COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual 2024
Patient Privacy and Security: Protected Health Information

By Connie Barrera, [1] MBA, CISSP, CISA

What Is Protected Health Information?

The risk area involving patient privacy, security, and protected health information (PHI) is greater than ever. This is, in no small part, due to the adoption of electronic health record (EHR) solutions, which brought exceptional opportunities for adversaries to compromise large quantities of patient data from anywhere in the world. In addition, the traditional internal threat actor risk also grew. Now, instead of having to take huge stacks of paper patient records, anyone with the right access but the wrong motivation can steal large quantities of patient data. Even the unfortunate, user error–based/nonmalicious breach became much more serious once patient records went electronic.

PHI under U.S. laws includes any health-related information that can be linked back to a specific individual. If the information is maintained electronically, it would be referred to as electronic protected health information (ePHI). The Health Insurance Portability and Accountability Act (HIPAA) identifies the following 18 data elements that must be safeguarded in order to ensure patient privacy:

1. Names
2. Dates (except year)
3. Telephone numbers
4. Geographic data
5. Fax numbers
6. Social Security numbers
7. Email addresses
8. Medical record numbers
9. Account numbers
10. Health plan beneficiary numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plates
13. Web addresses
14. Device identifiers and serial numbers
15. Internet protocol (IP) addresses

16. Full face photos and comparable images
17. Biometric identifiers (e.g., retinal scan, fingerprints)
18. Any unique identifying number or code[2]

A process of continual vigilance must be put in place to prevent disclosure of PHI (whether on paper or stored electronically). With the extensive spectrum of data elements on every patient, it's no wonder that healthcare organizations are constantly being attacked by external hackers or exploited by malicious insiders. Malicious insiders will sell the data to make some money, causing damage to each individual whose data will be used for identity theft or other related fraud. Hackers will extract data from health organizations and typically sell the data on the dark web. The breach itself is certainly serious, but industry metrics show that an organization may not realize it has been breached for nine to 18 months. Following the breach, forensically identifying the scope and magnitude of the breach will be difficult and certainly very costly.

In addition to the adversaries mentioned, avoidable breaches continue to occur despite everyone knowing the key issues. Despite a plethora of technical controls available for many years, the announcements of lost or stolen devices with unsecured data continues to be common and often. Other threat vectors to patient privacy include, but are not limited to, weak passwords, unsecured email, unauthorized cloud storage, and USB devices. It's important to point out that all of the traditional paper-based risks still exists, and so more than ever it is vital that every organization ensure it identifies and measures risk on a yearly basis.

Having a compliance program that continually addresses and mitigates threats will greatly help to reduce the risk of data compromise. While some risks may be common to all or most organizations, providers cannot leverage a cookie-cutter approach. Even when two providers or health systems have similar software, depending on the specifics of the technical configuration, business process, and access roles that users are granted, it could yield drastically different risk profiles for each organization. Therefore, deliberate and thorough analysis of threats versus administrative, technical, and physical controls is the essential first step in safeguarding patient privacy and mitigating potential breaches.

Risk Area Governance

HIPAA Privacy Rule, 45 C.F.R. §§ 160, 164.500–164.534

This rule was promulgated to establish global standards and protect the privacy of personal health information.[3]

HIPAA Security Rule, 45 C.F.R. §§ 160, 164.302-§164.318

This rule was promulgated to establish standards aimed to protect electronic health data. The security rules establish administrative, physician, and technical safeguards that are required for compliance.[4]

Health Information Technology for Economic and Clinical Health (HITECH) Act

HITECH was part of the American Recovery and Reinvestment Act, which provided financial incentives amounting to billions of dollars for health systems to implement and meaningfully use health information technology (IT) solutions.[5]

Meaningful Use, 42 C.F.R. §§ 412, 413, 422, 495

These sections of the HITECH Act established requirements for incentive-based payments for the adoption of health IT solutions meant to digitize patient records.[6]

State-Based Identity Theft Protection Laws

Every state has legislation regarding identity theft crimes. Certain states have specific provisions for restitution. A few states have even created programs to help victims from continuing identity theft issues, such as Iowa and Ohio.

Identity Theft Rules, 16 C.F.R. § 681

These rules require organizations to establish and maintain adequate controls and training to prevent identity theft.[7]