How to stay **HIPAA compliant** in the digital age

INTIVA HEALTH

2020

Excutive summary

The accelerated advancement of technology is rapidly shaping the way people communicate in their daily lives and conduct business across all industry sectors, especially healthcare. The digital age has created an expectation of immediacy in data delivery and interpersonal communication. While technology has undeniably enabled rapid access and real-time feedback, these developments can also have serious consequences on health care compliance. There are two primary challenges that health care facilities must overcome to maintain compliance and mitigate risk. Common industry practices, such as the use of short messaging services (SMS) or personal electronic devices to transmit protected health information (PHI), opens the door for a temporary lapse in HIPAA compliance resulting in enormous monetary penalties for health care systems. A security breach of a patient's PHI can have life-altering consequences for the individual. To achieve a balance between cybersecurity and provider responsiveness in the health care industry, health care facilities and networks need to adopt solutions that provide confidentiality while maintaining accessibility.

Table of contents

History of HIPAA

Congress passed the Health Insurance Portability and Accountability Act (HIPAA) into law on Oct. 21, 1996. The original legislation was defined as an act in order to amend the Internal Revenue Code of 1986 (https://aspe.hhs.gov/). In passing the legislation, Congress required the establishment of federal guidelines to ensure the security of electronic PHI to guarantee confidentiality, integrity, and availability of health information that maintains security and provides access for health care providers, clearinghouses, and health insurance plans (Edemekong & Haydel 2019).

GOALS OF HIPAA

1. Limit the use of PHI to those with a "need to know"
2. Penalize those who do not comply with confidentiality regulations

HIPAA TIMELINE

- **1996** — HIPAA PASSED
- **2002** — PRIVACY RULE PASSED
- **2003** — SECURITY RULE PASSED
- **2013** — OMNIBUS RULE PASSED

Health care communication technology & HIPAA compliance

When HIPAA first became law, the concepts of the internet, digital technology, and smart devices were not on the minds of those writing the legislation. Throughout the 24 years following its enactment, different rules were passed to address this issue, but technology is advancing at such a rapid pace that breaches are still quite common. While criminal violations of HIPAA involving personal gain exist, the percentage is relatively small. A majority of infringements are temporary lapses that, while unintentional, result in extremely expensive consequences (Edemekong & Haydel 2019). In order to fully comply with HIPAA, it is vital for any health care facility to establish secure methods of clinical documentation and communication.

Technological advancements are undoubtedly elevating the standard of care, yet conversely they make the original intentions of HIPAA harder to enforce. Health care organizations must address security requirements for electronic devices on which PHI is transmitted and received. In many health care systems, devices used for short messaging services (SMS) are personally owned by medical staff. During routine patient care, electronic PHI such as patient names, room numbers, and medical record numbers are often included in SMS texts. Since the devices used to send the text messages are often not owned, configured, or managed by the facility there are a host of security risks such as password requirements, screen locks, and data storage. If a provider loses their cell phone, a device gets stolen, or a doctor texts PHI on their personal electronic device, a violation of HIPAA compliance occurs. In the research conducted by Liu et. al (2019) it was found that between 60% and 80% of clinical staff use texting for clinical care. Further, widespread issues may occur when the medical staff do not share the same perception of risk as their health care organizations. Surveys suggest that at least 30 percent or more of staff incorrectly believes that SMS meets HIPAA security requirements (Liu et. al 2019). Unforeseen or unintended exposure of electronic PHI via insecure SMS on portable electronic devices puts health care facilities and organizations at risk for monetary penalties, as well as creates a direct risk to patient privacy (Drolet et. al 2017). Potential violations are not limited to portable electronic devices. It is common for health care workers to use their home computer or laptop to access patient information. This could result in a HIPAA violation if one of their family members uses the computer or information is left on an unlocked screen. Such mistakes can carry tremendous financial penalties, with fines ranging up to $1.5 million (Edemekong & Haydel 2019).

WHY HACKERS TARGET HEALTH CARE

Health care Cybersecurity and HIPAA Compliance

Breaches include theft of PHI and ransomware attacks on health care facilities (Coventry & Branley 2018). The consequences of a cyberattack include a lack of patient trust and lapses in HIPAA compliance, often resulting in massive fines. The value of health care data and PHI to unauthorized users or hackers is primarily targeted toward identity theft (Murphy 2015). A recent U.S. government interagency report indicated that, on average, there have been 4,000 daily ransomware attacks since early 2016. This is a 300% increase over the 1,000 daily ransomware attacks reported in 2015 (http://www.justice.gov). The HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware (https://www.hhs.gov). However, it should be noted that the legislation does not specify solutions. HIPAA only lays out requirements for health care entities to take the necessary steps to prevent any security breaches that could impact a patient's PHI (Murphy 2015).

Effective implementation of cybersecurity measures in the health care space is a complex balancing act. In his National Cyber Security Institute Journal article, Murphy states: "In a world where confidentiality, integrity, and availability are the tenets of cybersecurity, healthcare is different in that these are not equivalent concerns. Availability may be the most important of the three. Stated in another way, cybersecurity professionals in healthcare may find themselves in the uneasy position of flexing on confidentiality controls in favor of increase availability" (pg. 49-50). There clearly exists

Impact of Data Breaches on Health Care Systems, Individuals

The consequences of a security breach that impacts a patient's PHI can be extensive. Nearly one-third of the United States population was impacted by PHI data breaches in 2015, and during the last three years nearly 43% of all data breaches were attributed to the health care industry (Koch 2016). In her Journal of Health Care Finance article, Koch describes to what extent these breaches can have a massive economic impact on hospitals, health care systems, and individuals. Cyberattacks cost health care systems in the United States an average of $6 billion per year and an average data breach costs an individual hospital $2.1 million (Koch 2016). However, the negative impacts do not stop at the facility or system. Without proper PHI security, a person's financial and personal reputation can be impacted. Aside from unauthorized access to bank accounts, credit card information, and fraudulent loan applications, medical care could also be falsely obtained under the victim's identity. According to the Medical Identity Fraud Alliance, 65% of medical identity theft victims paid more than $13,000 each to resolve their issue. On top of financial burdens, victims face life-changing, negative impacts to their medical record. Consequences include incorrect pre-existing conditions, child custody disputes, denial of medical care, loss of insurance benefits, and more (Koch 2016). If a health care facility, network, or provider does not have sufficient protection and security in the event of a cyberattack or compliance breach, their reputation, finances, and future are all in jeopardy.

Intiva Health HIPAA Breach Insurance Marketplace

The Intiva Marketplace offers users a convenient method of purchasing medical malpractice insurance, HIPAA breach insurance, and cyber risk insurance. Intiva Health holds agreements with several key healthcare industry partners to bring critical tools and resources to licensed medical providers across the United States. These partners, among others, include professional liability companies such as Arthur J. Gallagher and Cooperative of American Physicians. Intiva Health has partnered with Lloyd's of London to bring an entire quote and binding service online. Intiva Health offers some of the market's most affordable cyber insurance, starting at $250,000 in coverage.

FINES, PENALTIES & LEGAL

We'll provide coverage for legal defense, insuring you against regulatory claims and any fines and penalties that result from an alleged data breach.

SECURITY BREACH RESPONSE

Get reimbursed for the costs of a security breach. Be it hiring PR agents to protect your brand or credit monitoring for affected parties.

PRIVACY LIABILITY COVERAGE

More than the average policy, we protect your rights to privacy and cover everything from corporate data risk to business interruption, cyber extortion, and more.

PROPERTY DAMAGE & BUSINESS INTERRUPTION

Assure coverage for lost earnings and expenses from a security compromise, restoration of disrupted digital assets, and computer systems, for both personal and third-party systems.

24-HOUR SUPPORT LINE

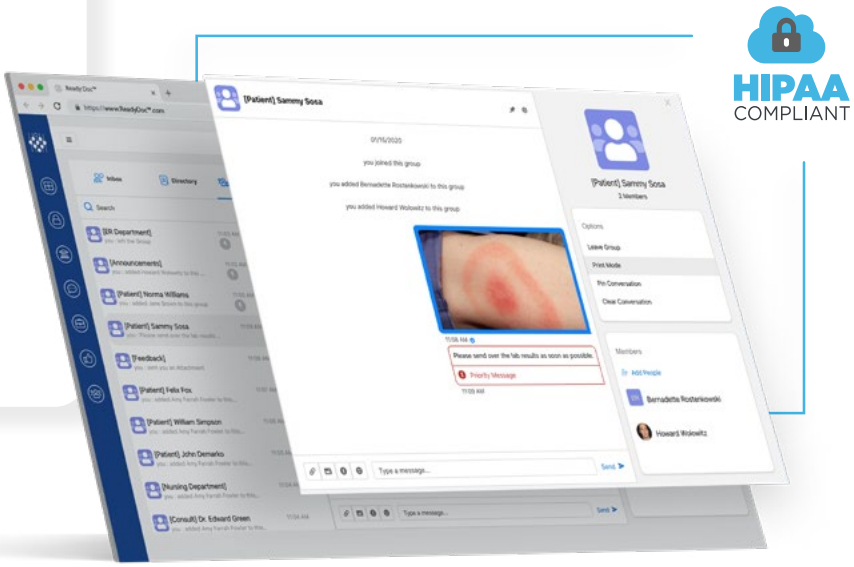
Get round-the-clock assistance from privacy law firm experts on data breach events, incident reports, or notice of claims.

Based on recent history, the need for secure technological systems in health care is indisputable. The digital age will continue to provide positive advancements for the industry, and with that will come challenges for health care systems and providers to maintain secure, HIPAA-compliant systems for clinical communication and documentation.

Ready Doc™ Messaging: A HIPAA-Compliant Communication Solution

Ready Doc™ Messaging is an easy-to-use messaging app for smartphones or workstations that helps organizations improve health care team communication and collaboration while achieving HIPAA-compliance. The application's secure and encrypted application protects patient information and meets HIPAA guidelines to reduce the risk of fines. You can manage digital PHI correspondence and streamline care team coordination via one accessible, user-friendly platform. Ready Doc™ Messaging lets you access and share patient records, submit lab orders, and connect with other providers worry-free of any HIPAA violations. The platform helps you save time and improve communication efficiency by alleviating multiple phone calls, unanswered texts, and disruption to patients and care team members. You are able to maintain full control with the administrative console for managing users and devices, allowing setting and enforcing of security policies, and enhancing workflows with other departments for consults, transfers, medication reconciliation, and more. The end result is a consolidation of procedures by integrating your entire network directory.

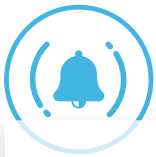
- PROTECT PATIENT INFORMATION
- IMPROVE WORKFLOWS
- COMPLY WITH INDUSTRY REGULATIONS



Ready Doc™ Messaging features

SECURE MESSAGING

Keep messages private with a fully encrypted, end-to-end, secure texting solution.



PRIORITY MESSAGING

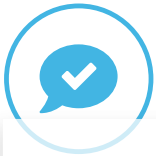
Send high-priority messages that stay at the top of the recipient's inbox and specify a unique alert for instant differentiation.

MESSAGE FORWARD

Have messages automatically forwarded to another colleague.

CUSTOM GROUPS

Have open and ongoing forum discussions with colleagues on specific topics. Join or leave a forum anytime.



DELIVERY CONFIRMATION

Know instantly when messages have been sent, delivered, and read.

MESSAGE LIFESPAN

Set message lifespan to dictate when messages will be automatically expunged.

MESSAGE RECALL

Recall a message and attachments before or after it has been read.

GROUP MESSAGING

Create groups to improve collaboration and see who has read your message and when.

SECURE ATTACHMENTS

Securely attach any type of photo, image, video, audio, X-ray, CT scan, or MRI directly to the conversation in real-time.

Ready Doc™
BY INTIVA HEALTH

To learn how Ready Doc™ can help your facility,
visit IntivaHealth.com or email ReadyDoc@intivahealth.com.

APPENDIX

HIPAA Titles

HIPAA consists of five titles which categorize the safeguards provided by the legislation:

Title I: Protects health insurance coverage for workers and their families that change or lose their jobs. It limits new health plans the ability to deny coverage due to a pre-existing condition.

Title II: Prevents Health Care Fraud and Abuse; Medical Liability Reform; and Administrative Simplification that requires the establishment of national standards for electronic health care transactions and national identifiers for providers, employers, and health insurance plans.
Title III: Guidelines for pre-tax medical spending accounts. It provides changes to health insurance law and deductions for medical insurance.
Title IV: Guidelines for group health plans. It provides modifications for health coverage.
Title V: Governs company-owned life insurance policies. It makes provisions for treating people without United States Citizenship and repealed financial institution rule to interest allocation rules (Edemekong & Haydel 2019).

HIPAA Rules

HIPAA included Administrative Simplification Rules in Sections 261 through 264 that required The Department of Health and Human Services (DHHS) to publicize standards for the electronic exchange, privacy and security of health information if Congress did not enact privacy legislation within three years of the passage of HIPAA.
No legislation was enacted and DHHS developed what came to be known as The Privacy Rule, which was first published on Dec. 28, 2000 and later modified in August of 2002. It focused on the rights of the individual and their ability to control their PHI. The DHHS published a final Security Rule in February of 2003. The second rule set national standards for protecting the confidentiality, integrity, and availability of electronic PHI.

The Security Rule and The Privacy Rule apply to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of DHHS has adopted standards under HIPAA (the "covered entities") and to their business associates (https://www.hhs.gov).

The Office of Civil Rights (OCR) within the Department of Health and Human Services (DHSS) oversees and enforces the Privacy Rule and Security Rule. Compliance with the Security Rule was required as of April 20, 2005 and April 20, 2006 for small health plans. The Enforcement Rule provides standards for the enforcement of all the Administrative Simplification Rules. The Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology.

HITECH stimulated the adoption of electronic health records (EHR) by offering incentives to medical groups that proved "effective" implementation of EHR technology. Another section of the HITECH Act also strengthened regulations for the Privacy and Security Rules of HIPAA. In doing so, HITECH added more technical requirements to hospitals and doctors who use electronic health records. HITECH provisions enhance the HIPAA regulations aimed directly at business associates. In essence, HITECH was primarily enacted to expand on HIPAA compliance notifications. Providers are now required to report a significant breach of information to the government and affected individuals. Patients, in turn, can request access to that information at any time.

HITECH's enactment directly strengthened prior HIPAA regulations regarding business administrative and carrier liabilities. HITECH addressed some of the gaps in the Privacy Rule's protections and in turn may help build public trust in the new environment of increased digitization of health information. As the product of two statutes, the Omnibus Rule, enacted in 2013 to update the HITECH Act, produced a new landscape for health information. The Omnibus Rule makes businesses directly liable for their covered entity, showcasing a push to strengthen patients' rights to have more control over their own data, including the right to restrict disclosure of PHI for purposes of carrying out payment or health care operations (Goldstein & Pewen 2013).

These last updates, especially those regarding HITECH, not only expand carrier and provider's sanctions to include criminal charges but allow for fines to climb up past the millions. This makes it imperative for providers to have a clear sense of compliance regulation, which can be the difference between a small mistake and a career-ending event.

Protected Health Information

Individually Identifiable Information: Includes many common identifiers such as Social Security Number, name, address, and date of birth. It also includes demographic data that relates to:

- Past, present, or future health conditions.
- Provision of health care
- Past, present, or future payment for the provision of health care to the individual
- Information that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual

Permitted Uses and Disclosures of Health Information

To the individual: A covered entity may disclose protected health information to the individual who is the subject of the information.

Treatment, Payment, Health Care Operations:
A covered entity may use and disclose PHI for its own treatment, payment, and health care operations activities. Uses and Disclosures with Opportunity to Agree or Object: Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual.

Public Interest and Benefit Activities:
The Privacy Rule permits the use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes. These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of health information outside of the health care context:

1. Required by law
2. Public health activities
3. Victims of abuse, neglect or domestic violence
4. Health oversight activities
5. Judicial and administrative proceedings
6. Law enforcement purposes
7. Decedents
8. Cadaveric organ, eye, or tissue donation
9. Research
10. Serious threat to health or safety
11. Essential government functions
12. Workers' compensation

Most Common Alleged Noncompliance Issues

- Impermissible uses and disclosures of protected health information
- Lack of safeguards of protected health information
- Lack of patient access to their PHI
- Lack of administrative safeguards of electronic PHI
- Use or disclosure of more than the minimum necessary PHI

Most common types of covered entities alleged to have committed violations

- Hospitals
- Private practices
- Physicians
- Outpatient facilities
- Pharmacies
- Health Plans (group health plans and health insurance issuers)

References

Cohen IG, Mello MM. HIPAA and Protecting Health Information in the 21st Century. Journal of American Medical Association. 2018;320(3):231–232. doi:10.1001/jama.2018.5630.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48–52. doi: 10.1016/j.maturitas.2018.04.008

Drolet B C, Marwaha J. S., Hyatt B., Blazar P. E., Lifchez S. D. Electronic communication of protected health information: privacy, security, and HIPAA compliance. Journal of Hand Surgery: American Volume. 2017;42(06):411–416.

Edemekong P.F. & Haydel M.J. Health Insurance Portability and Accountability Act (HIPAA) [Updated 2019 Jun 18]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2020 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK500019/

Goldstein, M. M., & Pewen, W. F. (2013). The HIPAA Omnibus Rule: implications for public health policy and practice. Public health reports (Washington, D.C. : 1974), 128(6), 554–558. doi:10.1177/003335491312800615.

"Health Insurance Portability and Accountability Act of 1996". Retrieved from https://aspe.hhs.gov/report/health-insurance-portability and-accountability-act-q 1996. Accessed on: Jan. 29, 2020.

"Health Information Privacy." Retrieved from: https://www.hhs.gov/hipaa/index.html. Accessed on: Jan. 29, 2020.

"Health information privacy beyond HIPAA: a 2018 environmental scan of major trends and challenges". National Committee on Vital and Health Statistics. Retrieved from: https://www.ncvhs.hhs.gov/wp-content/uploads/2018/02/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf. Accessed on January 30, 2020.

Koch, D. D. (2016). Is the HIPAA Security Rule Enough to Protect Electronic Personal Health Information (PHI) in the Cyber Age? Journal of Health Care Finance, 43(3), 2–27. Retrieved from: http://healthfinancejournal.com/~junland/index.php/johcf/article/view/67. Accessed on January 30, 2020.

Liu X, Sutton PR, McKenna R, Sinanan MN, Fellner BJ, Leu MG, Ewell C. "Evaluation of Secure Messaging Applications for a Health Care System: A Case Study. Applied Clinical Informatics. 2019 Jan;10(1):140-150.

Murphy, Sean. "Is Cybersecurity Possible in Healthcare?" National Cybersecurity Institute Journal. 2015.;1(3):49-62. http://publications.excelsior.edu/publications/NCI_Journal/1-3/offline/download.pdf.

Piya M. Gasper. The Impact of Federal Regulations on Health Care Operations, 19 Annals Health L. 249 (2010).

United States Government Interagency Guidance Document. How to Protect Your Networks from Ransomware. Retrieved from: https://www.justice.gov/criminal-ccips/file/872771/download. Accessed on: February 11, 2020.

INTIVA HEALTH

Ready Doc™
BY INTIVA HEALTH

intivahealth.com