Business white paper

Create a solid healthcare security position

Security risks and recommendations for healthcare organizations

Table of contents

Protect patient data

Given the wealth of sensitive personal data healthcare organizations process and store, it's no surprise that hospitals, medical offices, and other healthcare organizations are prime targets for cybercrime. As attacks get more sophisticated and the consequences of a breach more severe, security hardening across the operation becomes imperative. Fortunately, HP offers devices with built-in security features and add-on solutions that can help reduce risk and increase efficiencies.

Vulnerable endpoints can put the network and data at risk

Healthcare organizations spend a lot of time and money making sure firewalls are strong and the server infrastructure is protected. But what about endpoints like PCs and printers? These devices are connected to the network. If they become compromised, the entire network—and patient data connected to it—can be at risk.

Printers and MFPs are often overlooked. In a recent study by Spiceworks, only 16% of organizations perceive printers as a high risk for security breaches.[1] Even something as simple as an unclaimed print job can put sensitive patient data in the wrong hands.

Users pose another security risk that is often neglected. Users can be hacked more easily than their devices through deception. For instance, PC users can be tricked into browsing to a fraudulent website that can infect their machine with malware.

Common attack scenarios

A user receives a seemingly innocuous email from his organization. It lures the user to a malicious website that installs malware without the user's knowledge. The malware causes the PC to misbehave and generate a call to the helpdesk. When the helpdesk logs into the device to resolve the issue, the malware steals the helpdesk user's credentials, giving the hacker increased levels of privilege across the network. From here, the attacker can use the malware and the helpdesk user's credentials to access more endpoints and steal more credentials. Soon the hacker has a highly privileged IT account with administrative access to many network resources. He can launch several kinds of malicious attacks—from pranks to ransomware schemes to data theft. Stopping the cycle can be very difficult.

Or, a user receives an email with an attached document that has malicious code hidden within the file. When the user sends the document to the printer, the malware infects the printer. The malware could create all kinds of problems, from simple pranks (such as changing the front panel to a different language) to opening printer ports (thus allowing hackers to upload compromised firmware).

Another way sensitive data can be compromised is through physical theft of devices or documents. A user sends a highly confidential medical record to the printer but then is distracted by an important phone call. By the time she arrives at the printer, the document has been picked up by someone else. Or, a laptop is stolen from a technician's car. The laptop's password is easily guessed, giving the thief access to thousands of unencrypted patient records.

Seven years of backups stolen

A Texas health provider group discovered in early 2017 that an unencrypted hard drive had been stolen from a storage closet. The device held seven years' worth of electronic health record data, including names, Social Security numbers, dates of birth, addresses, phone numbers, driver's license numbers, medical record numbers, insurance provider and policy details, physician names, clinic account numbers, medical histories, medications, lab results, and other clinical data.[2]

Business impacts of a security breach

- Loss of data
- Loss of productivity
- Loss of operations
- Loss of monetary information (such as credit card data)

HP can help

Security must be built into PCs and printers, not bolted on as an afterthought. By designing for cyber resilience, healthcare organizations can help reduce the risk of attacks, increase user productivity by eliminating downtime, cut IT costs, improve compliance, and get back to what they do best—patient care.

This white paper explores some of the security challenges faced by healthcare organizations today and discusses recommended processes, including HP hardware and solutions, that can help reduce risk.

The costs of a breach can be staggering

A data breach can inflict huge costs on organizations, as well as the patients they are caring for. The ramifications of a security breach could include identity theft, stolen competitive information, a tarnished brand image and reputation, and litigation. Plus, regulatory and legal noncompliance can result in heavy fines.

Medical patient records are covered by particularly strict regulations, such as HIPAA (Health Insurance Portability and Accountability Act) in the US. Healthcare breaches remain the most costly per record because of their high visibility and multiple downstream impacts. Stolen patient health records can fetch as much as $402 per record, according to a 2016 report from the Ponemon Institute, which is more than any other piece of data from any other industry.[4]

And security breaches are on the rise. Last year alone, over 4 billion data records were compromised worldwide, a 400% increase over the previous two years.[5] In the US, 2016 saw more healthcare data breaches than any other year since the Department of Health and Human Services' Office for Civil Rights began publishing breach summaries in 2009. In 2016, according to HIPAA Journal, "329 breaches of more than 500 records were reported to the Office for Civil Rights and 16,655,952 healthcare records were exposed or stolen."[6] And there's no sign of letting up. In the first quarter of 2017, reported breaches increased by more than 23% over the same period last year.[6]

Costs of a security breach

- IT time and infrastructure updates to fix the issue and recover data
- Regulatory fines
- Civil actions
- Identity theft monitoring services
- Loss of business
- Loss of brand or share value

= $7.35 million

(Average annual cost of a healthcare breach)[3]

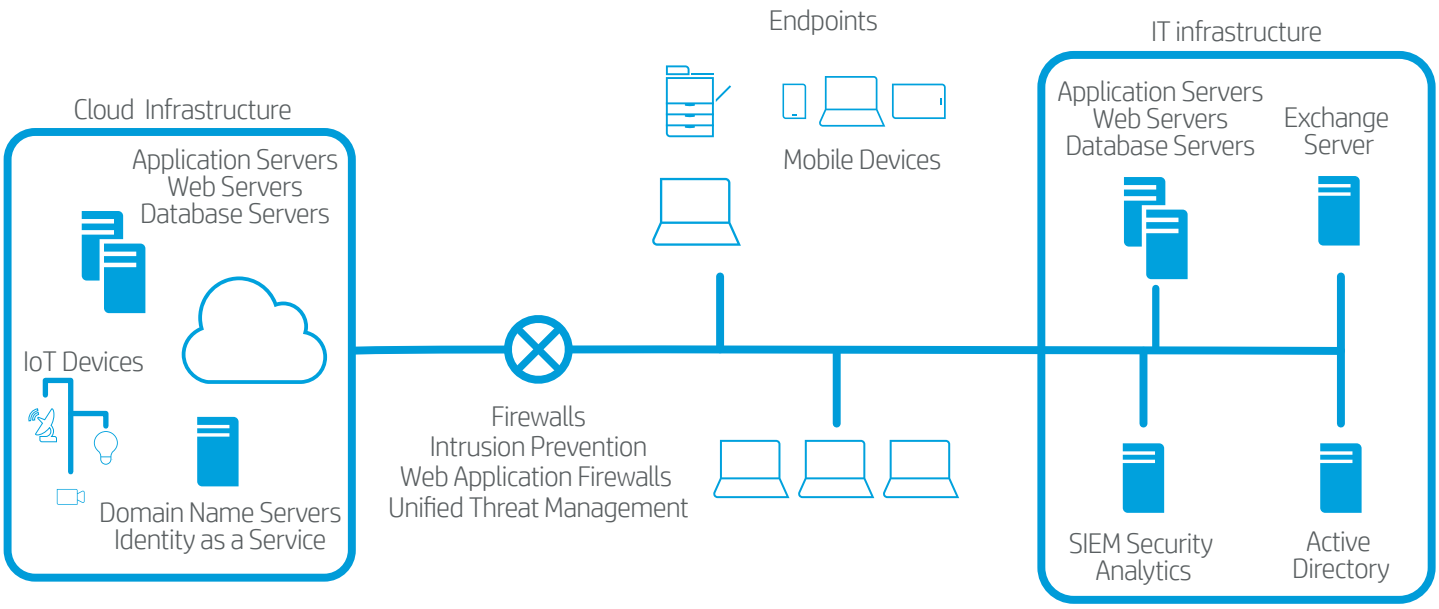
In addition to the financial costs of a security breach, loss of productivity can also cause big problems. Malicious attacks can make PCs unusable, or can cut off providers from the data they need to treat patients safely. An attack at the BIOS level can take hundreds or even thousands of devices down, bringing operations to a halt across an organization.

Healthcare organizations have specific security concerns

Security is important for all companies, but healthcare organizations have additional concerns. These organizations must meet the challenges of protecting Electronic Medical Records (EMR) while, at the same time, providing authorized personnel access to the information they need. To keep patients safe, information must be accurate and delivered quickly. In a public environment—with patients, clinicians, staff, visitors, and suppliers coming and going—the devices that healthcare professionals use must be protected from theft and malicious activity like visual hacking. When time and budgets are tight, IT must find ways to streamline management and monitoring of device fleets. And strict compliance requirements request healthcare organizations to be ready to prove they have protected sensitive information in the case of an audit. This includes safeguarding against internal accidental or malicious breaches by constantly monitoring and analyzing content for data loss detection.

The firewall isn't enough to protect the network

Many organizations are counting on their firewalls to protect the data and devices within the network, but this isn't enough. It's becoming much easier for hackers to break into networks through under-secured endpoints like IoT devices, PCs, and printers. In a typical organization, the number of endpoints is much greater than the number of servers, sometimes as many as two devices per employee. Consider all the computers and printers healthcare workers use throughout the day—including portable devices used in patient rooms and laptops taken home for use after-hours. The sheer volume of endpoints increases the risk. Just one stolen or vulnerable device can provide entry to the network, expose sensitive data, and put the entire infrastructure at risk. That's why it's so important to deploy devices with built-in security protections that can detect and automatically recover from attacks.

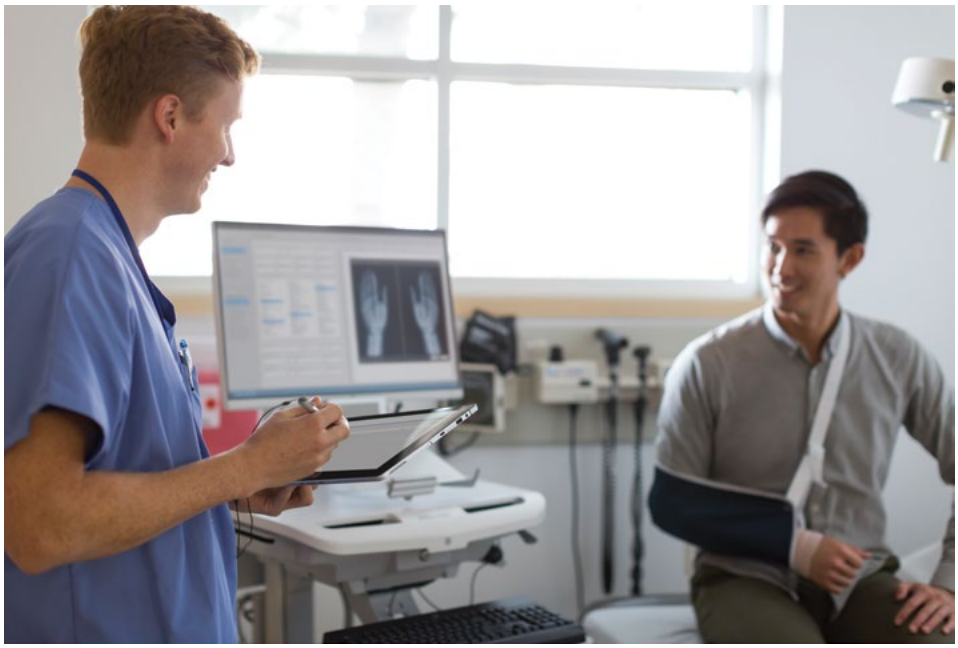


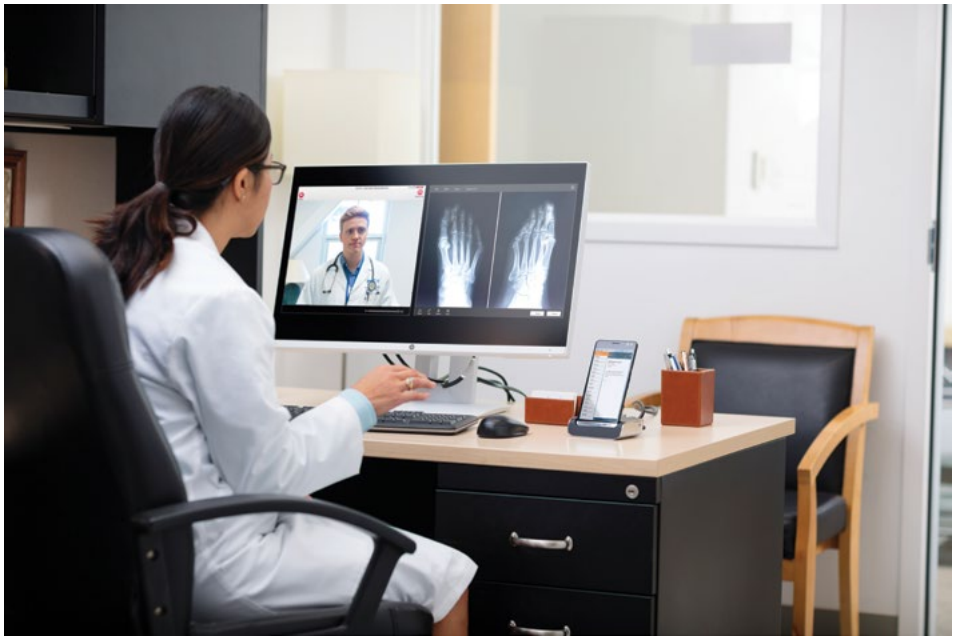
HP designs layers of security to help protect devices and the network

HP is revolutionizing security with a whole new approach: help protect the network and reduce risk by building layers of security into endpoint hardware. HP printers and PCs are designed to protect the device, identity, data, and document. A comprehensive mix of built-in features and add-on solutions help protect each of these from below (hardware-enforced), within, and above the operating system.

And, of course, any protection needs to be manageable, because security without manageability is unsustainable. HP's unique management solutions help organizations improve endpoint device security without over-burdening their IT staff. Many monitoring and management tasks can be handled automatically, without IT intervention. HP devices are also designed to seamlessly connect to Security Information and Event Monitoring (SIEM) tools to provide real-time security event analysis.

HP understands healthcare security challenges and how to meet them. Whether it's in a clinic, a visit room, a doctor's office, the back office, a provider's home office, or a health insurance company, HP has the devices and solutions to help organizations reduce risk while improving efficiencies.





Healthcare security challenges and HP solutions

Securing the device

Vulnerabilities

Vulnerable endpoints can open the entire network—and any data stored on it—to attack. If devices are rendered unusable by malware, or "bricked", organizations can suffer loss of productivity or even their entire operations.

Printers and MFPs are similar to PCs when it comes to their components, capabilities, and risks. Both PCs and printers start up using firmware called BIOS (Basic Input Output System). The BIOS is responsible for controlling the basic functions of a computing device. It holds the time and date, and configuration settings such as the boot order and the speeds at which the processor and memory run. This is core to how the PC and printer operate, so an unsecured BIOS can offer a dangerous amount of access to a hacker.

BIOS level attacks are very difficult to detect because they control the device below the operating system, and cannot be removed or modified by anti-virus software. Malware targeting the BIOS can continually supply data and reinstate itself after network defenses deploy. It can even survive a disk wipe and operating system reinstallation.

Unsecured wireless connections, open ports, and outdated protocols all can give hackers access to devices and the sensitive patient data stored on them.

Recommendations

To protect against malware, HP Elite PCs offer HP Sure Start Gen 3[7], which uses always-on monitoring to automatically detect, stop, and recover from a BIOS attack or corruption without IT intervention and with little or no interruption to user productivity. Every time a PC powers on, HP Sure Start automatically validates the integrity of the BIOS code to help ensure that the PC is safeguarded from malicious attacks. Once the PC is operational, run-time intrusion detection constantly monitors memory. In the case of an attack, the PC can self heal using a safe "golden copy" of the BIOS in less than a minute. Plus, BIOS Configuration and Policy Protection protects and restores BIOS setup variables, policies, and data. It's the industry's first and only self-healing BIOS with run-time intrusion detection—and it's built-in to HP Elite PCs.[7]

HP Sure Start and run-time intrusion detection are also included on HP Enterprise printers and MFPs to protect at startup and during operation. If malware is detected, the printer automatically shuts down and reboots the device. Every time a printer is turned on or restarts with an error, HP Sure Start automatically validates the integrity of the BIOS code and self-heals if necessary. There's no need for IT to intervene. HP Enterprise printers and MFPs also include whitelisting to help ensure that only authentic, known-good HP firmware—digitally signed by HP—is loaded into memory. Only HP Print Security offers real-time detection, automated monitoring, and built-in software validation to stop threats the moment they start.[8]

It's important to keep the OS updated to the latest version. HP Enterprise printers and MFPs are powered by upgradeable FutureSmart firmware, which allows organizations to update printers with new security features as they become available. HP Elite PCs come with Microsoft Windows 10, the most secure Windows ever. HP hardware is designed together with Windows to help secure the device below, within, and above the operating system. IT departments can save time with management tools that allow them to check firmware versions and update firmware across the printer and PC fleets. Plus, HP offers Managed Print Services to further reduce the burden.

For both printers and PCs, administrators should close unused ports and protocols—for example, to prevent malware being uploaded from or data being downloaded to a USB drive. For printers, IT can manage USB ports and removable media with HP Web JetAdmin or HP JetAdvantage Security Manager. For PCs, the HP Device Access Manager allows administrators to establish approved users who authenticate and then are granted access to specific PC features for a predetermined period.

And from a print policy point of view, organizations can set policies that enforce only network-approved, secured devices are attached to the network, to reduce the risk of non-compliant devices.

Half a million clients' data at risk in ransomware attack

A hacker targeted a Michigan home medical equipment supplier in April 2017. After getting access to the network, the hacker installed ransomware, which shut employees out of the system. Personal health information for 500,000 clients—the type of data often used for medical fraud—was stored on the affected network.[9]

Securing the identity

Vulnerabilities

PC credentials are a top target for thieves, because they can provide hackers an entry point to the IT infrastructure. Passwords alone no longer provide the level of security required for today's threats; and users often take shortcuts that reduce the integrity of passwords. According to Verizon's 2016 Data Breach Investigations Report, weak or default passwords were a factor in the majority of data breaches.[10]

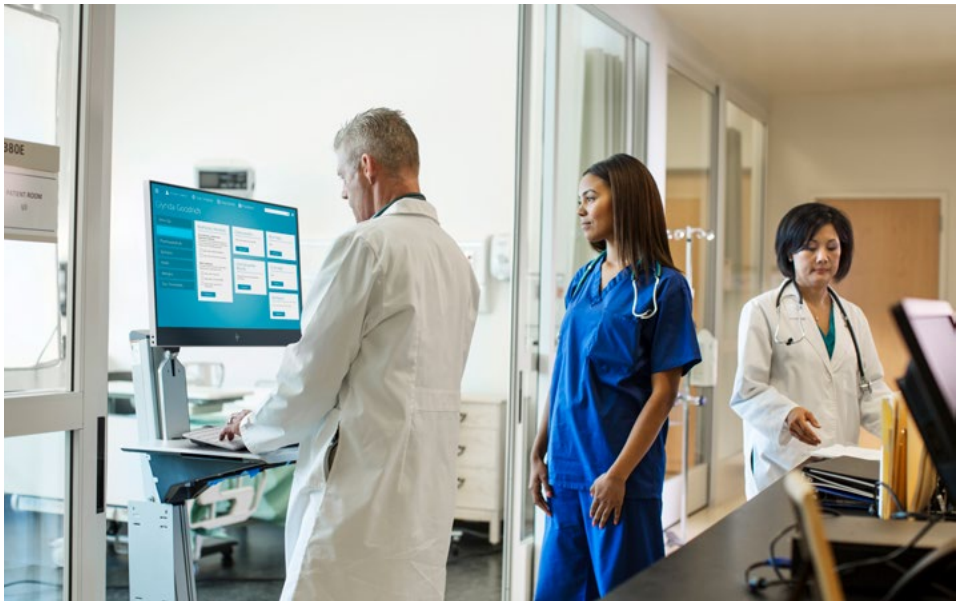
But even for PCs with strong authentication systems, once a user signs in, PCs generally stay unlocked if the user walks away and leaves the computer unattended. A hacker who is physically

present can simply sit down and gain access to any data on the device or on the network it's connected to. This is a particularly difficult problem in fast-paced healthcare environments that use notebooks, detachables, or convertibles where many people are coming and going. The portability of these devices gives providers more flexibility but increases the risk of an unattended device being accessed or stolen.

Recommendations

Good password security makes the user's life easy while making the attacker's job difficult. HP customized Intel® Authenticate™ to provide authentication with credentials and policies hardened at the silicon level. HP Elite PCs with HP Multi-Factor Authenticate[11] can verify identities by using a combination of factors. By requiring more than one factor, such as what a user knows (password, PIN), what a user is (fingerprint), and what a user has (proximity card, smartcard, contactless card, or smartphone connected by Bluetooth®), users get a faster, more seamless login experience that is one million times more secure than a single non-hardened password.

For automatic protection against unauthorized access of unattended PCs, there's HP WorkWise.[12] This solution uses a strong cryptographically secure connection to the user's smartphone to detect when the user walks away from his or her PC, and automatically locks it. While away from the PC, the user can receive notifications of tamper alerts. (Tampering events can include USB drive insertion, laptop lid open or close, power cord plug insertion or removal, and authentication failures.)



Securing the data

Vulnerabilities

Keeping patient data safe is one of the most important duties of healthcare organizations. When a breach occurs, the costs can be high—both financially and to the organization's reputation. Even without an actual breach, organizations that fail to meet compliance requirements can face steep regulatory fines.

Without a strong authentication system and administrative controls, devices—and the data they're connected to—can become available to unauthorized users.

And attacks are getting more sophisticated, with hackers often gaining access to the system by deceiving users. It's not that easy for users to identify a "good" link from a "bad" link with the dozens or hundreds of emails that most users get daily. Something that looks as innocent as a LinkedIn invite can contain hidden malware. In fact, 81% of IT security practitioners cite insecure web browsers as a primary attack vector.[15]

Breach puts data for 3.3 million patients at risk

In 2016, a provider of insurance ID cards discovered that a server had been accessed, potentially exposing the personal information of up to 3.3 million patients.[13] In addition to facing fines and loss of brand value, the company had to offer two years' worth of free identity theft monitoring and resolution services to all victims.[14]

It's not just data residing on a server that's vulnerable. In public healthcare environments, notebook computers can be susceptible to visual hacking. A visual hacker—say, a "patient" who observes a doctor entering credentials—may only need one piece of valuable information to unlock a large-scale data breach. And it's not that hard, according to studies by the Ponemon Institute. Nine out of 10 attempts to steal sensitive business information using only visual means were successful, with nearly four pieces of private information visually hacked per trial. In 68% of the visual hacking attempts, the visual hacker went unnoticed or unchallenged. Nearly half of the visual hacking attempts were successful in less than 15 minutes.[16]

Data can also be at risk if a device is lost or stolen, or when an organization is ready to decommission devices. Organizations often fail to completely wipe data from drives when disposing of PCs or printers at end of life or end of lease.

Recommendations

The first step to protect data is to make sure that only authorized users can access devices and the networks they are connected to. As discussed above, HP Multi-Factor Authenticate can help protect PCs and identities. For printers and MFPs, fleet-wide authentication solutions can require users to enter a password or PIN, or scan their badge or fingerprint. HP solutions include HP Universal Print Driver and HP Access Control for PC network printing; and HP JetAdvantage Connect and HP Access Control for mobile users.

Other recommendations to protect devices include using strong administrative controls to prevent configuration changes. HP JetAdvantage Security Manager can automatically apply these controls across the print fleet. Role-based access can limit access to only those users who need specific features. For example, HP Access Control allows IT to prevent users from using the email function of MFPs unless they are specifically authorized to do so.

To protect the data itself, encryption is the simplest and most effective safeguard, making stolen data unreadable. Select HP PCs include FIPS Certified Self Encrypting Drives to protect data at rest. HP Elite PCs come with BitLocker Drive Encryption, which is integrated with the Windows 10 operating system to help mitigate unauthorized data access by enhancing file and system protections. It also helps protect against data theft or exposure from lost, stolen, or inappropriately decommissioned computers. Many HP Enterprise printers also include encrypted hard drives. Built-in device encryption can help organizations meet compliance requirements.

Data in transit should also be encrypted. Data traveling between PCs and the network is often encrypted, but data flowing to and especially from printers is often overlooked. Administrators should use Wi-Fi and network encryption protocols along with solutions like HP Universal Print Driver, HP Access Control, or HP JetAdvantage Connect. Apply CA signed certificates to network printers and MFPs. Save time by using HP JetAdvantage Security Manager to automatically install and renew certificates.

Hardware-based Internet browsing security can give users confidence to visit unfamiliar websites while protecting the PC from attacks. HP Sure Click[17] means users don't need to guess whether an email is legitimate or a phishing attack. Each web browser and tab is isolated through virtualization. Malware affecting one tab has no effect on any other tab, app, or the operating system. Once the tab is closed, everything associated with that browsing history is gone.

Keep visual hackers in the dark with HP Sure View, an integrated privacy screen that protects against visual hacking in public environments.[18] Users can block out wandering eyes with just the push of a button—pressing [F2] toggles privacy mode on and off.

Healthcare organizations should make sure data on storage drives is made unreadable and unrecoverable before disposing of or repurposing hardware. HP Secure Erase[19] meets various industry regulations to permanently erase data on PC and printer storage drives. HP also offers on-site data destruction and off-site recycling to erase sensitive information and help keep organizations in compliance.

Securing the document

Vulnerabilities

Unclaimed print jobs are one of the simplest and most common ways sensitive patient data can be exposed. Any printed document is at risk of being stolen by an unauthorized person if the intended recipient isn't there when it comes out of the printer. Additionally, documents are often sent to the printer and forgotten—left unattended for anyone to claim.

While almost all health information is digitized these days, patient charts, critical lab results, treatment plans, discharge papers, and other stats are still frequently printed on paper. In the wrong hands, these paper records can expose protected health information, medical courses of action, or post-discharge treatment plans. Printed stats, when stolen, can have a devastating effect on patients' privacy and can cause the liable institution significant financial harm.

Even when health information is not printed, it still must be protected. Without proper tracking and control, sensitive records—including scanned content like patient admissions forms or lab results—can become available to unauthorized users. This kind of breach can put organizations at risk of noncompliance. Printer input trays can also present a risk. Special paper used for printing checks, prescriptions, or other sensitive documents can be stolen if not protected.

Recommendations

Healthcare organizations should deploy a pull print and user authentication solution fleet-wide so that documents are not printed until the user authenticates at the device using hospital identification security protocols. HP offers several authentication and pull print solutions for a variety of situations and IT environments:

- HP Access Control Secure Pull Print is a server-based pull print software solution that can be set to require all users to authenticate before retrieving their job.
- HP JetAdvantage Secure Print provides an option for print jobs to be sent and stored in a secure cloud queue until the user authenticates and prints the job.
- HP Universal Print Driver is a free print driver solution that includes a secure encrypted printing feature for sensitive documents. It allows users to send a print job to be held until they release the job via a PIN at the device.
- The HP Proximity Card Reader lets users quickly authenticate and print securely at a printer or MFP using their existing ID badge.

Capturing digital information can support record retention and privacy requirements. Securely track and control distribution of scanned content with HP Capture and Route. This HP JetAdvantage Workflow Solution makes it easy to manage, update, and route information—accurately and efficiently. HP Capture and Route is a secure and compliant solution that not only utilizes user authentication and validation, but data at rest encryption, along with a number of other security features.

For a more comprehensive content solution, consider the HP Data Protection solution. This flexible suite of solutions leverages the power of HP MFPs to help secure patient protected health information by tracking what is processed by the MFP and either alerting administrators or stopping print jobs that include sensitive information.

Control access to preprinted forms. Equip your printers and MFPs with locking input trays to help prevent theft of special paper used for printing checks, prescriptions, or other sensitive documents.

Protecting the patient

Vulnerabilities

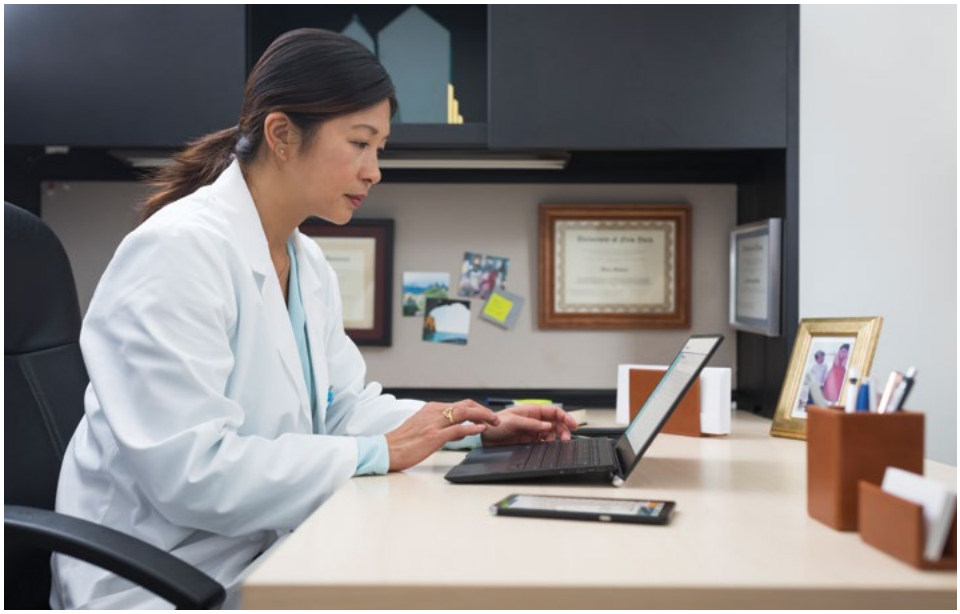
Safeguarding patient identification is a regulation set by healthcare accreditation agencies across the globe. In fact, proper patient identification is the foundation of patient safety. But patient admissions can be complex, manual, multi step processes that can easily lead to errors. New regulations and smaller budgets are causing undue burden on nursing, managerial, and intake staff. To help these people do their jobs accurately, healthcare organizations need to reduce administrative complexity even while they're focusing on improving patient safety and reducing medical errors. Wristbands that stay on the patient and remain readable after repeated use and extended treatments must be easy to print and cost effective to deploy.

Recommendations

The HP Patient Identification Printing Solution for Healthcare increases efficiency and patient safety by allowing healthcare organizations to leverage their investment in existing printers. Consolidate devices by using a broad range of HP devices approved for printing LaserBand® patient identification wristbands and labels.

The solution can help organizations meet Electronic Medical Records protocol without having to invest in new equipment. It allows admissions departments to print a complete patient admissions packet—including not only color-coded wristbands but privacy notices, consent forms, barcoded labels, and documents for lab work, X-rays, or other procedures—from one device, at one time.

Since it is self-laminating, the information on the band is protected against fluids, scratching, or other physical damage throughout the hospital stay. Clinical staff can use a portable barcode scanner to instantly access a wealth of patient information—including photographs, standard medical records, allergy warnings, and so on. This can greatly reduce the potential for error, helping to improve patient safety.



Protecting the prescription

Vulnerabilities

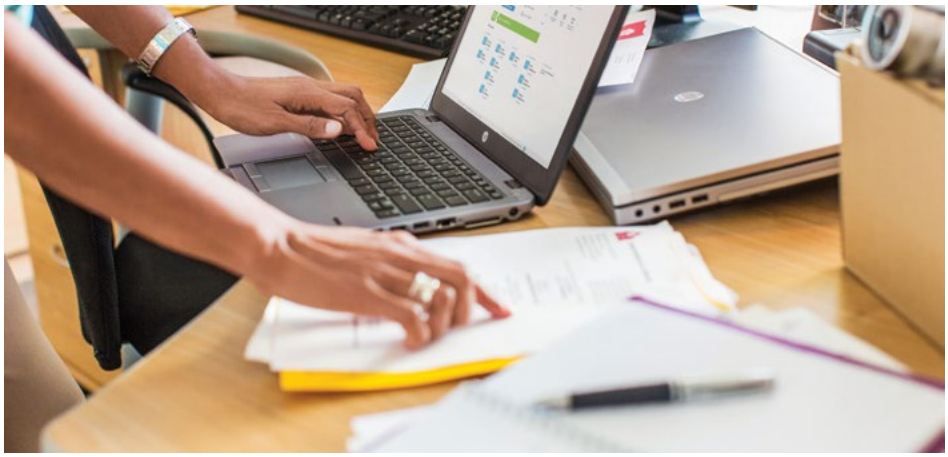
Today's hospital systems need more control over unauthorized prescription access than what's provided by handwritten orders on costly pre-printed forms. As theft of prescription pads becomes more frequent, lucrative prescription fraud threatens to turn healthcare institutions into unwilling enablers for abuse of controlled substances. Secure, tamper resistant, practical, and cost-conscious alternatives to pre-printed prescription forms are essential.

Recommendations

The HP Prescription Printing Security Solution enables healthcare providers to use HP Enterprise LaserJet and PageWide printers and MFPs—and plain paper—to print high-value, black-and-white documents with anti-fraud security features. Or, proven security features can be added to documents printed on security forms paper. The server-based application lets administrators define settings for security printing queues, adding anti-fraud features to print files before they are routed to the printer:

Copy-evident pantograph	Reveals a special pattern when any unauthorized copying or scanning occurs.
Variable data watermark	Prints unique user-defined data across the back of each document to protect against alteration.
MicroPrint optimized	Reveals secondary authentication under simple magnification.
Intelligent warning box	Allows first line inspectors to easily verify document authenticity.

The HP Prescription Printing Security Solution also includes EMR system-generated features for added security.



Streamlining management and monitoring

Vulnerabilities

Unsecured endpoints like printers and PCs can open the entire network to attack. But managing the security of printers and PCs can take a lot of time and expertise. Many IT administrators still use laborious, manual processes, which can drive up costs. Across a large fleet of devices, this inevitably leaves individual devices out of compliance and at higher risk.

Recommendations

HP offers management solutions that save time and help reduce costs and resources to maintain security across the fleet of HP printers/MFPs and PCs.

- For HP PC fleet security, the HP Manageability Integration Kit (MIK) is the world's first and only management toolkit certified for Microsoft System Center Configuration Manager (SCCM).[20] Microsoft SCCM is a widely used management solution to remotely plan, deploy, configure, and monitor a fleet of PCs. MIK is an SCCM plug-in that streamlines security and BIOS administration, as well as image creation, through a modern and intuitive user interface. Even new devices can have security policies automatically applied as soon as they are added to the network. MIK can also prevent users or malware from turning off security protection, and can manage roles (such as for HP Multi-Factor Authenticate).
- For HP printer fleet security, HP JetAdvantage Security Manager is the industry's only policy-based print security compliance tool.[21] Administrators can easily establish a fleet-wide security policy, automate device settings remediation, and install and renew unique certificates. Security Manager can even automatically assess and reconfigure security policies every time a device reboots or when a new device is added to the network. Plus, it can create fleet-wide compliance reports so the security team can see how many printers are at risk.

IT should regularly monitor and audit its environment to make sure no endpoints—including PCs and printers—are left unsecured.

- HP printers and PCs have syslog capabilities to create event notifications for security issues such as intrusion detection, whitelisting, or BIOS events.
- Printer and PC syslog capabilities can be integrated with SIEM (Security Information and Event Management) tools to provide real-time endpoint monitoring to help IT detect and resolve issues. In contrast to most printer manufacturers, HP's print devices can be configured to send security alerts to select SIEM tools, including ArcSight, Splunk, and SIEMonster.
- Data in SIEM tools can be extracted into an Enterprise Governance, Risk and Compliance (eGRC) solution for compliance reporting.

HP Print Security Services and specialists can help with print security assessments, planning, deployment, and ongoing management. HP Print Security Advisory Services can help organizations assess vulnerabilities and compliance, develop a custom print security policy, and make process and technology recommendations for improved security. HP Print Security Governance and Compliance can help organizations maintain security settings compliance across the printer fleet.

Build a better defense today

It's time to take proactive steps to reduce risk and help secure patient data. Security can be complicated, but HP offers hardware and solutions that make it easier for healthcare organizations to protect patients, secure data, address user vulnerabilities, streamline management, improve compliance, and reduce costs.

For more information, or to schedule a thorough risk assessment, contact your HP representative today.

Learn more

HP PC Security: hp.com/go/ComputerSecurity

HP Print Security: hp.com/go/secureprinting

Printing and workflow solutions for healthcare providers: hp.com/go/healthcareworkflow

[1]Spiceworks: HPI Printer Security Research 2016.

[2]Healthcare IT News, "Unencrypted drive with 7 years of patient data stolen from Denton Heart Group", Jessica Davis, March 14, 2017. http://www.healthcareitnews.com/news/unencrypted-drive-7-years-patient-data-stolen-denton-heart-group

[3]Ponemon Study sponsored by HPE "2016 Cost of Cyber Crime Study & the Risk of Business Innovation", 2016.

[4]HIPAA Journal, "Ponemon Institute Publishes 2016 Cost of Data Breach Study", http://www.hipaajournal.com/ponemon-institute-publishes-2016-cost-data-breach-study-3470/, June 16, 2016.

[5]The 2016 Year End Data Breach QuickView report by RiskBased Security, January 2017.

[6]HIPAA Journal, http://www.hipaajournal.com/2017-shaping-up-to-be-another-record-breaking-year-for-healthcare-data-breaches-8761/, April 7, 2017.

[7]HP Sure Start Gen 3 is available on HP Elite Products with Intel® 7th generation processors.

[8]Applies to HP Enterprise-class devices introduced beginning in 2015 and is based on HP review of 2016 published embedded security features of competitive in-class printers. Only HP offers a combination of security features for integrity checking down to the BIOS with self-healing capabilities. A FutureSmart service pack update may be required to activate security features. For a list of compatible products, see hp.com/go/PrintersThatProtect For more information, visit hp.com/go/printersecurityclaims

[9]Healthcare IT News, "500,000 affected in ransomware attack on home medical equipment supplier", Jessica Davis, June 26, 2017. http://www.healthcareitnews.com/news/500000-affected-ransomware-attack-home-medical-equipment-supplier

[10]Verizon, 2016 Data Breach Investigations Report, 2016.

[11]HP Multi-Factor Authenticate requires 7th Generation Intel® Core™ processor, Intel® integrated graphics, and Intel® WLAN.

[12]HP WorkWise smartphone app is available as a free download on the App Store and Google Play. See technical requirements at hp.com/go/workwise

[13]Healthcare IT News, "Breach at BlueCross BlueShield business associate puts data of 3.3 million patients at risk", Jessica Davis, August 8, 2016.

[14]Healthcare IT News, "500,000 affected in ransomware attack on home medical equipment supplier", Jessica Davis, June 26, 2017. http://www.healthcareitnews.com/news/500000-affected-ransomware-attack-home-medical-equipment-supplier

[15]Ponemon Institute, sponsored by Spikes Security, "The Challenge of Preventing Browser-Borne Malware", February 2015.

[16]Average based on global trials conducted by Ponemon Institute during the "Visual Hacking Experiment", 2015, and the "Global Visual Hacking Experiment", 2016, both sponsored by 3M.

[17]Available as a web-download for the HP EliteBook x360 G2; preinstalled on the HP EliteOne 1000 G1, HP EliteBook x360 1020 G2, HP EliteBook 1040 G2 on http://www.hp.com/go/clientmanagement and supports Microsoft® Internet Explorer and Chromium™.

[18]Available on select HP EliteBooks only and requires factory configuration.

[19]HP Secure Erase is for the methods outlined in the National Institute of Standards and Technology Special Publication 800-88.

[20]As of December 5, 2016. See https://partnercenter.microsoft.com/en-us/pcv/solution-providers/hp-inc_4299709950/1221645_1?k=hp HP Manageability Integration Kit is not preinstalled, available at hp.com/go/clientmanagement

[21]HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager Competitive claim based on HP internal research on competitor offerings (Device Security Comparison, January 2015) and Solutions Report on HP JetAdvantage Security Manager 2.1 from Buyers Laboratory LLC, February 2015.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA7-0931ENW, September 2017