The secure exchange of protected health information.

NUANCE

Table of contents

Executive summary

To demonstrate meaningful use of electronic health records (EHR), as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act, hospitals must fulfill the seemingly contradictory mandates to increase the sharing of patients' protected health information (PHI) while also keeping it secure.

The challenge for hospital compliance officers and IT directors is that there are too many information touch points throughout the patient lifecycle that entail the risk of Health Insurance Portability and Accountability Act (HIPAA) violations in generating, using and sharing PHI. Many of these involve hospitals' growing use of networked multifunction devices (MFDs) that copy, print, scan, fax and email.

Nuance Document Healthcare Solutions adds a layer of security and control to paper-based and electronic processes, enabling the secure exchange of PHI. This advanced capture and output platform helps hospitals to reduce errors, automatically mitigate the risk of non-compliance and avoid the fines, reputation damage and other costs of HIPAA violations and privacy breaches.

The high cost of protected health information being at risk.

The message from the federal government is clear: Hospitals need to do a better job of securing patients' protected health information (PHI).

In what some observers see as a signal of more strenuous enforcement to come, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) in May 2014 reached a record-setting $4.8 million settlement with New York Presbyterian Hospital and Columbia University in a case in which electronic PHI of 6,800 individuals, including patient status, vital signs, medications and laboratory results, was exposed on the Internet.

$1.5

million maximum OCR penalty per violation for HIPAA privacy and security rule breaches.

A year earlier, OCR had reached a $1.2 million settlement with Affinity Health Plan over that company's failures to remove the PHI of nearly 345,000 individuals from the hard drives inside photocopiers it returned to a leasing agent, to include the devices in its analysis of risks and vulnerabilities and to implement policies and procedures for the devices' return.

These settlements came in the wake of the Final HIPAA Omnibus Rule of 2013, in which OCR had increased the penalties for HIPAA privacy and security rule violations from $25,000 to a maximum of $1.5 million per violation.

From the start of the federal reporting requirement in September 2009 into early June 2014, the number of people with medical records exposed in a reportable data breach had reached nearly 31.7 million—equal to 10% of the U.S. population. The cumulative number of breaches involving more than 500 patients passed 1,000. The number of breaches involving fewer than 500 had passed 116,000 a year earlier.

31.7M

number of people with medical records exposed in a reportable data breach from Sept 2009 – June 2014.

And those are just the federally reported breaches. In its Fourth Annual Benchmark Study on Patient Privacy & Data Security, published in March 2014, the data security and privacy research organization the Ponemon Institute reported that 90% of the healthcare organizations in its survey had had at least one data breach in the previous two years; 38% said they had more than five incidents. Even if these breaches didn't result in federal fines or multimillion dollar settlements, they still took a toll. Ponemon calculates that, on average, breaches cost the surveyed organizations $2 million over two years. Projecting those figures industry-wide, Ponemon estimates data breaches cost the healthcare industry up to $5.6 billion annually.

The compliance officer's dilemma: keeping PHI secure while making it accessible

Besides hospital compliance officers being kept up at night by the costs, fines and reputation damage of data breaches or HIPAA violations, the sheer volume of data security risks and vulnerabilities further adds to their worries. Especially vexing is the irony that the technologies that hospitals are counting on to increase efficiency, improve outcomes and help them achieve meaningful use of electronic health records (EHR) technology may also be their largest security vulnerabilities.

Theft or loss of mobile devices, laptops and portable media containing unencrypted PHI continues to be the leading source of reported HIPAA data breaches, accounting for 45% of incidents and 83% of affected records in 2013. Over 20% of incidents involved unauthorized access, separate from hacking, often by employees or other insiders. In line with the reported incidence of theft, loss and unauthorized access, 83% of hospital respondents in the Healthcare Information and Management Systems Society's 6th Annual Security Survey (published in February 2014) said the risks that concerned them most were human-related factors such as employees losing devices, unintentionally disclosing information or actively circumventing or interfering with security access controls. In the Ponemon study, 47% of respondents had little to no confidence they could detect all loss or theft of patient data.

> "Theft or loss of mobile devices, laptops and portable media containing unencrypted PHI continues to be the leading source of reported HIPAA data breaches."

These concerns are well founded, because there are too many touch points in the creation, use and sharing of PHI that invite the risk of human error or bad intent. Plus, security is not the priority of employees who handle PHI. Hospital staff will often do what they think it takes to get their jobs done, such as sending documents or pictures to themselves from their cell phones, even if it is not compliant.

> "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."

Industry media is full of stories of hospitals faxing prescriptions, insurance information and clinical reports to wrong numbers, attaching files to the wrong patient record, emailing documents to a wrong address or transmitting PHI when not authorized or appropriate to do so. Some hospital workers have created problems for their employers by posting cell phone photos of patients on social media.

PHI is also put at risk by everyday activities that don't make the news, and which may go undiscovered. Admissions orders, discharge instructions, prescriptions, clinical summaries and other PHI containing documents printed to shared multifunction devices (MFDs) could expose patient information if left sitting in the output tray or picked up by the wrong person. Unsecured MFDs could be used to make and transmit unauthorized copies or scans. Documents stored in the MFD's hard drive could be improperly printed out or copied onto a USB stick.

In the absence of 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 accidentally misdirected 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 that:

– Authenticate users
– Control access to workflows
– Encrypt data handled on the device
– Maintain an audit trail of all activity

Hospitals also need to conduct a risk assessment to identify threats and vulnerabilities (including copiers), implement and 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.

Whether your hospital's processes are paper based, electronic or a combination of the two, the only way to share and distribute PHI within HIPAA compliance using smart devices that copy, print, scan, email or fax is under a system incorporating technological security and authentication.

Simple, secure exchange of patient information

Nuance document workflow solutions help hospitals achieve the secure exchange and use of patients' protected health information. Adding a layer of automated security and control to both electronic and paper-based processes, the Nuance software capture and output platform minimizes the manual work and decisions that invite human error, mitigates the risk of non-compliance and helps hospitals avoid the fines, reputation damage and other costs of HIPAA violations and privacy breaches.

Nuance document workflow solutions combine multiple security best practices into a complete process for reducing vulnerabilities in capturing and sharing PHI:

– **Authorization**: Only authorized staff can access specific devices, network applications and resources. This is secured through password- or smart-card-based authentication. Network authentication is seamlessly integrated with the document workflow and to ensure optimal auditing and security, documents containing PHI are captured and routed to various destinations such as email, folders, fax, line of business applications and EHR systems.

– **Authentication**: User credentials must be verified at the device, by PIN/PIC code, proximity (ID) or by swiping a smart card to access documents containing PHI. Once users are authenticated, the solution also controls what they can and cannot do. It enables or restricts email or faxing and prohibits documents with PHI from being printed, faxed or emailed.

– **Encryption**: Communications between smart MFDs and mobile terminals, the server and destinations such as the EHR, are encrypted to ensure documents are visible only to those users with proper authorization.

– **File Destination Control**: Simultaneous monitoring and auditing of patient information in documents ensures PHI is controlled before it ever gets to its intended destination.

Nuance document workflow and security solutions enable secure Follow-You Printing within leading EHR systems.

– **Content Filtering**: Nuance solutions automatically enforces security policies by filtering outbound communications and intercepting documents, to proactively prevent PHI from leaving the hospital and render misdirected or intercepted information unreadable to unauthorized users.

Nuance document workflow and security solutions are already at work at hospitals all across the U.S., providing protection for data at rest, data in motion and data in use required for institutions to demonstrate meaningful use of EHR technology.

For example, Nuance document workflow solutions enable secure Follow-You Printing from within leading EHR systems. Print jobs, such as forms created or completed in the EHR, are encrypted and held in a print queue on the Nuance server until the user signs in to release them at the MFD. Workers can even use a mobile device to activate "touch free" release of the document. Either way, secure Follow-You Printing reduces the risk of exposing information in documents left unattended at the printer.

Sharing information by fax or email, or scanning documents into the EHR, is also made more secure. Nuance document workflow solutions can prevent mis-delivery of faxes or emails sent from the MFD by checking the destination against a list of approved numbers or addresses. Intelligent content filtering of faxes and emails can recognize and redact confidential information that shouldn't be sent, preventing unauthorized transmission of patient information. Scanned documents can be secured at the point of capture by requiring a password for accessing them later.

Security made easy

By simplifying users' workflows as it transparently adds security, Nuance solutions increase employee acceptance and reduce the need for them to find workarounds that bypass security measures.

Consider the common action of scanning a document and emailing it to oneself as a simple way to work with it electronically. In a non-compliant workflow, a worker might authenticate at the MFD, select SCAN as a function and enter her own email address as the destination. Besides requiring upwards of 30 keystrokes, this process is not compliant if the document or sending device is identified by a generic descriptor—BrandNamePrinterScan001.pdf, for example—or the action is not captured in an audit log.

Nuance solutions can make this activity as easy as tap and go. A user walks up to the device, signs in by tapping their proximity card against the reader and then chooses SCAN TO MY EMAIL from a list of pre-defined and pre-authorized workflows displayed on the MFD's control panel. It's a faster, simpler, error-free process and—with the activity audited as to user, device, action, email address, date and time and document metadata—helps strengthen an organization's HIPAA compliance initiatives.

A complete audit trail

The importance and necessity of audit logging in HIPAA compliance cannot be overstated.

Even before the ONC's newest risk assessment tool extended HIPAA security requirement to copiers, HIPAA security standards had always required covered entities to "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." By building an audit trail of all copy, print, scan, email and fax activity at every networked MFD, including paths to document images, Nuance document workflow and security solutions help bring use of these devices into HIPAA compliance.

Just as important, reviewing the audit log can help a hospital to identify a breach, take prompt corrective action, issue the necessary notifications and avoid the cost of fines. That's because correcting a violation within 30 days of acquiring "actual or constructive" knowledge of it provides an "affirmative defense" and immunity against HIPAA's civil monetary penalties.

The importance and necessity of audit logging in HIPAA compliance cannot be overstated.

Conclusion

As a deadline approaches for hospitals to demonstrate meaningful use of electronic health records (EHR), the monetary penalties, settlements and costs for failing to secure patients' protected health information (PHI) are increasing. Meaningful use requires the ability to both share and protect that information. But there are simply too many touch points that create risk in sharing PHI, most of these involving the technologies that hospitals are counting on to deliver the benefits of EHR technology—especially smart devices that copy, print, scan, fax and email.

Nuance helps organizations facilitate the secure exchange of PHI by adding a layer of security and control to paper-based and electronic processes. Transparently applying automated security techniques that cannot be circumvented, this advanced capture and output platform authenticates users, controls access to workflows, encrypts data and builds and maintains an audit trail of all user activity. As a result, Nuance document workflow and security solutions minimize the manual work and decisions that invite human error, mitigate the risk of noncompliance and help hospitals avoid the fines, reputation damage and other costs of HIPAA violations and privacy breaches.

Hospitals nationwide already depend on Nuance to help secure data at rest, data in motion and data in use, as required for demonstrating meaningful use of EHR. Beyond meeting institutions' requirements today, Nuance solutions will continue to evolve, keeping pace as threats, vulnerabilities, breaches and the best practices for responding to them change in the future.

Violation Category	**Penalty** (each violation)	**Maximum penalty** for violations per category per calendar year
Did not know	$100-$50,000	$1,500,000
Reasonable cause	$1,000-$50,000	$1,500.000
Willful neglect—corrected	$10,000-$50,000	$1,500,000
Willful neglect—not corrected	$50,000	$1,500,000

Threat assessment/security scorecard print/ copy/scan/fax/email vulnerability

– Can anyone (even a visitor), walk up to your copiers (MFDs) and copy any document? Can they scan any document to a folder, email or fax?
– Are printed jobs left in the output trays of printers and copiers unattended?
– Have you disabled the USB ports to prevent someone from scanning to USB devices?
– Do you maintain an audit trail of print, copy, scan and fax activity: who, what, when, where, how?
– Can anyone walk up to your fax machines and fax documents—anywhere?
– When your MFDs leave your building (at the end of a lease, for example), is there any confidential data still stored in them?
– Is there any sensitive network information stored in your MFDs? Are device passwords yours?
– When archiving documents, are you using a file format that allows for long-term preservation?
– Is your scan and print transfer SSL encrypted?
– Do you keep a digital archive of all transmitted faxes?
– Do you control authorized fax destinations?
– Has your organization invested in any DLP technology? If yes, how have you integrated this into your MFD architecture?
– Do you have business processes that are unnecessarily complicated with many error-prone touch points, where people print, fax, copy, scan, and mail—all within one process?
– When people fax a document, do you have any way of knowing if they typed the wrong fax number? What measures have you implemented to mitigate this risk?

About Nuance Communications, Inc.
Nuance Communications is reinventing the relationship between people and technology. Through its voice and language offerings, the company is creating a more human conversation with the many systems, devices, electronics, apps and services around us. Every day, millions of people and thousands of businesses experience Nuance through intelligent systems that can listen, understand, learn and adapt to your life and your work. For more information, please visit nuance.com.

49A 914