally understand that their providers, insurers, and employers have an obligation to keep health information "private," but little more. In fact, the law is not always well understood even by those in the health care industry who are tasked with implementing HIPAA policies and procedures for their organizations. This is in part because HIPAA is a fairly complex set of laws and regulations that has gone through several changes since the first set of privacy regulations was proposed in 1999. And, of course, there will always be gray areas when dealing with an amorphous concept such as "privacy," particularly when there is a clash between enhancing privacy protections, on the one hand, and a concerted, government-driven effort to improve health care by facilitating the sharing of and access to information on the other.

When enacted in 1996, HIPAA included several parts, not just the privacy provisions, and was intended to "improve the efficiency and effectiveness of the health care system"[3] through various "administrative simplification" provisions. These provisions required the U.S. Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security.

---

[1]Fredrikson & Byron, P.A., Minneapolis, MN.

[2]Pub. L. No. 104-191, 110 Stat. 1936.

[3]*See* U.S. Department of Health & Human Services, Office for Civil Rights, Health Information Privacy, *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html.

In an effort to protect the privacy of health information in an increasingly electronic age, the law also included provisions that mandated the adoption of federal privacy regulations for health information (the Privacy Rule).

HHS published the "final" Privacy Rule in December 2000,[4] and then modified it in August 2002 (before its required compliance date) in response to loudly voiced concerns that the finalized rule was not workable.[5] Compliance with the Privacy Rule was required as of April 14, 2003 (although the compliance date was extended to April 14, 2004, for small health plans).

The HIPAA Security Rule[6] is a companion to the Privacy Rule; the Security Rule sets standards to protect a covered entity's electronic protected health information (ePHI). The Security Rule requires covered entities (and their business associates) to implement appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI. The Privacy Rule and the Security Rule[7] are administered and enforced by the Office for Civil Rights (OCR) within HHS, and an Enforcement Rule provides standards for the enforcement of HIPAA.[8] Although Security Rule and Enforcement Rule compliance are important obligations, Part I of this chapter focuses on the Privacy Rule, which is what most people think of when they hear "HIPAA."

What Does HIPAA Do, and What Does It Require?

The Privacy Rule, for the first time, set national standards for the safeguarding of protected health information (PHI), individually identifiable information (whether in written, electronic, or oral form) that relates to an individual's health, the provision of health care to an individual, or the payment for health care;

---

[4]65 Fed. Reg. 82,461 (Dec. 28, 2000).

[5]67 Fed. Reg. 53,181 (Aug. 14, 2002).

[6]The final Security Rule, which set national standards for protecting the confidentiality, integrity, and availability of electronic protected health information (PHI), was published in February 2003, and compliance was required as of April 20, 2005 (April 20, 2006 for small health plans).

[7]45 C.F.R. Part 160; 45 C.F.R. Part 164, Subparts A & C.

[8]The HITECH Act Enforcement Interim Final Rule was published at 74 Fed. Reg. 56,123 (Oct. 30, 2009). HITECH is discussed in more detail below under "Business Associates."

and that identifies the individual or provides a reasonable basis to identify the individual.[9]

The Privacy Rule applies to three types of "covered entities": health plans, health care clearinghouses, and health care providers that conduct the standard health care transactions electronically.[10] Essentially, this means that HIPAA applies to *almost* all health care providers, because electronic submission of claims is the standard in the industry, and in many cases is required for payment of the claim.[11] The Privacy Rule sets a "floor" for the protection of health information and provides a number of rights for individuals with regard to their own health information.

Generally, HIPAA prohibits the use or disclosure of PHI unless the use or disclosure is authorized by the individual (or his or her personal representative), or otherwise specifically permitted by the Privacy Rule. HIPAA does not *require* covered entities to make any particular disclosures (other than disclosures to the government for compliance investigations, or disclosures to the individual who is the subject of the information). The Privacy Rule does have a lengthy list of permitted disclosures, but before any disclosure is made, covered entities must review applicable state laws to ensure that the disclosure is permitted.

HIPAA generally preempts "contrary" state laws unless the state law is *more protective* of health information, or allows an individual to have *greater access to his or her own information*, in which case the "contrary" state law still controls.[12] The preemption issue can be particularly relevant with regard to state laws regarding consents and authorizations, court orders, subpoenas, or administrative requests for information—state law is often more protective of information in these cases and can require some additional hoops to jump through before PHI may be accessed or disclosed. The key is that, in addition to knowing HIPAA's requirements, an arbitrator and those participating in an arbitration must also know the

---

[9]If information has been "de-identified," then it is not subject to the Privacy Rule's protections. See discussion below under "De-Identified Information and Limited Data Sets."

[10]45 C.F.R. §160.102(a).

[11]Note, however, that a person or entity may meet the HIPAA definition of a "health care provider" without being a covered entity. For example, many medical device companies have employees who spend time in hospital operating rooms helping physicians determine the proper device for a specific patient. When they perform these services, they are providing "health care." These people do not, however, bill for their services in the same way that physicians, hospitals, or clinics do, and they are therefore not "covered entities" (nor are they business associates), so they are not technically bound by HIPAA's requirements.

[12]45 C.F.R. §160.203. See the definition of "contrary" *id.* §160.202.

applicable state law provisions in the jurisdiction in which the PHI is to be disclosed, in order to determine how HIPAA and state law interact, and which will control the use or release of the PHI.

HIPAA requires covered entities to take a number of administrative measures, including the provision of information to patients on how their information may be used and disclosed, and what rights patients have. These requirements are set forth in each covered entity's "Notice of Privacy Practices" or "Notice," which covered entities must provide to all of their patients. The Notice has a number of required elements, but covered entities are free to add additional information to their forms and to include a description of additional protections that the covered entity might provide for the PHI in its possession. The Notice is also supposed to address state laws that are more protective of health information or that allow an individual to have greater access to his or her PHI, but this is a commonly overlooked requirement.

HIPAA's Permitted Disclosures

The most common permitted disclosures are those made by covered entities for treatment,[13] payment,[14] and health care operations.[15] HIPAA does not require any consent or authorization for any of these disclosures, but state laws may require consents for some or all of these disclosures. If no specific exceptions apply to the general "may not disclose" rule, and a disclosure of PHI is not specifically permitted, then a covered entity will need a HIPAA-compliant "authorization" signed by the individual or his or her personal representative in order to disclose PHI. The authorization has a number of required elements, including a statement that, once the information is disclosed pursuant to the authorization, it may no longer be protected by federal law and may be re-disclosed by the recipient.

---

[13]This term includes the provision, coordination, or management of health care and related services by one or more health care providers, including consultations between health care providers relating to a patient, or referrals of patients. *See id.* §164.501.

[14]This term includes any activities to obtain payment or reimbursement for health care services. This would include billing and collection activities, or reviewing services for medical necessity, coverage, and justification of charges. *See id.* §164.501.

[15]This is a broad category that includes financial, administrative, legal, and quality improvement activities that are used to run a business and to support treatment and payment functions. It includes reviewing the competence of health care professionals and evaluating practitioner performance as well as conducting or arranging for medical review, legal, or auditing services. *See id.* §164.501.

As part of the recently finalized HIPAA Omnibus Rule, the Centers for Medicare and Medicaid Services (CMS), the agency responsible for the administrative simplification provisions of HIPAA, provided a new option for individuals who wish to use the individual's right of access to "direct" a covered entity to transmit PHI to a third party. If the individual's request is in writing, signed by the individual, and clearly identifies the designated person and where to send the information, the covered entity must transmit the requested PHI to the third party.[16] The inclusion of this option seems to lessen the need to use a more formal authorization in most situations.

Although disclosures not specifically permitted by HIPAA already require a patient's authorization, the Privacy Rule specifically requires authorizations for marketing uses or disclosures as well as for uses and disclosures of psychotherapy notes. The marketing provisions are highly complex and have several exceptions (they were modified in the finalized Privacy Rule update), and they will not be discussed in detail here. For psychotherapy notes, the key is that the category of information that meets the HIPAA definition of "psychotherapy notes" is very limited. The term does not include information that would be found in a patient's medical record—even for a patient undergoing psychiatric treatment. The term applies only to information that a therapist keeps for his or her own purposes, such as notes written—and not intended for inclusion in the patient's record—that remind the therapist of information that would be useful only to that therapist.

"Incidental disclosures" of PHI are commonplace and are not a violation of the Privacy Rule. An incidental disclosure is permitted if it is a byproduct of another permissible or required use or disclosure, but a covered entity must have reasonable safeguards in place to protect against impermissible uses and disclosures.[17] What is considered "incidental" is somewhat of a gray area, but some examples of typical incidental disclosures are the sign-in sheet at a clinic, where patients may see other patients' names, or an emergency room setting, where absolute privacy cannot be guaranteed in the triage process.

For most disclosures and uses of PHI, covered entities must use or disclose only the "minimum necessary" amount of PHI to accomplish the purpose of the use or disclosure. For internal uses

[16] 45 C.F.R. §164.524(c)(3)(ii).
[17] *Id.* §164.502(a)(iii).

of information, the use or disclosure must be consistent with job duties, and covered entities are supposed to describe the categories of information that are necessary for particular duties. So, for example, registration staff may have access to an electronic health record in order to schedule patients, but they may not need access to the patient's entire record to perform those duties, and therefore should not be permitted to access the entire record. The minimum necessary requirement does *not* apply for certain uses and disclosures, such as when information is disclosed to the subject of the PHI, when it is disclosed pursuant to a HIPAA-compliant authorization, or when it is disclosed to a public official when required by law and the public official has represented that the information requested is the minimum necessary for the purpose of the disclosure. Most importantly, the minimum necessary requirement does not apply when PHI is used or disclosed for treatment purposes. A covered entity may therefore disclose *all* PHI when it is requested by another covered entity for treatment purposes.

Other Specifically Permitted Disclosures

HIPAA specifically permits certain disclosures of PHI—although, again, states are free to impose restriction on these disclosures, and in many cases what HIPAA permits, states forbid unless a patient consents to the disclosure in question. The following sections discuss disclosures that are expressly permitted (but never required) by the Privacy Rule. In all cases, state law must be reviewed to determine whether the disclosure is actually permitted.

Judicial and Administrative Proceedings

PHI may sometimes be part of an arbitration proceeding, but before information may be disclosed as part of the arbitration, a covered entity will need to ensure that the disclosure is permissible. The Privacy Rule permits disclosure of PHI in response to orders of a court or "administrative tribunal." Unfortunately, the term "administrative tribunal" has not been defined in the Privacy Rule or otherwise discussed by OCR. Still, it seems likely that the Privacy Rule reference to an "administrative tribunal" is intended to include only bodies that have the force of law, and is unlikely in most cases to include arbitration.

In the absence of a court order or order from an administrative tribunal, PHI still may be disclosed in response to subpoenas (including subpoenas lawfully issued by an arbitrator), discovery requests, and other lawful process.[18] However, if there is no court or administrative tribunal order, then there are a number of other requirements that must be met before a covered entity may disclose the information in response to a subpoena, discovery request, or process. The covered entity must ensure that it has received "satisfactory assurance" from the party seeking the information that reasonable efforts have been made by the party to ensure that either (1) the individual who is the subject of the PHI has been given notice of the request for the PHI; or (2) the party seeking the information has secured a qualified protective order that meets HIPAA requirements.[19]

Receiving "satisfactory assurance" for providing notice to the individual who is the subject of the PHI means that the party seeking the information can provide a written statement and accompanying documentation that (1) it has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to have mailed a notice to his or her last known address); (2) the notice included sufficient information about the litigation or proceeding to permit the individual to raise an objection to the court or administrative tribunal; and (3) the time for the individual to raise objections has elapsed without any objections being filed or with the objections being resolved by the court or administrative tribunal.[20]

Receiving "satisfactory assurance" regarding the securing of a protective order means that the party seeking the information has provided a written statement and accompanying documentation that the parties to the dispute have agreed to a qualified protective order and have presented it to the court or administrative tribunal or that the party seeking the information has requested a qualified protective order from the court or administrative tribunal.[21]

A "qualified protective order" is an order of the court or administrative tribunal or a stipulation by the parties to the litigation that (1) prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such

[18] *Id.* §164.512(e).
[19] *Id.* §164.512(e)(1)(ii).
[20] *Id.* §164.512(e)(1)(iii).
[21] 45 C.F.R. §164.512(e)(1)(iv).

information was requested, and (2) requires either the return of the PHI to the covered entity or the destruction of the PHI (including all copies) at the end of the litigation or proceeding.[22]

Again, state laws are often very specific about what may be produced in response to a subpoena or discovery request. When state laws are more limiting than HIPAA, the complex Privacy Rule requirements for satisfactory assurance generally do not come into play.

If a party that is a covered entity plans to disclose PHI in an arbitration, then the covered entity will need to get either the individual's authorization for the disclosure (or a signed and written request from the individual to direct the covered entity to transmit the PHI to a third party—including the arbitrator) or the satisfactory assurance just described. Generally, it will not be up to the arbitrator to determine whether to permit the disclosure; the parties should stipulate to the disclosure and the protections required, or the party seeking the disclosure should satisfy either the individual notification requirements or the court/administrative tribunal requirements. Any PHI disclosed pursuant to those stipulations and limitations should be considered by the arbitrator during the arbitration, then handled per the requirements of the stipulation, order, or other limitations.

It is fairly common for PHI to be produced in redacted form for arbitrations and other proceedings, but note that simply redacting patient names and other "direct" identifiers is not enough for the information to be considered "de-identified" and therefore no longer covered by HIPAA. The requirements above continue to apply even for redacted information if it does not meet the criteria for de-identified data.[23] Even so, redacting information is a reasonable and appropriate measure, and PHI should be redacted to the extent that it can be and still is useful in the arbitration. Arbitrators should advise the parties to the arbitration to redact information when possible.

Family and Friends

HIPAA allows disclosures of PHI to family and friends if (and to the extent) those people are involved in the individual's care. If it is relevant for care, then PHI also can be used and disclosed for

[22] *Id.* §164.512(e)(1)(v).

[23] De-identified information is discussed in more detail below under "De-Identified Information and Limited Data Sets."

notification purposes. There are some slightly different requirements depending on whether the subject of the PHI is present or not present. If the individual is present (and has capacity) and has agreed or previously agreed or has had the opportunity to object to the sharing of PHI and does not object, or it can be reasonably inferred from the circumstances that the person does not object, then HIPAA permits the sharing. If the individual is not present (or is incapacitated), or if there is an emergency situation, then disclosure is permitted when the health care professional determines that it is in the individual's best interests, and then only as directly relevant to the person's involvement in the individual's care. A health care professional can use his or her judgment to make reasonable inferences about family members or friends picking up prescriptions, supplies, or other similar forms of PHI. The most common trap here is for a health care professional to reveal too much information, or to reveal information to a person who is not involved in the individual's care. Spouses, for example, do not automatically have a right to information about each other's treatment, and health care professionals should be cautious in such situations.

Parents, Minors, and Other Legally Authorized Representatives

Under HIPAA, an "individual" is the person who is the subject of the PHI.[24] Under the Privacy Rule, a "personal representative" is a person with "authority, under applicable law, to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care."[25] A personal representative must be treated as if he or she were the individual. Personal representatives may include those designated in a health care power of attorney, guardians, or other designated individuals who may be given authority under state law. HIPAA defers to state laws on when parents may have access to the PHI of their minor children; so, if a minor has the right to confidential treatment of pregnancy-related information, then HIPAA would not treat the minor's parent as a personal representative for purposes of that specific PHI.

[24] 45 C.F.R. §160.103.
[25] *Id.* §164.502(g).

Public Health Activities

Covered entities may disclose PHI to a public health authority for public health purposes.[26] This includes government agencies authorized by law to collect information for controlling disease, injury, or disability, including vital statistics (births and deaths), public health surveillance, etc. This provision also allows reporting for Food and Drug Administration (FDA) tracking purposes. The public health provision also allows disclosure of PHI to a public health authority authorized to receive reports of child abuse or neglect, although there is another section of the Privacy Rule that specifically permits disclosures about victims of abuse, neglect, or domestic violence.

Health Oversight Activities

PHI may be disclosed for oversight activities that are authorized by law, including audits; civil, administrative, or criminal investigations; inspections; and other types of proceedings or actions, when the proceedings are necessary for oversight of the health care system or government benefits where health information is relevant to eligibility, or for entities that are subject to government regulatory programs where health information is necessary to determine compliance.[27]

Law Enforcement

Covered entities may disclose PHI for the following law enforcement purposes:[28]

- When the law requires the disclosure for reporting certain kinds of wounds or injuries (for example, gunshot wounds or burns); or in response to a court order, warrant, subpoena, summons, grand jury subpoena, or certain administrative requests (as long as the information sought is relevant and material to a legitimate law enforcement inquiry, the request is specific and limited in scope to the extent practicable, and de-identified information could not reasonably be used).
- In response to a law enforcement request for location and identification purposes of a suspect, fugitive, material witness,

[26] *Id.* §164.512(b).
[27] *Id.* §164.512(d).
[28] *Id.* §164.512(f).

or missing person, provided that the information disclosed is limited to name and address, date and place of birth, Social Security number, blood type and Rh factor, type of injury, date and time of treatment, date and time of death, and a description of distinguishing physical characteristics.

- When law enforcement requests information about the victim of a crime, so long as the individual agrees to the disclosure or (if the individual cannot agree because of incapacity or emergency) if the law enforcement official says the information is needed to determine whether there has been a violation of law by someone other than the victim, and that immediate law enforcement activity depends on the disclosure and would be materially and adversely affected by waiting until the individual is able to agree, and the disclosure is in the best interests of the individual.
- When an individual has died, for the purpose of alerting law enforcement of the death, if the covered entity has a suspicion that the death might have resulted from criminal conduct.
- When the covered entity believes in good faith that the PHI constitutes evidence of criminal conduct that occurred on the premises of the covered entity.
- To report crime in a medical emergency not on the premises of a covered health care provider if the disclosure is necessary to alert law enforcement to the commission and nature of a crime; the location of a crime or of the victim of the crime; and the identity, description, and location of the perpetrator of the crime.

Abuse, Neglect, and Domestic Violence

The Privacy Rule permits disclosures of PHI to a government authority about an individual who is believed to be the victim of abuse, neglect, or domestic violence.[29] The covered entity may do so if the disclosure is required by law or if the individual agrees to the disclosure, or to the extent the disclosure is specifically authorized by law and the covered entity believes it is necessary to prevent harm to the individual or other potential victims. Individuals must be notified promptly that such a disclosure has been or will be made, unless doing so would place the individual at risk or if

[29]45 C.F.R. §164.512(c).

the notification would be to a personal representative who is also believed to be the abuser.

Research

Research under the Privacy Rule can be somewhat complicated, but generally use or disclosure of PHI for research purposes requires either a HIPAA-compliant authorization or a finding from a privacy board or institutional review board that a waiver of the authorization requirement is appropriate because the PHI to be used or disclosed will be adequately protected, and that the research could not practicably be conducted without access to and use of the PHI.

Workers' Compensation

HIPAA does not affect uses and disclosures of PHI for workers' compensation purposes, so any disclosure permitted by state law for workers' compensation will also be permitted by HIPAA.[30]

Information About Decedents

HIPAA allows covered entities to share information with coroners and medical examiners for duties authorized by law. Similarly, information may be shared with funeral directors, consistent with applicable law.[31] Note that the death of an individual does not generally affect a covered entity's obligations under HIPAA to protect the individual's PHI; however**,** the newly finalized updates to the Privacy Rule include a provision that covered entities must protect an individual's PHI for only 50 years after the individual's death.[32] After 50 years, the information is no longer subject to HIPAA's protections (although some state laws may continue to protect such decedent information).

Averting a Serious Threat to Health or Safety

The Privacy Rule permits disclosures of PHI, when consistent with applicable law and standards of ethical conduct, if necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.[33] The disclosure has to be made

---

[30] *Id.* §164.512(*l*).
[31] *Id.* §164.512(g).
[32] *Id.* §164.502(f).
[33] *Id.* §164.512(j).

to a person reasonably able to prevent the threat (including the target of the threat). This is generally a "duty to warn" type of disclosure. Disclosure is not permitted, however, when the information is learned in the course of treatment to affect the propensity to commit the criminal conduct.

Miscellaneous Releases

The Privacy Rule also permits disclosures for specialized government functions,[34] including military and veterans activities, national security and intelligence, protective services for the president of the United States, medical suitability determinations, correctional institution and law enforcement custodial situations; and for covered entities that are government programs that provide public benefits.

Business Associates

In recognition of the fact that health care providers need the help of outsiders to provide certain services, the Privacy Rule permits disclosure of PHI to "business associates." A business associate is a person or entity that performs functions or activities involving the use or disclosure of PHI "on behalf of" a covered entity. If a function or activity involves legal, actuarial, accounting, consulting, management, administrative, or financial services where the provision of the services involves the disclosure of PHI, then there is a business associate relationship. A lawyer who needs PHI to perform legal services on behalf of a hospital—for litigation or risk management, for example—would be a business associate of the hospital. A lawyer who handles real estate deals for the hospital, and therefore has no need to use PHI for her services, would not be a business associate (and also should never be provided with PHI). Service providers who do not have extended access to PHI in order to perform services on behalf of the covered entity, such as cleaning services, are not business associates.

Although OCR apparently has not directly addressed the question of whether arbitrators should be considered business associates of covered entities that are parties to arbitration, the most likely analysis is that an arbitrator is a business associate of a covered entity party *if* the arbitration will require the disclosure of PHI. This is because an arbitrator is hired by the covered entity (in

[34] 45 C.F.R. §164.512(k).

part) in order to provide the arbitration service on behalf of the covered entity. Even though an arbitrator functions in a similar capacity to a judge, a judge is performing a service on behalf of the state, county, or other government entity. Similarly, an administrative law judge is performing services on behalf of an administrative agency of the government. Given this, covered entities should request business associate agreements (BAAs) from the arbitrators with whom they work.

Covered entities are required to execute BAAs with their business associates. (Note that, at the current time, a business associate does not appear to have the same responsibility; that is, if the covered entity fails to get a business associate agreement in place, the business associate should not be liable for that failure.) BAAs are usually fairly standard documents, with a number of Privacy Rule–required elements, but many covered entities (and some business associates) include additional provisions or more specific requirements for their business associates. Indemnification provisions, for example, are becoming an increasingly common—and often heavily negotiated—part of BAAs. In order to attempt to stave off heavy-handed BAAs, arbitrators should consider having a standard-issue BAA ready to execute with covered entities.

Under the new HIPAA statutory and regulatory landscape (HITECH),[35] business associates are *directly* responsible for compliance with certain provisions of the HIPAA Privacy Rule and Security Rule, and have direct liability for failing to comply with those provisions. Essentially this means that business associates now have a direct statutory obligation to comply with HIPAA that mirrors what they were required to do under the terms of a standard BAA. Arbitrators should keep in mind the following general considerations:

1. Business associates may use and disclose information received from providers only as permitted by agreement or law.
2. Business associates must have safeguards to prevent unauthorized use or disclosure of PHI and must perform a "security risk analysis" under the Security Rule provisions.[36]

---

[35]Health Information Technology for Economic and Clinical Health (HITECH) provisions of the American Recovery and Reinvestment Act (HITECH). Pub. L. No. 111-5 (2009), Title XIII.

[36]*See* 45 C.F.R. §164.302.

3. A covered entity may terminate the BAA if the business associate does not comply with its requirements.
4. Do not disclose PHI to third parties that are not part of the arbitration. (Certain exceptions apply if a third party agrees to similar protections for the PHI—for example, if the arbitrator needs to consult with an expert).
5. Document any disclosures to third parties.
6. Do not use PHI for purposes other than to provide the arbitration services or for internal management or administrative activities.
7. Report any known unauthorized uses or disclosures of PHI to the covered entity (and take special note of "breaches" as discussed below).
8. Inform the covered entity if it is necessary to retain copies of PHI after the arbitration is complete. If it is not necessary, then return or destroy the PHI.

Although enforcement has, in the past, generally not focused on monetary penalties, a business associate who fails to comply with the HITECH provisions is subject to the same enforcement possibilities as a covered entity—including the potential imposition of civil monetary penalties.

When an arbitration is over, the arbitrator should take steps to destroy all PHI in his or her possession, unless it is necessary to retain it. Properly destroying the information means that there is little risk of violating HIPAA or causing a PHI "breach" through some accidental oversight or from a technology problem. The government has provided guidance on how to make PHI "secure"; thus far, the only two technologies or methodologies that are acceptable are encryption and destruction of the information. Encrypting or destroying the information makes it "secured."

Per government guidance, media on which PHI is stored or recorded may be destroyed in one of the following ways:

- For paper, film, or other hard copy media: shredding or destroying such that the PHI cannot be read or otherwise cannot be reconstructed.
- For electronic PHI: clearing, purging, or destroying consistent with National Institute of Standards and Technology (NIST) Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

Individual Rights Under HIPAA

Individuals are provided with a number of rights under the Privacy Rule, and these rights are described in each covered entity's Notice of Privacy Practices. State laws may provide individuals with greater rights than the Privacy Rule mandates, but the minimum requirements are listed below.

Right to Inspect and Copy[37]

Individuals may inspect and receive a copy of their PHI. This includes information that was not created by the covered entity; as long as the covered entity has the information in its own records, the individual has the right access it. If the covered entity maintains the PHI in an electronic health record, then the individual has the right to receive his or her PHI in electronic form. Covered entities may deny a request to inspect and copy in certain very limited circumstances—for example, if a physician believes it will be harmful to the individual's health, or that the access could cause a threat to others. If there is a denial of access, then the patient may request that the denial be reviewed, and another licensed health care professional chosen by the covered entity (but not the person who denied the request) must review the request and the denial.

Right to Request Amendment[38]

Individuals can request amendments to their medical records if they believe that information is incorrect or incomplete. The request may be denied if the PHI was not created by the covered entity (unless the creator is no longer available to make the amendment), if it is not part of the PHI kept by the covered entity, if it is not part of the information that a patient would be permitted to inspect and copy, or if it is accurate and complete. If an amendment request is rejected, then the patient must receive an explanation. The patient then has the right to submit a rebuttal, which must be included in the patient's record if requested.

---

[37] *Id.* §164.524(a).
[38] *Id.* §164.526.

Right to an Accounting of Disclosures[39]

Patients have the right to request an "accounting of disclosures." This is a list of the disclosures of the patient's PHI that have been made in the previous six years. The accounting does not have to include disclosures that were made for treatment, payment, or health care operations purposes; disclosures that the patient authorized or that have been made to the patient; disclosures for facility directories; disclosures for national security or intelligence purposes; or disclosures to correctional institutions or law enforcement with custody of the patient, among other disclosures. It is expected that upcoming modifications of the Privacy Rule will provide some revision to the accounting requirements.

Right to Request Restrictions[40]

Individuals may request a restriction or limitation on the medical information that a covered entity may use or disclose. This could include a request not to share information with a certain health care provider, or for a particular employee not to have access to the individual's PHI. If a patient pays out-of-pocket in full for an item or service, then the patient may request that the covered entity not disclose information pertaining solely to that paid-for item or service to the patient's health plan for purposes of payment or health care operations.[41] Covered entities must agree with such a request, but they are not required to agree to any other requested restriction.

Right to Request Confidential Communications[42]

Patients may request that a covered entity communicate about medical matters in a certain way or at a certain location. For example, the patient could ask to be contacted only at work or only by e-mail. The covered entity is not permitted to ask the reason for the request and must accommodate all reasonable requests. The covered entity may require that any request specify how or where the patient wishes to be contacted and may require the patient to provide information about how payment will be handled.

---

[39] *Id.* §164.528.
[40] *Id.* §164.522(a).
[41] 45 C.F.R. §164.522(a)(vi).
[42] *Id.* §164.522(b).

De-Identified Information and Limited Data Sets

To be considered de-identified and therefore no longer PHI and no longer covered by the Privacy Rule's requirements, either the information must be determined to be "de-identified" via consultation with a qualified statistical expert or the information must meet the Privacy Rule's "safe harbor" criteria—that is, it must not contain *any* of the following identifiers:

- name;
- geographic subdivisions smaller than a state, including ZIP code;
- date elements (except year) for dates directly related to an individual, including birth date, admission dates, discharge dates, date of death, and all ages and elements of dates (including year) over 89 (although ages may be aggregated into a single category of age 90 or older);
- telephone/fax number(s);
- e-mail address;
- Social Security number;
- medical record number;
- health plan beneficiary number and other account number(s);
- certificate or license number(s);
- vehicle identification and serial number(s);
- device identifier and serial number(s);
- uniform resource locators (URLs) and Internet protocol (IP) addresses;
- biometric identifiers (e.g., finger and voice prints);
- full face photographic images; and
- any other unique identifying characteristic(s) or code(s) (other than those established by an organization to permit re-identification).

Obviously, the requirements for de-identification of PHI are strict, and elimination of all of the above elements (particularly date elements such as dates of treatment) may make the information useless in an arbitration. For that reason, de-identification may not be a particularly useful option for arbitrators. As mentioned previously, redacting as much PHI as possible is a good step for protecting PHI, but the covered entity that wishes to, or is

being asked to, disclose PHI will need to fulfill the requirements related to satisfactory assurance even for redacted information.

Occasionally, covered entities may wish to disclose for research, public health, and health care operations purposes when patient authorization is not able to be obtained and de-identified information will not be useful. The government has recognized that there are some legitimate circumstances where such disclosures are appropriate and does permit those disclosures as part of a "limited data set." To be a limited data set, PHI must be altered via the removal of the following components:

- name,
- street address (but not town/city, state, ZIP code),
- telephone/fax number(s),
- e-mail address,
- Social Security number,
- certificate/license number(s),
- vehicle identification/serial number(s),
- URLs and IP addresses,
- full-face photo(s) and other comparable image(s),
- medical record number,
- health plan beneficiary member number and other account number(s),
- device identification and serial number(s), and
- biometric identifiers (e.g., finger and voice prints).

The following information need not be removed from a limited data set:

- admission, discharge, and service date(s);
- date of death;
- age (including months, days, or hours) (birth date may be used only if both the provider and the researcher agree that it is needed for purposes of research); and
- town/city, state, 5-digit ZIP code.

At the time of the disclosure of a limited data set, a "data use agreement" must be obtained from the recipient of the limited data set. The data use agreement may be in the form of a contract, a memo of understanding, or, for internal use, an agreement signed by the employee.

Enforcement

One of the biggest changes in HIPAA is the implementation of breach notification provisions. Although there has long been a patchwork of state laws on notifying patients of improper disclosures of their health information, the breach notification provisions implemented by the HITECH provisions of the American Recovery and Reinvestment Act mean that, for the first time, there is an obligation under HIPAA to notify patients of breaches of their information.[43] In addition, penalties have generally gotten more significant, and indications are that the government is going to step back a bit from its past policy of simply assisting with compliance and move instead toward penalties or "resolution amounts." There are new "tiers" of civil monetary penalties that are intended to reflect increasing punishment based on levels of culpability. In each of the following cases (except for willful neglect), the maximum penalty is $50,000 per violation, with a cap of $1.5 million for identical violations in a calendar year:[44]

- Violations that are unknown (or with due diligence would not have become known): minimum of $100/violation.
- Violations due to reasonable cause that is not willful neglect: minimum of $1,000/violation.
- Violations due to willful neglect where the violation is corrected within 30 days: minimum of $10,000/violation.
- Violations due to willful neglect that are not corrected within 30 days: minimum of $50,000/violation.

The new law also limits some of the affirmative defenses that previously had been in place.[45] Despite the increased trend toward penalties and enforcement actions, the Secretary is allowed to continue to use discretion to provide technical assistance, obtain corrective action, and resolve possible noncompliance "by informal means" when the noncompliance is due to reasonable cause or when the covered entity did not know that the violation occurred.[46] In addition, state attorneys general also have a newly established right to bring actions on behalf of residents of a state.

---

[43] *See id.* §164.401–.414.
[44] *Id.* §160.404.
[45] *Id.* §160.410.
[46] 74 Fed. Reg. 56,123, 56,128 (Oct. 30, 2009).

Along with increased enforcement is a heightened public expectation that health care companies will hold individuals responsible for their roles in privacy violations. More health care entities are terminating the employment of those who violate HIPAA's privacy obligations, particularly when the behavior is not just negligent, but intentional—particularly in cases of employee curiosity (snooping into ex-spouses or ex-spouses' current significant others' records is a common violation). Particularly when employers face large fines and public embarrassment when improper privacy practices are revealed, many are trying to take a bright-line, zero-tolerance approach to privacy violations.

Enforcement Actions

There have been very few legal cases dealing explicitly with HIPAA, but there have been several investigations that have resulted in settlements (or "resolution agreements"), monetary settlements, or penalties.

CVS: Resolution Agreement and $2.25 million resolution amount, Corrective Action Plan:

- CVS used dumpsters to dispose of PHI.
- Investigation based on media reports.

Rite Aid: Resolution Agreement and $1 million resolution amount, Corrective Action Plan:

- Rite Aid used dumpster to dispose of prescription pill bottles and prescriptions that included patient identifying information.
- Investigation based on media reports.

Providence Health & Services: Resolution Agreement and $100,000 resolution amount, Corrective Action Plan:

- Four back-up tapes and two optical disks were stolen from an employee's car.
- Laptops were stolen on four occasions.
- None of the information was encrypted.

Health Net of the NorthEast, Inc.: Resolution Agreement and $250,000 resolution amount, Corrective Action Plan:

- Portable computer disk drive with PHI of 1.5 million members disappeared from the company's office.
- Health Net spent approximately $7 million to investigate the theft/disappearance and found no evidence that any member had actually been victimized by fraud or identity theft as a result of the lost portable device.

Cignet Health Center: Civil Monetary Penalty of $4,351,600:

- 41 patients requested copies of records; Cignet did not provide them with access. 38 people complained to OCR.
- Cignet failed to respond to OCR's (multiple) inquiries.
- Cignet failed to respond to an OCR subpoena.
- When Cignet finally responded, it sent 59 boxes of original medical records to the U.S. Department of Justice—this included the records of the 11 patients whose records had been requested and the records of 4,500 patients whose information had not been requested.
- Cignet was cited for failure to provide access for 41 individuals ($1,351,600), and failure to cooperate with an investigation (as required by HIPAA) ($3 million).

Phoenix Cardiac Surgery, P.C.: Resolution Agreement and $100,000 resolution amount, Corrective Action Plan:

- Small practice (two physicians) failed to comply with HIPAA in general—lack of training, lack of policies, lack of business associate agreements, etc.
- Practice posted more than 1,000 separate entries of PHI on a publicly accessible Web site (calendar), and on a daily basis transmitted PHI to employees' personal e-mail accounts.

BlueCross BlueShield of Tennessee: Resolution Agreement and $1.5 million resolution amount, Corrective Action Plan:

- Computer theft from network data closet: 57 hard drives with encoded electronic data (including Social Security numbers and PHI), more than 300,000 video recordings, and more than 1 million audio recordings of customer service calls.
- Network data closet was secured by biometric and keycard scan security with a magnetic lock and an additional door with a keyed lock.

- 1,023,209 individuals affected.

UCLA Health System: Resolution Agreement and $865,500 resolution amount, Corrective Action Plan:

- Employees repeatedly examined PHI of patients.
- UCLA Health System failed to appropriately sanction employees.
- UCLA Health System lacked appropriate security measures to reduce risks.

Massachusetts General Hospital: Resolution Agreement and $1 million resolution amount, Corrective Action Plan:

- Employee removed PHI of 66 patients, and the daily office schedules for three days that included the names of 192 patients, from premises to work at home.
- Employee left the records, bound with rubber band, on a subway seat—they were never recovered.

Management Services Organization Washington, Inc.: Resolution Agreement and $35,000 resolution amount, Corrective Action Plan:

- Disclosed PHI to an owned Medicare Advantage plan management company for marketing purposes without an authorization.

Business associates generally have not faced much enforcement action, but the Minnesota Attorney General recently filed suit against Accretive Health, a business associate of two hospitals in Minnesota.[47] Accretive's employee left an unencrypted laptop in his car, and it was stolen. The laptop contained information on thousands of patients at the two hospitals. The incident was investigated by the Office for Civil Rights, the Joint Commission, and the Attorney General. This matter is ongoing with respect to the Office for Civil Rights and its investigation of the hospitals, but Accretive settled with the Minnesota Attorney General for $2.5 million and agreed to stop doing business in Minnesota for six

[47] *See* Complaint, Minnesota v. Accretive Health, Inc. (D. Minn. Jan. 19, 2012), *available at* http://www.ag.state.mn.us/PDF/Consumer/AccretiveHealth20120119.pdf.

years. Although this settlement between the Attorney General and Accretive was not due entirely to HIPAA issues (the focus of the settlement was Accretive's aggressive payment collection approach in certain emergency rooms), the situation was brought to the Attorney General's attention as a result of the laptop situation.

Arbitrators who need PHI to perform their arbitration functions face some risk as business associates, and should take seriously their obligation to keep PHI confidential and to protect it from further disclosure. Business associates should have policies and procedures in place regarding their protection of PHI. Because most of the PHI received by an arbitrator will be fairly limited in scope, the policies of the arbitrator can be fairly simple. Even so, if there will be electronically produced PHI, then the arbitrator should take steps to ensure its protection, including encrypting laptops or other portable devices that could be stolen, and protecting other electronic workstations so that no unauthorized person will gain access.

What Happens When There Is a Violation or Breach?

HIPAA's breach notification regulations were issued in interim final form in August 2009.[48] These regulations implement HITECH Section 13402 by requiring covered entities and their business associates to provide notification to patients following a breach of their unsecured PHI. If PHI is "breached," then the subjects of the PHI must be notified, but the manner in which an individual is notified depends on the specific situation. If a disclosure of PHI truly meets the definition of a "breach" under the regulations (and not all violations of HIPAA and improper disclosures meet that definition),[49] then the covered entity will be required to notify the subjects of the information of the disclosure (or, in the case of a business associate, to notify the covered entity) why it happened, and what the party is doing about it.[50] If the breach affected more than 500 individuals in a state or federal jurisdiction, then media notification will also be required.[51] The government also must be notified, either in a year-end summary

[48] 74 Fed. Reg. 42,740 (Aug. 24, 2009).

[49] To be a "breach," there must be an acquisition, access, use, or disclosure of PHI that is not permitted by HIPAA that compromises the security or privacy of the PHI. *See* 45 C.F.R. §164.402.

[50] 45 C.F.R. §164.404.

[51] *Id.* §164.406.

or immediately if the breach affected more than 500 individuals.[52] Most health care entities are aware of the breach notification requirements, although a relatively low percentage have put policies into place to deal with such an occurrence, and many may not know that each potential breach should be analyzed to make certain that an improper disclosure actually meets the definition of a breach.

Generally speaking, employers (both covered entities and business associates) should train their employees on a regular basis—at the beginning of employment, and then as needed. In some cases, a yearly training program will be appropriate. In other cases, less frequent training may be acceptable. HIPAA does not have specific requirements on what is considered to be "appropriate" training, and so each covered entity (and business associate) will have to make its own determination about what is the best format for training. Covered entities should avoid mistakes such as "one size fits all" training, where all employees are trained in the same way, with the same information, despite differing responsibilities. Another common error is failing to regularly remind employees of the most common violations, and the fact that "common" practices—such as looking up a friend's medical information out of curiosity—can actually cause major HIPAA problems.

Conclusion

HIPAA's reach is expanding, and requirements for both covered entities and business associates have been clarified somewhat through publication of final regulations early in 2013.[53] Arbitrators who have access to PHI as part of an arbitration are likely to be affected as business associates, must be aware of and comply with the requirements of the Privacy Rule (and the Security Rule), and must ensure that their employees comply with all applicable requirements. In making decisions about the cases before them, arbitrators also must be aware of the trends in enforcement of HIPAA and the obligations of covered entities to protect PHI.

---

[52] *Id.* §164.408.
[53] 78 Fed. Reg. 5,566 (Jan. 25, 2013).