



What HIPAA Is and What It's Not

■ ALAN A. AYERS, MBA, MAcc

Urgent message: While many people perceive HIPAA as a law governing patient privacy, protection and standards for personal health information is only one aspect of this law, which was originally intended to regulate health insurance.

Introduction

Ask anyone—even the owner of an urgent care center—what HIPAA is, and they'll most likely tell you it's all about patient privacy. While the Health Insurance Portability and Accountability Act did establish national standards for the protection of individuals' medical records and other personal health information,¹ there are other aspects of the law—and many misconceptions that have created confusion for those in the healthcare industry.

This article will examine the true purposes of the law and what this historic legislation—as much concerned with insurance as privacy—entails, and why understanding HIPAA is important for urgent care center owners.

HIPAA—Not What You Think It Is

HIPAA was signed into law on August 21, 1996, with a stated purpose to:

“...improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.”²

Note that the first part of the statement is to provide “portability and accountability of health insurance coverage for employees between jobs.”³ Because of this mandate, the industry

simplified the administration of health insurance, which encouraged the digitization of patient health records. Computerization of patients' medical records, in turn, made it necessary to safeguard the security of that data in digital format.⁴

The other objectives of the Act were to promote the use of medical savings accounts (MSAs) by introducing tax breaks, provide coverage for employees with preexisting medical conditions, and simplify health insurance administration.⁴

Focus on Insurance

A primary concern addressed in HIPAA was ensuring that individuals would be able to maintain their health insurance between jobs. The relatively straightforward health insurance portability portion of the Act has been implemented successfully.⁵

For example, HIPAA precludes a group health plan insurer from enforcing an exclusion of preexisting medical conditions.⁵ One U.S. circuit court has explained that the effect of HIPAA in that situation is to increase the relative cost of the plan by compelling continued healthcare coverage for employees who are likely to incur greater-than-average healthcare expenses.⁶

A Louisiana federal district court held that to avoid a break in insurance coverage, an employee must apply to the state HIPAA pool within 63 days of the day group coverage ended. The court went on to explain that HIPAA requires that when an employee moves to a new job, her subsequent employer or health plan must give her “credit” for having held that prior continuous coverage.⁷ If an employee was provided insurance coverage by the previous employer or health plan for the requisite period of time with no gap in coverage of more than 63 days, the employee must be eligible for insurance from the new employer, regardless of any preexisting condition.⁷

Likewise, HIPAA prohibits group health plans and insurers offering coverage through group health plans from charging different premiums or contributions to “similarly situated individuals on account of any health status-related factor in relation to the individual[s]....”⁸

Application to Urgent Care Operators

It's important for urgent care operators to remember that



Alan A. Ayers, MBA, MAcc is Vice President of Strategic Initiatives for Practice Velocity, LLC and is Practice Management Editor of *The Journal of Urgent Care Medicine*.

HIPAA is not a general medical privacy law. While complicated and confusing in some aspects, the Act provides protections to individuals in certain contexts—primarily where protected health information (PHI) originates with or flows through a HIPAA “covered entity,” such as a healthcare provider or urgent care center. It applies to certain entities in certain situations only for certain information. Of these, patient consent is one of the areas most misconstrued by urgent care facilities

TPO Purposes in HIPAA. HIPAA provides for patient consent by assumption for certain categories of use and disclosure. The “assumption” is that there are certain kinds of uses and disclosures of patient information that are essential to the operation of the healthcare system. Collectively, these are known as **TPO** (**T**reatment, **P**ayment for healthcare services, and healthcare **O**perations or administration).

The uses and disclosures that fit under TPO require no action. These disclosures make up a vast majority of the information use in the healthcare system.

Public Priority Purposes. These categories of disclosures make patient consent, in effect, irrelevant and unnecessary. These include public health disclosures, enforcement investigations, certain research, law enforcement, judicial and administrative proceedings, and several other purposes where there’s a public goal served by the disclosure—independent of patient consent.⁹ These disclosures can be made without patient consent.

Patient Authorization. Aside from TPO and public priority purposes, disclosure can only be made with patient authorization, which is a specifically defined document executed by a patient in a particular situation.¹⁰ With this, a patient can “authorize” any use or disclosure of his information.

In addition to these notions of consent, the “minimum necessary” principle provides a blanket for most uses and disclosures. This means that an entity subject to HIPAA—even when a use or disclosure is permitted—is to disclose the “minimum necessary” information needed to perform the particular function.¹² It must make “reasonable efforts” to limit the use, disclosure, or request of protected health information to what’s minimally necessary.¹¹

Experts say that this isn’t a hard-and-fast rule, so urgent care center owners need not spend an inordinate amount of time and effort analyzing each disclosure. However, an owner should draft a set of general principles concerning how an urgent care determines what the “minimum necessary” information to be disclosed actually is. Employees will then need to be trained on these principles.

The HIPAA Privacy Rule. Under this rule, there’s a requirement to develop specific administrative procedures to ensure compliance with HIPAA. To make this feasible, the U.S. Department of Health and Human Services developed a “flexible” approach to compliance by making the requirements “scalable” based on the characteristics of an organization.¹²

“Urgent care centers will provide better care by applying the true prerequisites and not using valuable resources based on fallacies and misunderstandings of HIPAA.”

Misconceptions

With all the rules created by HIPAA, there are some broad and overreaching misconceptions that have confused and hampered urgent care business owners in the effective operation of their centers in attempting to comply with the Act. Here are four common inaccuracies:

- **Unnecessary Business Associate Agreements.** HIPAA requires urgent care centers to have written agreements called business associate agreements (BAAs) with other entities that receive or work with their PHI. The agreements say that the business associates will appropriately safeguard the information.¹³ However, some facilities take unneeded precautions with BAAs and have everyone sign a BAA—though there’s no need to make your cleaning service sign a BAA, for one, because they don’t fall into the definition of a business associate. They’re not interacting with PHI.
- **Unnecessary Patient Authorizations.** Many urgent care centers require a patient authorization prior to transferring patient information to another provider for treatment purposes. Although it’s important to comply with HIPAA’s requirements concerning access to PHI—because it’s covered under TPO purposes¹⁴—there’s no need to get authorization. This misunderstanding results in delays and confusion, as well as added stress between the patient and the provider. Again, if access is specifically necessary for treatment purposes, an urgent care center doesn’t need a patient authorization.
- **HIPAA Cancels Out All Other State and Federal Privacy Laws.** This is not accurate. There are many other patient laws that apply to the privacy of medical data for HIV, mental health, substance abuse, sexual assault, domestic abuse, and the medical treatment of minors. Although HIPAA’s privacy rules supersede many of the laws that are on the books in specific states, some state laws are still important in specific scenarios. Remember that HIPAA covers only *digital* medical information—not PHI that’s oral or written. A state’s medical privacy laws would most likely still cover PHI in hard copy. In addition, there are some state medical privacy laws that are more stringent than HIPAA, so those

rules must also be consulted to get a full picture of medical privacy laws in a specific state.

- **HIPAA's Privacy Laws Apply to Industries Outside of Healthcare.** While many industries are heavily regulated, HIPAA isn't applicable to hotels, retail stores, airlines, or veterinary clinics. None of these fit the HIPAA definition of a "covered entity." Remember, HIPAA's Privacy Rule covers health plans, healthcare clearinghouses, and healthcare providers.¹⁵

Conclusion

Contrary to some beliefs, HIPAA hasn't created a momentous change in the way healthcare is provided in the U.S.

Although it's complex, the law has been fashioned to meet the reality of medical practice. Compliance with its requirements is aided greatly by understanding what the Act truly means and separating fact from fiction. Urgent care centers will provide better care to their patients by applying the true prerequisites and not using valuable resources based on fallacies and misunderstandings of the law. ■

References

1. Rich MJ. Health information and privacy interests in the 21st century. 20 *Delaware Lawyer* 6 (Summer 2002).
 2. Pub. L. No. 104-191, 110 Stat. 1936.

3. *MacArthur v. San Juan County*, 416 F. Supp. 2d 1098, 1191 (D. Utah June 13, 2005).
 Davis KB. Davis, *Privacy Rights in Personal Information: HIPAA and the Privacy Gap Between Fundamental Privacy Rights and Medical Information*, 19 J. Marshall J. Computer & Info. L. 535, 536 (2001).
 4. HIPAA history. *HIPAA Journal*. Available at: <http://www.hipaajournal.com/hipaa-history/>. Accessed November 7, 2017.
 5. 29 U.S.C. § 1181(a)(3), (c)(1); 29 U.S.C. § 1182(b)(2)(A).
 6. *Werdehausen v Benicorp Ins. Co.*, 487 F.3d 660 (8th Cir. Mo. 2007).
 7. *Bitter v. Orthotic & Prosthetic Specialists, Inc.*, 2005 U.S. Dist. LEXIS 17818, 14-15 (E.D. La. Aug. 17, 2005); *Negley v. Breads of the World Med. Plan*, 2003 U.S. Dist. LEXIS 14006 (D. Colo. Aug. 1, 2003).
 8. 29 U.S.C. § 1182(b)(1).
 9. Stevens GM. *A brief summary of the medical privacy rule*. Congressional Research Service, Library of Congress (February 2003), at 5. Available at: <https://epic.org/privacy/medical/RS20934.pdf>. Accessed November 7, 2017.
 10. Annas GJ. HIPAA regulations—a new era of medical-record privacy? *N Engl J Med*. 2003;348:1486-1490.
 11. Guthrie J. Time is running out—the burdens and challenges of HIPAA compliance: a look at preemption analysis, the minimum necessary standard, and the notice of privacy practices. *Ann Health Law*. 2003;12(1):1143-1177.
 12. U.S. Department of Health and Human Services. *Summary of the HIPAA Security Rule*. Available at: <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>. Accessed November 7, 2017.
 13. U.S. Department of Health and Human Services. *Business Associates*. Available at: <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>.
 14. Bush J. The HIPAA privacy rule: three key forms. Complying with the HIPAA privacy rule may seem trickier than pulling a rabbit out of a hat, but these forms should help. *Fam Pract Manag*. 2003;10(2):29-31.
 15. U.S. Department of Health and Human Services. *Who must comply with HIPAA privacy standards?* Available at: <https://www.hhs.gov/hipaa/for-professionals/faq/190/who-must-comply-with-hipaa-privacy-standards/index.html>. Accessed November 7, 2017.



VisualDx is your trusted second opinion.

Features include:

- ✓ Fast access to insights from the best specialists
- ✓ Handle complex cases directly
- ✓ Engage patients with our handouts

20% OFF
 for JUCM readers
visualdx.com/jucm

