HIPAA for Urgent Care Centers: A Primer

Urgent message: This article discusses potential penalties for violations of HIPAA and key steps urgent care centers should take in order to avoid such penalties.

BART WALKER and MEGGAN BUSHEE

Complying with the Health Insurance Portability and Accountability Act (HIPAA) can be a daunting challenge for smaller providers. As the urgent care industry grows, its providers will become much more visible targets for scrutiny by the federal government with respect to HIPAA compliance. In addition, the high-volume, retail-facing, walk-in nature of urgent care provides greater exposure to the public, who are increasingly learning that HIPAA exists and prone to make allegations.

In general, HIPAA governs: (1) when providers may use or disclose a patient's health information (known as "protected health information" or PHI under HIPAA); (2) to whom PHI may be disclosed; and (3) for what purpose PHI may be used or disclosed. Most states also have their own laws regulating the privacy of patient health information. HIPAA compliance is monitored and enforced by the Secretary of the Department of Health and Human Services (HHS).

Penalties for HIPAA Violations

Penalties for violations of HIPAA can be severe. For example, on February 24, 2013, Massachusetts General Hospital entered into a $1 million settlement with HHS following a patient's complaint about the hospital's loss of documents containing the PHI of approximately 192 patients that were left on the subway by an employee. On September 17, 2012, Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. entered into a 1.5 million settlement with HHS following their self-disclosure of a stolen laptop that contained the PHI of approximately 3,500 patients.

HIPAA applies to all "covered entities" and their "business associates" (and all subcontractors of business associates). Because they provide health care, urgent care centers are considered "covered entities" under HIPAA. Management and billing companies that work with urgent care providers are usually deemed to be "business associates" of the urgent care providers for purposes of HIPAA.

HIPAA violations are usually discovered due to a complaint, often by a disgruntled patient, a former

Bart Walker is a partner in the Charlotte, North Carolina office of McGuireWoods LLP. **Meggan Bushee** is an associate in the Charlotte, North Carolina office of McGuireWoods LLP. Both attorneys are in the firm's health care group.

Table 1. Four-tier Civil Penalty System for HIPAA Violations		
Civil Penalties		
Tier 1	***Unknowing*** **-** Covered Entity or Business Associate did not know and, by exercising reasonable diligence, would not have known that the violation occurred.	$100-$50,000 per violation/$1.5M cap
Tier 2	***Reasonable Cause*** **-** Covered Entity or Business Associate knew, or by exercising reasonable diligence would have known, that the violation occurred, but did not act with willful neglect.	$1,000-$50,000 per violation/$1.5M cap
Tier 3	***Willful Neglect*** **-** It is established that the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the Covered Entity or Business Associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred.	$10,000-$50,000 per violation/$1.5M cap
Tier 4	***Uncorrected Willful Neglect*** **-** it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the Covered Entity or Business Associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred.	At least $50,000 per violation/$1.5M cap

employee, self-disclosure of a breach by the provider, or an audit, all of which can lead to an investigation by the Secretary of HHS. The Secretary can impose civil penalties ranging from $100 to $50,000 per violation, with a $1.5 million cap for aggregate violations of the same HIPAA provision in a single calendar year. The amount of the civil penalty largely depends upon the level of culpability associated with the violations as established by a four-tiered civil penalty system set forth in **Table 1**, although several of the more recent settlements with HHS have been for the maximum civil penalty amount.

Both large and small providers have been subject to recent investigations by the Secretary, evidencing the importance of a thorough compliance plan regardless of the size of the provider. For example, on April 17, 2012, Phoenix Cardiac Surgery, PC, a five-physician practice, entered into a settlement with HHS for $100,000, a significant penalty for a very small provider. The HHS investigation of the practice was triggered by an anonymous complaint that the practice was posting patient appointment information on a publicly accessible Internet-based calendar.

In addition to the civil monetary penalties outlined in **Table 2**, a provider may be required to notify local prominent media outlets after more extensive breaches, in addition to the notification of HHS and all affected individuals that is required for all breaches. Although rare, HIPAA violations can also result in criminal penalties of up to $250,000 and up to 10 years imprisonment.

Steps for Urgent Care Centers to Comply with HIPAA and Avoid Penalties

1. Implement Privacy and Security Policies and Procedures

The first step an urgent care center should take in order to comply with the often complex requirements of HIPAA is to have formal policies and procedures in place that govern the privacy and security of patient PHI and set forth a process for investigating any breach and mitigating any harm resulting from a breach. HIPAA policies and procedures generally are divided into two pieces: (1) privacy policies and procedures that comply with the HIPAA Privacy Rule, which focuses on the right of an individual to control the use and disclosure of his or her PHI; and (2) security policies and procedures that comply with the HIPAA Security Rule, which focuses on administrative, technical, and physical safeguards of electronic PHI (ePHI). In connection with creating security policies and procedures, the provider must perform a comprehensive risk assessment of its storage and transmission of ePHI. The risk assessment should assist the provider in developing safeguards for hardware and portable devices that contain ePHI. It is particularly important that the security policies strictly regulate the removal of portable devices containing PHI from the urgent care center, as well as the use of e-mail for the transmission of PHI.

Table 2. Four Factors for Risk Assessment

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

PHI = protected health information

Providers often engage a consulting firm to perform the initial risk assessment and assist with the implementation of security policies and procedures.

While an urgent care center may have existing policies in place, significant revisions to such policies will likely need to be made to reflect the changes to HIPAA under the Omnibus Final Rule that was published January 25, 2013. Urgent care centers should have made all revisions required by the Omnibus Final Rule's compliance deadline of September 23, 2013.

2. Appoint Privacy and Security Officers

An urgent care center is required to designate a privacy officer and a security officer (which is permitted to be the same individual), who will be tasked with overseeing the implementation of the center's privacy and security policies and procedures and various other obligations.

3. Training Employees

Once an urgent care center has developed a complete set of privacy and security policies and procedures, the next step toward HIPAA compliance is to train all employees and staff members on those policies and procedures. Simply maintaining a copy of privacy and security policies will not satisfy HHS in the event of an investigation. During investigations, HHS fre-

quently requests copies of training logs evidencing employee training on the provider's HIPAA policies and procedures. All new employees must be trained on those privacy and security policies that are relevant to the employees' job duties. In addition, existing employees must receive additional training on any changes made to the policies and procedures, such as those changes resulting from the Omnibus Final Rule, if the changes will affect the employee's job duties. Training sessions do not have to be extremely formal and can be as simple as providing training at an already scheduled staff meeting.

"An urgent care center should evaluate all of its business relationships to ensure that it has a BAA in place with any entity that creates, receives, maintains, or transmits PHI on behalf of the urgent care center."

4. Enter Into Business Associate Agreements (Where Necessary)

HIPAA requires covered entities such as urgent care centers to enter into written, signed business associate agreements (BAAs) with all entities considered "business associates" under HIPAA. Although a covered entity is not required under HIPAA to ensure that its business associates are compliant with HIPAA and it is not directly liable for a business associate's violation of HIPAA if an appropriate BAA is in place, a covered entity should still be selective with its business relationships. An urgent care center should evaluate all of its business relationships to ensure that it has a BAA in place with any entity that creates, receives, maintains, or transmits PHI on behalf of the urgent care center. This definition of business associate was recently expanded by the Omnibus Final Rule and may require urgent care centers to enter into BAAs with entities that were not previously deemed business associates under HIPAA. Existing BAAs will need to be revised or replaced to reflect certain changes under the Omnibus Final Rule. Form BAAs are generally available, although urgent care centers should ensure that the form they are using is drafted so as to favor the covered entity (and in compliance with their policies and procedures).

5. Prepare Notice of Privacy Practices

Each urgent care center must maintain a current notice of privacy practices (NPP) that it provides to every patient prior to or on the patient's first date of service at the center. Given the nature of the urgent care business model, most centers would expect to provide the NPP to a patient at the time that he or she presents to the center. A signed acknowledgement of every patient's receipt of the center's NPP should be maintained in each patient's medical record. The NPP must be on display in a prominent location within the urgent care center, such as on a wall near the front desk where patients check in. In addition, if an urgent care center maintains a website, the NPP will also need to be prominently located on it. Like the center's policies and procedures, the NPP also should have been revised by September 23, 2013 to reflect the changes required under the Omnibus Final Rule.

6. Understand Breach Notification Requirements

Upon learning of an unauthorized use or disclosure of patient PHI, an urgent care center must determine if there has been a breach using the new 4-factor risk assessment provided under the Omnibus Final Rule, as shown in Table 1. The use or disclosure is presumed to be a breach unless the center's analysis of the four factors demonstrates there is a low probability that the PHI has been compromised.

In the event the urgent care center determines that there has been a breach of unsecured PHI, the center must comply with the following breach notification requirements of HIPAA:

- **Notice to individual:** All affected individuals must be notified by the urgent care center without unreasonable delay, but no later than 60 calendar days after the center's discovery of the breach.
- **Notice to media:** If a breach affects more than 500 residents of a state or smaller jurisdiction (such as a county, city, or town), the urgent care center must notify a prominent media outlet.
- **Notice to HHS:** If a breach affects 500 or more individuals (regardless of location), information must be submitted to HHS at the same time notices are given to individuals. If a breach affects fewer than 500 individuals, the urgent care center need only report such breaches to HHS annually, no

later than 60 days after the start of the calendar year following the year in which the breach occurred.

7. Maintain Documentation Requirements

Finally, it is important for an urgent care center to keep up with the documentation requirements under HIPAA. HIPAA requires documentation—including business associate agreements, employee training logs, logs of unauthorized disclosures of PHI, records of any sanctions taken against employees, and documentation related to the investigation and analysis of any breach—to be maintained by the center for at least 6 years from the date of the document's creation. It is this documentation that the center will need to be able to provide to HHS to demonstrate compliance in the event of an audit or investigation.

Conclusion

Although urgent care centers tend to be smaller entity providers, they should not disregard the importance of a thorough HIPAA compliance plan, particularly in light of HHS's recent pattern of sanctioning entities of all sizes. HHS is expected to implement an audit program within the next year that will result in covered entities of all sizes being randomly selected for an extensive audit of compliance with HIPAA. The audit pilot program was completed in December of 2012 and resulted in the audit of 115 covered entities, the majority of which were health care providers including hospitals, physician practices, dental practices, laboratories, nursing facilities and pharmacies. No urgent care centers were selected as part of the pilot program, but as covered entities, they are subject to randomly selection for future audits which are expected to resume in the fall of 2014. The best offense is a good defense and centers should not wait for an audit or investigation to focus efforts toward HIPAA compliance. ■