WORKFLOW TECHNOLOGY AND HIPAA COMPLIANCE:

CHALLENGES AND BEST PRACTICES

By David Harlow JD MPH | A White Paper Commissioned by Brother International Corporation

Healthcare has one foot in the past and one foot in the future. This is true across so many dimensions, but nowhere is it more obvious than in the daily struggles with information management. Healthcare has traditionally been a paper-intensive environment, and that continues to be the case even while most healthcare providers have transitioned to electronic health record (EHR) systems. While work is being done to ensure that EHR systems are better able to "talk" to each other and to other health information systems, the day-to-day experience of many healthcare organizations is still rooted in paper and in the need to print, copy, scan, and fax innumerable paper documents.

Because virtually all healthcare organizations use electronic transactions of one sort or another (e.g., billing and payment) even their paper records are subject to the HIPAA privacy and security rules – a set of federal rules first adopted about fifteen years ago, and substantially revised in 2013 under the HITECH Act.

Healthcare organizations are subject to a plethora of other laws as well in the use of records: state privacy laws (many of which are more stringent than HIPAA), Federal Trade Commission oversight (a data breach may be considered an "unfair business practice" under the FTC Act), as well as rules requiring healthcare organizations to maintain accurate patient records and personnel records.

These laws are enforced by various state and federal agencies – and HIPAA may also be enforced by state attorneys general. FTC enforcement can prove to be more onerous than HIPAA enforcement (the FTC can impose long-term compliance plans with monitoring requirements, in addition to fines). Private lawsuits may also be brought where a HIPAA violation has been found – not under HIPAA, which prohibits private actions, but under state law, which may recognize a HIPAA violation as a breach of a duty that can give rise to a lawsuit.

brother
at your side

WORKFLOW TECHNOLOGY AND HIPAA COMPLIANCE:
CHALLENGES AND BEST PRACTICES

brother
at your side

HIPAA enforcement cases regarding data breaches on unencrypted electronic office equipment have resulted in million-dollar fines and other sanctions. For example, when CBS News purchased a used copier previously owned by a healthcare management organization, the copier's hard drive had not been purged or destroyed, and it still contained protected health information (PHI) for 350,000 plan members. ($1 million fine and plan of correction imposed on the health plan.) To give another example, a Boston-area teaching hospital suffered the loss of an unencrypted, non-password-protected laptop, left in an unlocked room in the hospital. (Similar sanctions.)

What lessons can we learn from past data breaches, which have increased dramatically in number and in volume over the past year or so? First, that data breaches are a fact of life in our modern world. Second, and just as important, that a solid compliance program encompassing appropriate administrative, technical and physical controls can minimize the likelihood of a data breach. Such a program will be built on policies and procedures designed to ensure that the right equipment is in place and is being used in the right way. Technical vulnerabilities are a key category of vulnerabilities to be addressed (through encryption and secure storage), and human factors are another (many breaches are initiated through emailed links clicked on by individual employees that load malware into enterprise systems).

In order to ensure compliance with HIPAA (and other data privacy and security rules) health care organizations must implement policies and procedures that are tailored to the work that they do as well as their size. HIPAA is not a one-size-fits-all regulatory regime, and best practices for data privacy and security programs demand attention to the specific operating environment of each healthcare organization.

Once an organization has its policies and procedures in place, it must conduct a risk assessment (and must repeat it annually – more frequently if it changes any of its hardware, software, or controls). This includes taking an inventory of assets that may be related to health data – including office equipment such as scanners, printers, fax machines, and copiers – to identify both the breach potential inherent in those pieces of equipment and their related software tools, and the steps taken to minimize the likelihood of a data breach. At the same time, a healthcare organization should also be thinking about how to ensure data integrity.

Best practices would include the following:

- Ensuring that paper PHI is stored properly and securely before and after copying, scanning or faxing. If there is a secure physical location that it should be returned to, then it should be returned there sooner rather than later, and its return should be documented in a file log.
- Ensuring that scanned images are confirmed to be accurate and complete.
- Observing consistent file naming conventions so that scanned documents are properly filed and retrievable.
- Ensuring that paper and/or digitized documents are retained for the appropriate length of time – but no longer. In many circumstances, that means seven years for physicians' records, though there are of course exceptions (e.g., medical records of a child need to be retained for longer). Hospital records may have to be retained for something on the order of twenty years, though of course this rule varies by state. (Since storage is cheap, we tend to keep too many digitized documents and files for too long.)
- Destroying unneeded paper records in a manner that renders them unusable, unreadable or indecipherable to unauthorized persons, e.g. by using a crosscut shredder.
- Similarly, purging, erasing or destroying electronic media including hard drives in copiers, scanners and fax machines at the end of their service cycles, so that the PHI they contain may not be accessed by unauthorized persons.
- Ensuring more broadly that all appropriate and necessary administrative, technical and physical security measures are in place.

Maintaining good data "hygiene" with paper records and files is made easier when one has access to user-friendly, compliant software and equipment, with proper workflows implemented to take full advantage of their technical capabilities. Solution providers can work with you and your team to acquire and integrate the hardware and software necessary to ensure the best practices described above. Some examples of this include:

- Locking individual machine functions by user (e.g., Print, Copy, Scan, Fax Send, Fax Receive and PC Fax), thus limiting the ability of unauthorized users to share data inappropriately. The "key" can be an NFC device, a swipe card or an individual key code.
- Allowing a user to password-protect print jobs to secure his document until he enters his PIN via the machine's control panel. (Thus, sensitive documents will not remain unattended in the output trays of shared printers.)
- Scanning sensitive or confidential documents to a secure FTP site, thus securing data as soon as it is scanned.
- Ensuring that all faxes are received to memory and cannot be printed without a password
- Preventing unauthorized users from sending faxes, thus limiting the potential for inappropriate sharing of PHI.
- Enabling secure faxing and fax forwarding to help maintain patient confidentiality.
- Designing equipment to support face-down printing and faxing, which guards against inadvertent unauthorized document viewing.
- Bypassing hard-copy printouts by using PC-to-fax or "e-fax" function.
- Relaying faxes to clinicians on the go with fax forwarding which improves their efficiency and helps reduce potential data breaches related to fax printouts.
- Scanning integration with some EHR systems.

The key principle that binds these functionalities together is the minimization of exposure of protected health information to anyone but the personnel who have a "need to know." This approach, informed by the regulatory environment and underpinned by the hardware and software capabilities of compliant information systems, enable the workflows needed to provide care effectively and efficiently while maintaining compliance with all of the required data privacy and security policies and procedures.

How does all this work in the real world?

A prime example is Night Nurse, a leader in after-hours pediatric and adult triage services for private practice physicians, clinics, hospitals and educational institutions across the U.S. Night Nurse manages approximately 20,000 paper documents per month, integrated with EHRs and data sources. The company required reliable high-speed, high-volume printer and fax-to-printer solutions to process records and help maintain HIPAA compliance.

Night Nurse excels in an industry with no room for error. The company developed a proprietary IT system - incorporating an integrated series of Brother business-class devices - that helps deliver HIPAA-compliant transactions across faxed paper documents and dozens of disparate EHRs, contact centers and healthcare facilities nationwide.

Chief Operations Officer Stuart Pologe noted, "While electronic systems continue to gain traction, paper documents are still important in the healthcare industry. For many healthcare providers, the most seamless HIPAA-compliant way to transmit information is still by fax technology."

Brother devices play a key role in contributing to their regulatory compliance journey and earning the trust of Night Nurse partners and patients. With its ability to support high-volume information transfer activity using secure technologies, this workflow helped Night Nurse with its compliance efforts, facilitating the expansion of its Massachusetts-only business to operations in 33 states.

In short, using the right tools can help healthcare organizations bridge the gap between the past and the future.

A leader in office productivity solutions, Brother International Corporation is dedicated to innovation, quality, and reliability. As the premier provider of award-winning products and services that enhance and improve the way our customers live and work, Brother offers a complete line of printers, multifunction technologies, scanners, fax machines, label makers, video conferencing, and accessories - along with Web and cloud-based communication, creativity, and connectivity services.

For more information on how Brother is serving the healthcare industry, contact 1-866-455-7713, optimizesales@brother.com or visit www.brotherthinkoptimize.com

David Harlow, principal of The Harlow Group LLC and publisher of the highly-acclaimed HealthBlawg, is a Boston-based health care attorney and consultant focused on digital health and health data privacy and security.