Protecting Health Information: the HIPAA Security and Breach Notification Rules [1]

1. Introduction

As health information continues to transition from paper to electronic records, it is increasingly necessary to secure and protect it from inappropriate access and disclosure. If patients’ data is lost or stolen, it is equally important to notify them and hold the people or companies at fault accountable.

The Health Insurance Portability and Accountability Act (HIPAA) addresses some of these concerns. This guide discusses the move away from paper records, and covers the HIPAA Security Rule [2] and Data Breach Notification Rule [3]. For in-depth information about the HIPAA Privacy Rule [4], see PRC Fact Sheets [5] 8a-8d. For information on the HIPAA Enforcement Rule, see Fact Sheet 8a: Health Privacy: HIPAA Basics, Section 7 [6].

2. Electronic Health Records

When a medical record is stored in digital format, it is called an Electronic Health Record [7] (EHR). Providers once stored patients’ medical information in paper charts, but government incentives and private initiatives are encouraging a transition to EHRs in the hope of improving health care quality and efficiency, and perhaps lowering costs. One major benefit (and privacy concern) is the ability for different authorized users to access and add to a patient’s records from different locations.
a. What information is in an EHR?

EHRs may include information providers collect when they see patients in person as well as information they collect through electronic communications. An EHR may contain medical history, a medical professional’s notes, medications, allergies, lab results, demographic data, radiology images, billing data, immunizations, diagnoses, and other patient health information. An EHR may also include communications a patient makes through a health provider’s dedicated network, email, mobile electronic devices, and e-prescribing network that send electronic prescriptions directly to the pharmacy.

b. Is there a national database containing EHRs?

No. However, the U.S. Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology is developing a Nationwide Health Information Network (NHIN) to enable the secure exchange of health information over the Internet. If this effort succeeds, it will create what is effectively a federated database where an individual’s PHI can be accessed wherever it resides (rather than a single data repository for all data).

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) set a goal of having an operative NHIN by 2014 to create a national system that is “interoperable,” meaning that EHR software and systems have the ability to share data with other EHR software and systems.

The 2014 goal was a stretch, and the barriers to interoperability are formidable. Not only are there incompatible technologies and data formats to overcome, but also institutional policies, the need to re-engineer workflow, and the time and effort required to develop the trust that enables covered entities to share PHI outside their own walls. After statewide Health Information Exchanges (HIE) are in place, they will be combined to create the NHIN. The Healthit.gov website contains extensive information about this initiative.

c. How are EHRs different from personal health records (PHRs)?

Health care providers and other HIPAA covered entities maintain EHRs. While some health care providers offer PHR products to their patients, patients can also maintain their own PHRs independently of their providers. For example, many commercial vendors offer PHR systems that allow individuals to store health care information on their computers or in the cloud.

For more information on PHRs in general, see HHS publication, Personal Health Records and the HIPAA Privacy Rule. For more California-specific information about PHRs, see Privacy Rights Clearinghouse California Medical Privacy Fact Sheet C7: Personal Health Records and Privacy.

d. Does HIPAA apply to the data in an EHR?

Yes. The fact that a patient’s data is electronic does not reduce a covered entity’s obligations under HIPAA. In fact, the HIPAA Security Rule only applies to electronic data. By contrast, the HIPAA Privacy Rule applies to data in any format, including paper and electronic records, even oral communications that may or may not have been reduced to paper or electronic format.

e. What are the uses and benefits of EHRs?

EHRs allow health care providers and organizations such as primary care physicians, specialists, laboratories, radiologists, clinics, and emergency rooms to share and access a patient’s health information, thereby enabling patients to be treated from a more complete record. EHRs are supposed to improve health care, increase efficiency, and lower health care costs. In addition, data from EHRs have the potential to aid research efforts and to simplify data collection for mandatory public health reporting.

f. Does the move to EHRs increase privacy and data security risks?

Regardless of whether health information is stored in paper charts or EHRs, privacy and security are major concerns, given the highly sensitive nature of health information. As medical information becomes increasingly accessible in electronic form, the privacy and security risks change. For example with a paper copy of a health record, a patient might worry about it being lost or improperly discarded or copied. With an electronic copy, there are more ways to access the record. In other words, the same aspect of electronic health records that makes them attractive and useful—the ability to share with others—also has the potential to increase privacy and security risks.

Local and national news media frequently report on health data breaches and unauthorized access to medical records. Some of these involve hackers or insiders; others involve lost or stolen computers, mobile devices or removable storage devices (like
flash drives). For information on health data breaches, see PRC’s Chronology of Data Breaches [17].

For a list of commonly asked questions and answers regarding EHR privacy and security, see the “Safeguards” section of HHS’s FAQ [18] on Health Information Privacy.

3. HIPAA Security Rule

The HIPAA Security Rule [2] describes what covered entities [13] must do to secure electronic personal health information [19] (PHI). Even though data security operates behind the scenes and out of patients’ hands, the Security Rule is important for patients to understand because it sets a national standard. All HIPAA covered entities that collect, maintain, use, and transmit electronic personal health information (ePHI) must adopt certain technical and non-technical safeguards to protect it.

a. What kind of records does the Security Rule protect?


This means that paper records stored in filing cabinets are not subject to the Security Rule requirements. Regardless, covered entities and business associates [20] may be held accountable for unauthorized disclosures [21] of PHI in paper or even oral format, as described in the next section.

b. Are there any rules for safeguarding paper records?

Yes. Although the Security Rule does not apply to paper records, all covered entities [13] are subject to the HIPAA Privacy Rule, which prohibits unauthorized disclosure of protected health information [19] (PHI) in any format.

Unauthorized disclosure of paper records may also trigger notice requirements under the Breach Notification Rule [3]. Incidents where more than 500 individuals’ health records are compromised are posted on the HHS website [22]. Most of the paper record incidents boil down to simple carelessness. The following are a few examples of breaches that may occur with paper records.

- A medical practice donates a filing cabinet but forgets to remove the records.
- A doctor leaves records in her car, and the records are stolen.
- A pharmacy disposes of intact, unshredded records in a dumpster.
- A covered entity mails medical records to the wrong recipients.

c. What does the Security Rule require of covered entities and business associates?

The Security Rule requires all covered entities [13] and business associates [23] to have a written security plan.

Under the Security Rule, a security plan must include three components:

- Administrative safeguards. Examples include having a process in place to identify risks, designating a security official, implementing a process to authorize access to information only when appropriate, providing training and supervision to workforce members, and performing periodic assessments of security policies and procedures.

- Physical safeguards. Examples include implementing processes and procedures to limit unauthorized access to facilities, workstations, and devices.

- Technical safeguards. Examples include technical policies and procedures to control access, to ensure data integrity, and to safeguard electronic transmission over a network.

Each component has a number of requirements, some of which may depend on specific factors (such as size).

To learn more about Security Rule requirements, see the HHS Office for Civil Rights’ (OCR) Guidance on Risk Analysis [24] and its Summary of the HIPAA Security Rule [25].

d. Which government agency enforces the Security Rule?

The U.S. Department of Health and Human Services [26] (HHS) Office for Civil Rights (OCR) has enforced the HIPAA Security Rule since 2009. Prior to 2009, the HHS Center for Medicare and Medicaid Services [27] enforced the rule.

e. Will a provider’s notice of privacy practices address health record security?
f. Does the HIPAA Security Rule address disposal of electronic or paper records?

No. However, the HHS [26] Office for Civil Rights (OCR) has issued guidelines [29]. In addition, OCR has imposed $1 million-plus penalties against large pharmacy chains that violated the HIPAA Privacy Rule by improperly disposing of medicine bottles and prescriptions that contained protected health information [30] (PHI).

g. What security risks exist for electronic protected health information (PHI) that did not exist when the Security Rule was adopted in 2003?

There are many, but here are a few more recent security risks:

- **Mobile electronic devices** such as smartphones, laptops, and tablets have become common storage and communication vehicles for both healthcare professionals and patients. Many reported breaches of PHI [30] involve mobile device theft or loss. To learn more about risks associated with mobile devices and tips to maximize security, see HealthIT.gov’s publication *Your Mobile Device and Health Information Privacy and Security* [8].

- **Medical identity theft** occurs when an imposter uses someone else’s personal information to obtain medical treatment or file a claim for treatment with that person’s insurer. Healthcare providers have treatment information on file, but may also have sensitive information such as a Social Security number, credit card or bank account number. Insurance identification numbers are also valuable tools for fraudsters. To learn more about medical identity theft, see the World Privacy Forum’s *Medical Identity Theft Information Page* [31] or the California Attorney General's tips for consumers in *First Aid for Medical Identity Theft* [32].

- **Implantable electronic devices** allow physicians to remotely monitor a patient’s condition and adjust settings. To learn more about implantable devices and security, see the *Government Accountability Report* [33]: *Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices* (August 2012).

4. **Breach Notification Rule**


Remember, that HIPAA sets baseline rules, and a state [34] may enact stricter laws. For California-specific information, see PRC’s California Medical Privacy Guide C3: *Your Medical Information and Your Rights* [35].

a. What is a breach?

Under HIPAA, a breach [36] is defined as “the unauthorized acquisition, access, use or disclosure of protected health information [30] (PHI) which compromises the security or privacy of such information.”

There are three exceptions [36] to this definition:

- when a member of the covered entity’s [13] workforce, acquires, accesses or uses PHI in good faith without further using or disclosing the information in a way that the HIPAA Privacy Rule does not permit;
- when a person authorized to access PHI inadvertently discloses PHI to another person who is authorized to access PHI; or
- when there is a good faith belief that the unauthorized person to whom the PHI has been disclosed would not be able to retain the information.

b. When must a covered entity or business associate notify others of a breach?

Covered entities [13] and business associates [23] do not have to provide notification in the case of every data breach. The protected health information [30] (PHI) breached must have been unsecured (unencrypted data, for example). In addition, the covered entity or business associate may not have to notify individuals if it determines there is a low chance that PHI was accessed, acquired, used, or disclosed as a result of the breach. See 45 CFR § 164.404 [37].
From 2009 until 2013, under HHS’s Interim Final Rule [38], a covered entity did not need to report a breach unless, upon investigation, it determined that disclosure would pose a “significant risk of financial, reputational, or other harm to the individual.” This was controversial [39] because it allowed covered entities to use subjective judgment to determine whether to report a breach. This standard has been supplanted by the 2013 Omnibus Rule [40] which replaced the “risk of harm” standard with a standard based on the chance PHI was compromised.

### c. How does a covered entity or business associate decide when PHI is compromised?

Covered entities [13] must conduct a risk analysis to determine whether PHI [30] has been compromised. The analysis must take into account:

- the nature and extent of the PHI such as the types of identifiers (e.g. name, address, Social Security number);
- the person who gained unauthorized access to PHI;
- whether the PHI was actually acquired or viewed; and
- the extent to which the risk has been mitigated

If, after conducting the risk analysis, a covered entity determines there is a low risk that PHI was compromised, it does not have to provide notice. The HIPAA Omnibus Rule [40] offers the following example of a low risk disclosure: A covered entity misdirects a fax to the wrong physician, and, upon receipt, the receiving physician says he has destroyed the fax.

### d. How do individuals know if their PHI is breached?

Individuals should be notified by first-class mail or email (if they choose to receive email notices) no later than 60 days after the breach is discovered or should have been discovered. However, notice may be delayed if law enforcement requires it, for example, to conduct an investigation of the breach.

The covered entity [13] may post a notice on its website if it has insufficient contact information for 10 or more individuals. If there are fewer than 10, it may try to telephone or provide other notice.

### e. What information will be in a breach notice?

The notice should include at least the following information:

- a brief description of what happened as well as the date of the breach and the date it was discovered;
- the types of information that were involved;
- a description of what actions the covered entity [13] took after the breach was discovered; and
- contact information that allows individuals to ask questions and learn more about the breach, the follow-up, and what steps they should take to protect themselves. Contact information should be either a toll-free number, an email address, a website, or a postal address.

To learn more about breach notifications, see the HHS/OCR website Breach Notification Rule [3].

### f. When must a covered entity notify HHS or the media about a breach?

When there is a breach that affects more than 500 residents of a state, the covered entity [13] must notify relevant media outlets.

Covered entities must notify HHS as well. They must notify HHS of breaches involving fewer than 500 people within a year after the breach is discovered. When a breach involves more than 500 people, HHS/OCR requires notice immediately and posts those breach incidents on its website [22].

### g. Does the HHS website list data breaches caused by a covered entity’s employees or other insiders?

Not specifically. Incidents caused by insiders may be simply reported under the category of “unauthorized access.” However, the HHS website only reports incidents involving more than 500 individuals. Unauthorized access by “insiders” often involves individuals snooping on neighbors, ex-spouses, celebrities, or other employees.

### h. What role does the Federal Trade Commission (FTC) play in safeguarding health information?

The FTC [41] can issue rules regarding breaches of data stored by web-based consumer personal health records (PHR) vendors. However, FTC rules only apply to PHR companies that are not subject to HIPAA.

According to the FTC’s final data breach rule [42] for web-based PHR vendors, the rule also applies to related entities that:
• offer products or services through the website of the PHR vendor;
• offer products or services through the websites of HIPAA-covered entities that offer individuals PHRs;
• access information in a personal health record; or
• send information to a personal health record.

According to the FTC, an example of a PHR entity is an online weight-tracking program that sends information to a personal health record or pulls information from it. Another example would be a HIPAA-covered entity such as a hospital that offers its employees a PHR.

Like covered entities that report breaches to HHS, web-based health data vendors must report a breach to the FTC. Unlike covered entities [13], even incidents involving a single individual are posted on the agency’s website.

To learn more, see Breach Notices Received by the FTC [43] and Health Privacy [44].

6. Resources

Laws and Regulations

Health Insurance Portability and Accountability Act of 1996 [45], PubLaw 104-191

Health Information Technology for Economic and Clinical Health Act [46] (HITECH), (part of the American Recovery and Reinvestment Act of 2009, Public Law 111-5)

Omnibus Rule [40], 78 Federal Register 5566 (January 25, 2013)

Regulation Text [37] – (45 CFR Parts 160, 162, and 164, the HIPAA rules) Unofficial Version as amended through March 26, 2013 (NOTE: The 50 Titles of the Code of Federal Regulations (CFRs) are updated annually by the Government Printing Office [47] on a staggered basis. Title 45, which includes the HIPAA rules, is scheduled for revision on October 1 of each year.)


HHS/OCR Information by Topic

Data Breach Notification [3]
Disposal of Protected Health Information [49]
Health Information Technology [18]
Notice of Privacy Practices [50]
Right to File a Complaint [51]
Safeguards [52]
Security Rule FAQ [53]
HIPAA Enforcement

[54]

Government Publications and Resources


Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule [57], HHS/OCR

Guide to Privacy and Security of Health Information [58], Office of the National Coordinator for Health Information Technology

OCR Reports on the Enforcement of the HIPAA Rules [59], Health Care Compliance Association, April 22, 2013

FDA Should Expand Its Consideration of Information Security for Certain Types of Devices [33], Government Accountability Office (GAO), August 2012

Medical Identity Theft: FAQs for Health Care Providers and Health Plans [60], Federal Trade Commission

Health Privacy [44], Federal Trade Commission

Studies, Reports and Other Publications

More Changes in Health Care Needed to Fulfill Promise of Health Information Technology [61], Rand Corporation, January 7, 2013

Third Annual Benchmark Study on Patient Privacy and Data Security [62], Ponemon Institute, December 2012

Annual Report to Congress on HIPAA Privacy Rule and Security Rule Compliance, For Calendar Years 2009 and 2010 [63], HHS

2011 Survey of Patient Privacy Breaches [64], Veriphyr

2012 HIMSS Analytics Report: Security of Patient Data, commissioned by Kroll Advisory Solutions [65], April 2012

Medical Identity Theft Information Page [31], World Privacy Forum

Other Medical Privacy Resources

Health Information and the Law [67], George Washington University

State Medical Boards [68], American Medical Association

Links
[5] https://www.privacyrights.org/Medical-Privacy
[6] https://www.privacyrights.org/content/health-privacy-hipaa-basics#HHS-enforce-hipaa