Maintaining HIPAA Compliance across Digital, Paper Records

HIPAA compliance must remain a top priority, even as organizations utilize printers, scanners, and faxes to monitor different types of patient records.

Maintaining HIPAA compliance and numerous data privacy and security mandates is of paramount importance for healthcare organizations. Since HIPAA is not a one-size-fits-all regulatory regime, best practices for data privacy and security programs demand attention to the specific operating environment of each and every healthcare provider. To ensure compliance, healthcare organizations must implement policies and procedures that are tailored to their operations and the size of their organization.

To complicate matters, many organizations are also challenged by the need to balance both digital and paper documents while maintaining HIPAA compliance. Many healthcare organizations handle paper documents and digital files smoothly, however it’s the integration of the two that can add increased compliance layers and often hamper productivity.

This can be solved with a combination of procedures and technologies that enable rapid paper-to-digital and digital-to-paper transformation and transmission, ensuring patient care is handled efficiently and within compliance demands. Printers, scanners, faxes, and multifunction devices can provide a highly connected on-ramp/off-ramp between digital healthcare systems and physical documents. Both electronic data and paper records are subject to the HIPAA Privacy and Security Rules – a set of federal rules first adopted some 15 years ago and substantially revised in 2013 under the HITECH Act.

However, some healthcare organizations are surprised to learn that the risk of non-compliance can greatly increase with the misuse of office devices such as printers, scanners and fax machines. As a result, it is incumbent upon healthcare providers — in both clinical and administrative environments — to institute sound data handling practices for these devices and the documents processed by each. Maintaining good data “hygiene” with paper records and files is made easier with user-friendly, compliant print/fax/scan devices and compatible software. Knowledgeable solution providers can assist in integrating hardware and software necessary to ensure the best practices. To attain compliance with printers, adhere to the following guidelines:

- Allow users to password-protect print jobs that may only be retrieved via a PIN at the device’s control panel. This prevents sensitive documents from sitting unattended on output trays of shared printers.
- Configure printers to support face-down printing, faxing, and copying to guard against inadvertent viewing by unauthorized staff.
- If you must fax, bypass hard-copy printouts by using PC-to-fax or “e-fax” function.

Document digitization enables paper-locked data to enter EMR systems, cloud sharing repositories, and mobile workflows. When employing scanners to assist in executing efficient and accurate data integration, consider digitizing sensitive or confidential documents to a secure FTP site, securing data as soon as it is scanned.

In some cases, moving paper workflows to electronic and automated processes can introduce new efficiencies and increase data security. Turn to tools such as scan-to-email, scan-to-workflow, and electronic file search and retrieval to help bring paper records into the digital workflow.

For many healthcare organizations, the most convenient HIPAA compliant way to transmit information is still by fax technology. Many fax devices are built with advanced security features to address the increasing demand for secure document management. Apply these practices to assist in compliant faxing:

- Ensure that all faxes are received into memory and cannot be printed without a password, or through an NFC card reader for user-based walk-up authorization.
- Prevent unauthorized users from sending faxes, limiting the potential for unauthorized sharing of personal health information.
- Enable secure faxing and fax forwarding to help maintain patient confidentiality by restricting or granting access and privileges on a per-user or per-group basis.

Once device and data policies and procedures are in place, a healthcare organization should conduct a risk assessment and repeat it annually – or even more frequently if it changes any of its hardware, software, or other 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, healthcare organizations should also think about how to ensure data integrity.

From the triage desk to the operating room, fast-paced, regulation-laden healthcare environments leave no room for error. Healthcare organizations can earn the trust of patients, employees and partners by implementing compliant strategies and technologies to help meet HIPAA challenges while balancing paper records and digital documents.

This approach informed by the regulatory environment and underpinned by the hardware and software capabilities of compliant information systems, enable efficient workflows to provide care while maintaining compliance with required data privacy and security policies. The end result can produce a more efficient use of printer/scan/fax devices, with significantly reduced risk of non-compliance.