The Security Risk in Healthcare

Unsecured Faxing

Preventing HIPAA Fines

You could be at risk of having confidential information viewed, copied, and stolen without your knowledge and in doing so face **severe fines**.

What is at risk?

Medical records, health history reports, financial information, personal information, social security numbers, treatment plans, etc. Healthcare organizations are under a lot of pressure to maintain privacy and abide by regulations. Taking into account the type of information healthcare organizations collect and exchange, they are valuable targets for identity theft. For this reason and other discretion provisions, the health industry faces an extra amount of scrutiny because of their responsibility to protect patient's records and privacy. Information scammers can create an entire profile and take over a complete identity based on the content of a single document. Surprisingly, a closer look into health organizations reveals just how ill prepared and unaware most are.

This whitepaper is published by DPD International, makers of the popular GoldFax network faxing solution. For more information visit: www.GoldFax.com.

GoldFax

DPD INTERNATIONAL

Are you in compliance?

- A single HIPAA **fine** can be up to $100,000 with a maximum of $25,000 per person in a single year.
- CVS **settled** at $2.25 million for recent violations against HIPAA.
- Providence Health Systems was **fined** $100,000 for security lapses in 2008.
- Kaiser was **charged** $187,000 for administration penalties resulting from a lack of protection in the hospital for patient health information.

How is your company taking control and ensuring private information be kept secure?

The **Health Insurance Portability and Accountability Act** (HIPAA) established strict privacy regulations pertaining to the security and confidentiality of patients' personal information. Healthcare organizations are required to exercise extreme precautions. Any healthcare provider that electronically files, processes, or transmits medical records, claims, payments, certifications etc. is obligated to comply with HIPAA rules. Individuals who handle the privileged information face strong infringement charges if they fail to maintain the confidentiality of patient's medical records. Not only can individuals be personally fined but individuals can also suffer imprisonment if determined responsible for the mishandling of information.

*HIPAA violation leads to **prison term** for surgeon who peeked at celebrities' records*

Achieving compliance:

What does an organization need to do to comply with HIPAA expectations?

The need to protect health information involves the need for a secure communication system. Private Health Information (PHI) often needs to be communicated whether between doctors, patients and doctors or among medical technicians and personal. HIPAA does not prohibit personal information from being exchanged if necessary but it does require that information is restricted to qualified and privileged eyes. Information sent to any area where exposure to outside personnel is possible is prohibited.

HIPPA's Privacy Rule and Safeguard Principle emphasize *that individually identifiable health information be protected with reasonable administrative, technical and physical safeguards to ensure its confidentiality, integrity and availability and to prevent unauthorized or inappropriate access, use or disclosure*. Implementing safeguard measures is crucial when making communications to prevent inappropriate use or disclosure. Essential for healthcare executives to understand is that some devices responsible for transmitting critical content are inherently insecure.

Where in your organization is information being transmitted?

- Email
- Fax Machine
- Copy Machine
- Telephone
- Standard Mail

Relying on these devices and continuing to use them without restrictions is setting your organization up for violation. Most hospitals and healthcare facilities have implemented security features and policies to protect their employees and patients' data and property including common measures and some very sophisticated technology.

- **Physical Security**- door/cabinet locks, proximity readers (card keys), finger print scan, retinal scan, metal detection, x-ray, etc.
- **Data Security**- firewalls, virus protection, email filtering, data and email archiving, disaster recovery, etc.
- **Monitoring**- video surveillance, motion detection, thermal detection, etc.
- **Security policies**- lock up confidential documents, do not write down passwords, do not open email from unknown sources etc.

All of these are good steps in increasing security; however, faxing is too often overlooked.

The Underestimated Fax Machine:

Your organization most likely has a fax device, possibly many more than you are even aware of. Are they being sent and received in extremely secure environments? Do you feel comfortable sending and receiving your own personal documents through these devices?

Obtaining control of documents that contain important information is critical to any and every organization, especially when those records contain protected health information.

Security Issues: Concerns with Conventional Fax Devices

Access

- Who has access to the faxes?
- Can any doctor or patient walking by view a received fax?
- Faxes can remain on a server for minutes to hours. How is unauthorized access being ensured?
- What precautions are in order to prevent an outsider or another employee in the organization from accessing information?

Authentication

- Who was the fax sent to or received from?
- Can it be documented?
- Are you confident a sent fax was only viewed by the intended recipient's eyes?
- How do you confirm if a fax was sent or that a fax was received?

Reporting and Tracking

- Can fax transactions be audited?
- If needed, can a document be retrieved after faxing it?
- Can you tell who faxed a document on a late Saturday night?
- What process is in effect to make sure not just anyone can retrieve that document?

Received Fax Issues - A received fax is typically **printed, waiting in the open** to be picked up and delivered where it can be viewed by unauthorized personal. How many people actually sit around and wait for a 40 page fax? Faxes can be received 24/7. Is an authorized person always there to receive them? For example, a package delivery person could walk past a paper fax machine and view a patient's medical results sent from a lab with obvious confidential information. More risky is an unauthorized person could inadvertently or intentionally pick up, view and remove a confidential document on a paper fax machine without the intended recipient ever receiving it.

Sent Fax Issues - A sent fax may be left in the open after it has been faxed. Additionally, an electronic document needs to be printed before faxing - creating a **piece of hard evidence** that contains privileged information. It is in the open on both the printer and the fax machine. This creates an additional break for access to confidential information to be compromised. Any information that needs to be copied creates another risk. Not only is there another opportunity for someone to take or view information, but content scanned on copy machines remains on the copy machine. If the machine is ever sold or replaced, scanned document data can be retrieved if not swiped efficiently.

Stolen Identity via the fax - The risks associated with confidential faxes being viewed, lost, or stolen are huge. Confidential data sent and received via fax may contain social security numbers, credit card numbers, bank account numbers, authorization codes, personal health information, proprietary information and agreements, confidential pricing, etc. If this information gets into the wrong hands or eyes, expect to lose business, face fraud, and facilitate the process of stolen identity for both employees and customers.

Increase Security and Compliance:

GoldFax is an enterprise fax software solution that removes the security risks associated with a standard fax machine. With a web client interface, faxes are allowed to be sent from any desktop application, mobile device or MFP. By enabling sending and receiving from email, confirmation receipts and intended recipients are delivered proper information. With GoldFax, each fax can be safely attached in an email and granted access to view by only those who are the targeted recipient. The fax from email capability permits secure delivery directly into an individual's inbox with authentication available. Temporary storage is secure with an audit trail available to track the process if needed, facilitating compliance demands.

Organizations have a choice on how to meet compliance expectations associated with faxing:

1. **Employ more security and procedures.**
2. **Eliminate unsecure devices such as standard fax machines.**
3. **Implement network fax solutions for transmitting documents.**

Contact the GoldFax team today to learn how a network fax solution can improve security and reduce costs.

www.GoldFax.com