Printer, Copier, and Fax Machine Security

Office of Information Technology
Division of Information Security
JUNE 2022

Due to legal and regulatory requirements, the secure storage, processing, and transmission of Personal Health Information (PHI) and Personally Identifiable Information (PII) are central to the Indian Health Service (IHS) mission. Keeping our served population's PHI and PII secure is a shared responsibility, whether the information is in system or portable storage, on a hard drive, or in hard copy, on paper. Printers, copiers, and fax machines have become more complex over time, with multifunctional and wireless capabilities. These assets, their storage components, and any artifacts they produce require the same protection we apply to soft-copy data. Let's take a look at some ways we can do that.

Copiers are Computers

Our desktops, laptops, mobile phones, and tablets are probably the first things we think of when we hear the term 'computer,' however, digital business copiers, printers, and fax machines are also computers. They contain hard drives to manage jobs, workload, and production. These hard drives store data about every single document they copy, print, scan, fax or email. The data needs protection from unauthorized access, even remotely, while the hard drive is in use or by data extraction after hard drive removal.

Let's look at some good guidance for IHS information technology (IT) staff and employees to help keep these machines, their data, and their documents, secure.

IT Staff

The greatest security concerns with printers, copiers, and fax machines relate to data transmission and storage.

Many modern versions of these devices are capable of transmitting and receiving data wirelessly. If a device will not use the wireless capability, IT personnel should disable the capability altogether. If it will, these are some ways to protect the data in transit:

- Change all default administrative user names and passwords.
- Use printers and copiers only on secured (that is, encrypted) Wi-Fi connections.
- Apply patches from the manufacturer as soon as possible and keep device software up to date.
- Disable Simple Network Management Protocol (SNMP) if the environment does not require it.

Most modern printers and copiers have hard drives that store print jobs for varying lengths of time. The printer has no way of knowing which data is PHI/PII, so keeping hard drive contents secure from unauthorized disclosure is of great importance. When we protect sensitive information, we are protecting the communities we serve. IT personnel can ensure we only use equipment with hard drive encryption so data is irretrievable, even if someone removes the drive. IT personnel may also use password protection on the hard drive and periodically overwrite the drive to remove evidence of copied, printed, scanned, faxed, or emailed data. For maximum effectiveness, IT personnel should perform multiple overwrites to ensure no retrievable data remains.

Copier Hard Drive Security at End of Life

IHS devices are either leased or government-owned, so safe data disposal at device retirement can present a challenge. It is important for our IT staff to understand data disposal options when a device is no longer in use. The leasing company may be obligated to remove the hard drive and return it to IHS or our staff may have latitude to keep, dispose of, or destroy the hard drive. Hard disk encryption or passcode protection may help protect it once it is no longer under Agency control.

For government-owned equipment, remove and physically destroy the hard drive prior to disposal.

Now, we will look at the critical role non-IT employees play in protecting sensitive information when using a copier, printer or fax machine.

Non-IT Employees

Hard Copy Security

Prompt hard copy retrieval is an important aspect of security when using these machines. Map your laptop or desktop to the correct printer so you can retrieve any print out containing PHI/PII before any unauthorized persons may view it or take possession of it, intentionally or inadvertently. To lessen this possibility, machines that print sensitive data should be in restricted locations, not in publically accessible areas. When you retrieve your hard copy, avoid any unnecessary detours. Return to your workspace and ensure the hard copy is secured properly, out of sight of curious eyes. When sending a fax containing PII/PHI, use a cover sheet, make sure there is a business need, and do not send the fax unless you are certain the recipient will retrieve it immediately on the other end.

DOs and DON'Ts

Do	Do Not
Handle hard copies in accordance with legal and regulatory requirements.	Pick up hard copies that you didn't print.
Report unattended PHI/PII when you see it.	Transmit PII/PHI if there is no business need to do so.
Stay current on IHS Privacy training.	Keep hard copies with sensitive information in plain sight where unauthorized personnel can view them.
Pick up hard copies as soon as you print them.	Dispose of hard copies containing PII/PHI in a trash can or recycle bin.
Print sensitive information only when necessary.	Make copies of sensitive information without a business need.

What to Do

Information is an IHS asset, so it is everyone's responsibility to keep it secure. If you suspect any unauthorized access to PII or PHI of patients, staff, or other personnel, report it right away to incident@ihs.gov. If you have any questions about this article, please send a message to cybersecurity@ihs.gov.