The importance of HIPAA compliance for all modes of clinical communication

December 2014
Contents

HIPAA noncompliance is a potential danger for hospitals and physician practices 3

HIPAA stipulates that all forms of ePHI must be secure 4

Clinicians use a multitude of modes to communicate 5

To ensure security of all modes of communication, hospitals and physician practices need established processes and effective tools in place 7

Conclusion 7

References 8
Data breaches have become an increasingly common occurrence, with several large retail corporations experiencing losses in recent years that affected their bottom lines and reputations. The same risks exist in healthcare, with the added concern of jeopardizing the security of patients’ electronic protected health information (ePHI). Many healthcare organizations—both hospitals and physician practices—remain at risk for data breaches. A governmental audit found that 47 of 59 healthcare organizations failed to have complete and accurate risk assessments, as required by HIPAA. The response of many organizations has been to focus on protecting specific modes of clinical communication, such as text messaging, while leaving other forms of communication at risk. In truth, to be HIPAA compliant, hospitals and physician practices must develop and execute a comprehensive plan that addresses all modes of communication.

Since 2003, the Office of Civil Rights (OCR) in the Department of Health and Human Services has received more than 100,000 complaints of HIPAA violations. Almost 23,000 required corrective action. Overall, physician private practices were the entities most frequently requiring corrective action, followed by general hospitals. A 2014 study found that 90 percent of the 90 hospitals and clinics surveyed reported at least one breach in the past two years. About four in 10 reported more than five incidents.

Data breaches involving ePHI are expensive. In addition to the costs of investigation, notification, mitigation and penalties, they can result in litigation, expensive settlements and corrective action plans, or other enforcement, including potential civil monetary penalties (see table). In the study of data breaches previously mentioned, the average cost of breaches during the previous two years was $2 million per organization.
<table>
<thead>
<tr>
<th>Violation category</th>
<th>Penalty for each violation</th>
<th>Penalty for all such identical violations in a calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know</td>
<td>$100–$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable cause</td>
<td>$1,000–$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful neglect, corrected</td>
<td>$10,000–$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful neglect, not corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

In addition to the monetary costs, organizations that experience a data breach suffer a blow to their reputations and disruption to their daily business activities.

The HIPAA Security Rule is technology neutral; it does not expressly require the use or avoidance of any specific modes of communication but requires that all forms of ePHI are secure. Compliance with the Rule is not an attribute of a particular application or device but rather of the safeguards that support the HIPAA-compliant use of electronic communication. There is no such thing as a HIPAA-compliant application or device.

The media has focused attention on the need for secure texting of clinical information. However, appropriate safeguards must be in place to ensure the privacy and security of ePHI transmitted by any form of communication. While these safeguards must adequately address the specific risks associated with texting ePHI, they must also ensure the security of voice messages, alphanumeric pager messages and messages sent via a telecommunications vendor’s website. SMS text messages between mobile devices are generally not secure because they lack encryption. Additionally, telecommunications vendors and wireless carriers may store text messages on an nonsecure network. If these modes of communication are used, ePHI security may be at risk.
Although texting has received a great deal of attention, clinicians commonly use other modes to communicate ePHI. As an illustration, PerfectServe tracked the communications patterns of healthcare providers at a 364-bed hospital. The data revealed approximately 200,000 outbound communications to physicians each year. Text messages were the most common communication mode, but real-time calls, pages and use of third-party answering services were also important modes used to communicate clinical information at the hospital (see figure).

A larger study by PerfectServe evaluated the communication modes used at 60 hospitals. The analysis showed that there were almost six million communication events to more than 22,000 recipients. Less than half of these events involved text messages. A detailed analysis of three of these hospitals found that only 6 percent of the communication events involved physician-to-physician texting and a majority of the communication events between physicians involved real-time calls. Hospital staff used a variety of modes to contact physicians, including real-time calls, text messaging, SMS messages and voice messages.

In a PerfectServe analysis of more than 6,900 physician practices, there were more than one million communication events completed to more
than 25,000 physicians. Staff used a variety of methods to contact physicians, as shown in the figure. Text messaging was the most frequently used mode, but other contact methods were used in about one-third of cases.

In addition, many different communication channels are used to transmit text messages. For example, a nurse might create a message by logging on to the website of a mobile carrier. The message may be sent via the mobile carrier’s network to a pager or via SMS to a physician’s mobile phone. A pharmacist might telephone a call center with a message for a physician; the call center agent may create an electronic text message that is then sent to the physician via a mobile carrier’s network or routed through the Internet. Text messages may be stored on mobile devices, workstations and the servers of the telecommunications vendor or wireless carrier.
HIPAA regulations state that covered entities must assess their risks regarding transmitting and protecting ePHI and must create policies that they can defend to protect its security. They must implement appropriate physical, administrative and technical safeguards to ensure the confidentiality, integrity and availability of the ePHI they create, receive, maintain or transmit.4

Examples of administrative safeguards include conducting risk analyses and staff training. Ensuring a locked location for network servers and shielding screens from unauthorized viewers are examples of physical safeguards. Technical safeguards include encryption and the use of secure passwords.

Rather than focusing on a particular device or mode of communication, HIPAA compliance requires a focus on risk management across the clinical communication process for the entire hospital or physician practice. In its guidance on HIPAA, the OCR states, “An organization’s risk analysis should take into account all of its ePHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its ePHI.”5

Noncompliance with HIPAA regulations can have serious repercussions for hospitals and physician practices. Recent media attention has focused on the need for secure texting of clinical information. However, HIPAA is technology neutral, focusing on the security of all modes of communication rather than particular applications or devices. In addition, clinicians use a variety of modes of communication to transmit clinical information, all of which must be secured. To achieve HIPAA compliance, healthcare organizations must establish appropriate safeguards to ensure the privacy and security of all ePHI transmitted across the care continuum through all forms of communication.

To ensure security of all modes of communication, hospitals and physician practices need established processes and effective tools in place.

Conclusion
References


