Security Starts at Admissions, But Can't End After Discharge

Save to myBoK

By Mike Morper

Admissions and discharge processes can be rife with vulnerabilities and potential HIPAA violations. It is important to address security vulnerabilities and potential compliance problems in the patient admissions and discharge processes. A focus on file destination control, encryption, authorization, and authentication are important to achieving "meaningful use" of electronic health records (EHRs).

Mind Admission and Discharge Data

One of the greatest challenges hospitals face is how to successfully deliver on dual requirements to make information in an EHR more accessible while ensuring security, especially with a reliance on paper, analog fax machines, unmonitored multi-function devices (MFDs), and smart devices.

When a document or form is copied, scanned, printed, faxed, or e-mailed, patient health information (PHI) can be exposed or compromised. With no encryption, user authentication, audit trails, or other security controls, each document and action presents a risk of exposure and a point of vulnerability where PHI can be accidently or intentionally compromised.

That's why a new risk assessment tool prepared by the Office of the National Coordinator for Health Information Technology (ONC) mentions copiers 15 times as being workstations on which PHI must be protected with administrative, physical, and technical safeguards, including authenticating users, controlling access to workflows, encrypting data handled on the device, and maintaining an audit trail of all activity.

Hospitals should conduct risk assessments to identify threats and vulnerabilities, train workers in data loss protection (DLP) technology and procedures, and establish security incident reporting. These requirements are found throughout sections 164.306 (general), 164.308 (administrative safeguards), 164.310 (physical safeguards), and 164.312 (technical safeguards) of the HIPAA Security Rule.

Security vulnerabilities and potential compliance issues impacting patient admissions and discharge processes are usually found with analog fax machines that lack activity logging; every digital multi-functional device that copies, prints, scans, and faxes documents stores images on an internal drive and retains e-mail addresses, network and user IDs, and even passwords in its memory. Secure information collection and output management experts strongly recommend that healthcare organizations add a layer of security and control to electronic and paper-based patient admissions and discharge processes. This will help minimize the manual work that invites human error, and automatically mitigates the risk of non-compliance, which will help avoid the cost and reputation damage of HIPAA violations and privacy breaches.

Securing PHI

Admission orders, patient consent forms, insurance ID cards, prescriptions, and even driver's licenses are routinely copied, scanned, printed, faxed, or e-mailed as part of the process for getting patient information into the EHR. Upon discharge, the patient typically receives a package that includes summaries of care, instructions, and more. Without security controls, each document and action presents a risk and vulnerability.

While paper can be difficult to track and control, the same vulnerabilities exist in electronic admissions and discharge processes. Electronic admissions might involve scanning a new patient's admission form into the EHR or populating a form with a previous patient's stored information. The hospital's method of sharing that information might include e-mailing it or even faxing it to other departments, such as the pharmacy.

Securing Patient Information on Mobile Devices

Mobile devices present another set of risks to the EHR. Theft or loss of mobile devices, laptops, and portable media is the biggest source of reported HIPAA data breaches. In one instance, a portable computer lost in Connecticut contained the PHI of 1.5 million individuals—over a third of the state's residents. And the theft of two laptops in California compromised the PHI of 729,000 patients treated at six hospitals, according to the Department of Health and Human Services' website.

The risk of mobile device theft or loss comes from their non-secured use. If a hospital's mobile strategy has not fully accounted for security, employees might be using devices inappropriately in their own EHR workarounds. Imagine an admissions clerk who photographs a patient's insurance card or driver's license on a mobile phone, e-mails those images to her hospital e-mail address, then imports them into the patient's EHR—with no record of how the information got there and no guaranteed deletion of the images from the employee's mobile phone.

Adding a layer of automated security and control to processes that involve paper is essential in helping hospitals protect PHI and achieving HIPAA compliance. Software can minimize the manual work and decisions that invite human error, mitigate the risk of non-compliance, and avoid the fines, reputation, damage, and other costs of HIPAA violations and privacy breaches.

Know Your Security Rule Safeguards

Admissions and discharge processes should ensure that processes meet the security safeguards spelled out in the HIPAA Security Rule:

- Authorization: Only authorized staff can access specific devices and network applications with password- or smartcard-based authentication that is seamlessly integrated with the document workflow.
- Authentication: User credentials are verified at the device, by PIN/PIC code, proximity (ID), or by swiping a smartcard to access documents containing PHI. Once authenticated, the solution controls what users can and cannot do. It enables or restricts e-mail or faxing and prohibits documents with PHI from being printed, faxed, or e-mailed.
- Encryption: Communications between smart MFDs and mobile terminals, the server and destinations, such as the EHR, are encrypted to ensure documents are only visible to those users with proper authorization.
- File destination control: Simultaneously monitors and audits the patient information in documents, ensuring PHI is controlled before it gets to its intended destination.
- Content filtering: Automatically enforces security policies to proactively prevent PHI from leaving the hospital by filtering outbound communications and intercepting documents, or rendering misdirected or intercepted information unreadable to unauthorized users.

In secure admissions and discharge processes, manually completed forms and documents are still scanned into the hospital's master patient index. But the admissions clerk must first authenticate themselves at the MFD to gain access to authorized functions or pre-defined workflows. Only then is the document securely transferred to the software server and routed together with its metadata to the hospital's document management system or EHR. It is important to secure documents at the point of capture by requiring a password to later access any document scanned to PDF.

This process can just as easily begin electronically, with the clerk capturing files on a computer desktop or mobile device. When documents need to be printed, a system is required that prevents exposure of information by holding jobs in a secure print queue and not releasing them without authentication/authorization. Data capture and output management software completely eliminates the risk of faxes being sent to wrong or unauthorized numbers. Outbound fax number verification compares manually entered numbers against a database of allowable numbers, so if a number is mis-entered or invalid, then the fax won't be sent. For even greater security the solution can present a pick list of authorized fax numbers.

From the MFD the fax is transmitted securely via SSL (the same technology used to encrypt e-commerce transactions) to a document processing server where the resulting image can be cleaned and straightened automatically. Any text on the page is then converted into a machine readable format allowing for key information about the document, known as metadata, to be automatically extracted. Next, an advanced content filtering solution can further interpret the text of the document and quickly identify if it contains confidential information specified by the hospital, and if so, automatically redact sensitive information or simply stop the fax from proceeding. Either way, the system can notify the administrator of the attempted entry of an invalid number. The fax is also routed to the patient's EHR, together with a complete Health Level Seven recommended audit trail

identifying who sent the fax, when, from which device, to what number, how many pages it contained, and the name of the patient.

A secure solution also allows HIPAA-compliant use of mobile devices for creating, accessing, or sharing patient information. Electronic admissions and discharge forms—including patient signatures—can be completed on tablets and the information securely transferred to the EHR. Insurance cards, patient IDs, and other paper documents can be photographed with the device's camera and automatically deleted, so that a lost or stolen device provides no access to patient information.

Security Starts at Admissions

The admissions department is the gateway to a hospital's meaningful use of their EHR, and the frontline in the effort to secure patient PHI. It is a fight that must continue through and beyond patient discharge.

Mike Morper (mike.morper@notablesolutions.com) is vice president of marketing at Notable Solutions, based in Rockville, MD.

Article citation:
Morper, Mike. "Security Starts at Admissions, But Can't End After Discharge" *Journal of AHIMA* 85, no.11 (November 2014): 54-55.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.