FORESCOUT

White Paper

Rampant Confusion Affects the Security of Medical Devices and Healthcare Networks

Healthcare IT and clinical engineering teams are responsible for both enabling and securing all the clinical technology that healthcare providers rely on as they interact with and care for their patients. They need to ensure the technology functions as it should, and that the data of patients, providers and the organization is protected from loss and cyber incidents—especially data that is subject to breach notification rules. Given the complexity of the IT environment and the regulatory landscape within healthcare, this is far from a straightforward task.

The level of support the IT team generally provides to protect the infrastructure is often limited when dealing with clinical devices. There is much confusion around what the clinical engineering team can and cannot do to their equipment and services to maintain compliance with regulatory requirements, which can be at odds with an organization's own IT policies and best practices.

For example, despite the directive from the U.S. Food and Drug Administration (FDA) that regulated medical equipment with off-the-shelf software must be kept up to date in accordance with industry best practices, clinical engineering teams struggle to determine what can and cannot be patched. It is often not clear which equipment can be updated and maintained internally, and which requires vendor involvement.

It may be that a vendor stipulates that FDA regulations do not allow patching, as it would invalidate the FDA certification.

At the same time, the clinical engineering team is often getting pressure from the organization's information security group, which is responsible for ensuring devices meet baseline requirements to maintain the integrity and confidentiality of data and electronic patient health information (ePHI), as well as confirm that all instructions performed by the devices are appropriate. They may insist that patches on a device be installed before access to network resources is allowed. Failure to do this may create periods of time when the devices are not allowed on the network because of non-compliance with the organization's policies.

The clinical engineering team often finds itself in an untenable position—caught between industry compliance requirements and information security policies. Both are designed to improve security, yet the guidelines of one can be at odds with the other. In December 2014, the U.S. Department of Health and Human Services (HHS) released a "BULLETIN: HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software," which highlights the difficult position clinical engineers can sometimes be put in as they try to secure clinical technology.

Ending the Confusion to Effectively Secure Clinical Devices

To increase the effectiveness of the security measures within healthcare networks, clinical engineering teams need to navigate the variety of policies, objectives and mandates that influence what they can and cannot do. The first step is to understand the parameters within which healthcare networks must operate to ensure the network is kept up to date and in compliance. A good place to start is to understand the FDA's guidance on the issue:

21 CFR 807.81(a)(3), 814.39

21 CFR 807.81(a)(3), 814.39 states that, "for medical devices cleared for market under the 510(k) program, you may refer to our guidance entitled, "Deciding When to Submit a 510(k) for a Change to an Existing Device."[1] That guidance explains that a new 510(k) submission to the FDA is necessary for a change or modification to an existing medical device if:

- The medical device has a new or changed indication for use (for example, the list of diseases or conditions the medical device is intended to treat has been altered or amended) or
- The proposed change could significantly affect the safety or effectiveness of the medical device (for example, modification in design, energy source, chemical composition, or material)

21 CFR 820.100

In 21 CFR 820.100, the FDA stipulates that healthcare IT groups must "systematically analyze sources of information and implement actions needed to correct and prevent problems."[2] This broad mandate compels support teams to make sure that minimum baselines are established and maintained across a healthcare network, including the identification and tracking of clinical engineering devices.

Safety Communication

In June 2013, the FDA released a Safety Communication citing that "Recently, the FDA has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations."[3] Some of the vulnerabilities and incidents cited by the FDA include:

- Network-connected/configured medical devices infected or disabled by malware
- Failure to provide timely security software updates and patches to medical devices and networks and an inability to address related vulnerabilities in older medical device models
- Security vulnerabilities in off-the-shelf software designed to prevent unauthorized device or network access, such as plain-text or no authentication, hard-coded passwords, documented service accounts in service manuals, and poor coding/SQL injection

FDA guidance take-aways: What does all the FDA's guidance mean for healthcare IT practitioners? It means patches and baseline security software such as antivirus and encryption software are expected to be deployed unless the FDA changes the indicated use of the device or significantly increases its risk profile. It also means that manufacturers must remediate vulnerabilities in their equipment. If a manufacturer pushes back against patch requirements, healthcare IT teams can authoritatively direct them to this guidance. Additionally, in cases when the vendor is contractually obligated to perform maintenance tasks to a clinical system, this guidance can be leveraged to ensure they are responding in a timely manner. Timeliness is incredibly important with regard to healthcare devices and networks in ensuring the integrity and privacy of sensitive patient information and health records, as a breach can trigger notification rules and significant costs for the organization.

Breach Notification Protection for Healthcare: Safe Harbor

The Health Information Technology for Economic and Clinical Health (HITECH) Act has altered the breach disclosure landscape. The final rule[4] of the HITECH Act puts the burden of proof squarely onto the covered entity or business associate. In the event of a breach, it is their responsibility to prove the data is unusable and therefore cannot cause harm to affected individuals. With the final rule, a *possible* breach is now presumed to *be* a breach, unless the covered entity or business associate can demonstrate there is a low probability the protected health information has been compromised, based on a risk assessment of at least the following factors:

(1) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(2) The unauthorized person who used the protected health information or to whom the disclosure was made;

(3) Whether the protected health information was actually acquired or viewed; and

(4) The extent to which the risk to the protected health information has been mitigated.

Factor 1 — What was the nature and extent of PHI involved?

- Assess whether data of a sensitive nature was involved, such as credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud
- Evaluate whether or the extent to which detailed clinical information was involved, such as treatment plans, diagnoses, medications, medical histories and test results

Factor 2 — Who disclosed the PHI and to whom was the disclosure made?

- Consider the risk of re-identification within the context of whether the unauthorized person who received the information has obligations to protect the privacy and security of the information. For example, if the unauthorized person who received the information has obligations to protect the privacy and security of the information under the HIPAA Privacy and Security Rules or another Federal agency requirement, there may be a lower probability that the protected health information has been compromised.
- Determine whether the unauthorized person who received the protected health information has the ability to re-identify the information, such as when an employee's dates of health care service and diagnosis was impermissibly disclosed to their employer, and the employer can then identify the employee based on HR information. In this case, there may be more than a low probability that the PHI has been compromised.

Factor 3 — Was the PHI actually acquired or viewed?

- If a covered entity mails PHI to the wrong recipient, who opens the envelope and calls to complain, the information has been viewed and a breach certainly occurred
- If a laptop is lost or stolen, but forensic evidence indicates that the PHI it contains was not accessed, viewed, acquired, transferred, or otherwise compromised, the covered entity could determine that the information was not actually acquired by an unauthorized individual even though the opportunity existed

Factor 4 — To what extent has the risk to PHI been mitigated?

- Attempt to mitigate the risks following any impermissible use or disclosure
  - o Obtain satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed
  - o Assurances of an employee, affiliated entity, business associate, or another covered entity that information received in error was destroyed are generally reliable, but such assurances from certain third parties may not be sufficient.

Many healthcare organizations make use of data encryption to render data unusable, hence taking advantage of the "Safe Harbor" provision in the Final HITECH Rule. In 74 FR 42740, the HSS allows data to be deemed unusable if it is encrypted and, therefore, unusable if it is lost. Part of a "Safe Harbor" strategy for healthcare is to show that all endpoints that may store ePHI are encrypted, so that in the event of loss, the organization's breach disclosure process is not triggered.

While organizations are limited in their capacity to deploy encryption on some clinical engineering devices, it can have a tremendous impact on laptops and desktops in the environment.

A review of the data published on the HIPAA Wall of Shame highlights how impactful this single control can be at keeping an organization from losing data and disclosing a breach.

Total on Wall of Shame – 11/10/2015	1, 187
Number caused by laptops, desktops, mobile devices, and servers (non hacking related)	696
Percentage of disclosures that would have been eliminated by using encryption	58.64%

With fines for PHI breaches reaching into the millions of dollars per incident, it is noteworthy that these risks can be almost completely mitigated by producing documentation as evidence that data on the device was encrypted when it was lost or stolen. To help quantify this avoidable risk, the table below lists the fines from HHS, which demonstrate the severity of the fines being levied:

Company	Fine
Cignet	$4.3 million[5]
Alaska DHHS	$1.7 million[6]
WellPoint	$1.7 million[7]
Blue Cross Blue Shield of Tennessee	$1.5 million[8]
Affinity Health Plan	$1.21 million[9]
Cancer Care Group	$750,000[10]
Idaho State University	$400,000[11]
Shasta Regional Medical Center	$257,000[12]

Source: Dept. Health & Human Services — Case Examples and Resolutions

Healthcare organizations that are required to disclose breaches are also faced with non-fine related costs as well, stemming from credit protection services, public notifications, legal suits, public relations activities and brand/reputational damage to reputations.

Guidance from HHS/FTC

To determine when information is "unsecured" and notification is required by the HHS and Federal Trade Commission (FTC) rules, HHS has issued an update to its guidance specifying encryption and destruction as the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Entities that secure health information as specified by the guidance are not required to notify in the event of a breach.[13]

How Forescout CounterACT™ Can Help

Healthcare organizations are utilizing Forescout CounterACT™ to solve some of the most challenging issues facing healthcare IT today. At the core, CounterACT provides visibility into devices on the network, including laptops, desktops, mobile devices and clinical engineering devices. Conditions are checked and, based upon policy, actions can be taken to remediate non-compliant devices and make network access decisions.

Policy Manager Attributes

Conditions	Actions
Device type of device manufacturer location connection type	**User Communication** send email send to web page open trouble ticket force re-authentication
User name authentication status workgroup email and phone number	**Network Access Control** allow block restrict register guest
Operating System OS type version number patch level services and processes	**OS Remediation** install patch configure registry start or stop process trigger external remediation service
Security Posture anti-malware agents patch management agents firewall status configuration	**Security Agent Remediation** install agent start agent update agent update configuration
Applications installed running version number	**Application Control** stop or stop application update application
Peripherals type of device manufacturer connection type	**Peripherals Control** disable peripheral
Network Traffic malicious traffic traffic source & destination rogue DHCP or NAT behavior	**Network Protection** block malicious traffic quarantine malicious device

Comprehensive Visibility into Network Devices

If healthcare IT and clinical engineering teams do not have visibility into what is happening on their networks, they cannot work to effectively secure them. Moreover, in the face of today's increasingly sophisticated threat landscape and costly regulatory requirements, they can't afford to be caught unaware. They need to know about all:

- Authorized and unauthorized users (employees, guests, contractors)
- Authorized and unauthorized devices (computers, wireless access points, handheld phones, USB memory devices, printers and more)
- Authorized and unauthorized applications
- The security configurations and posture of all devices on the network

The information provided by agent-based security systems (Symantec®, McAfee®, Trend Micro™, Sophos and others) or patch management systems (BigFix, Lumension®, Microsoft® and others) is often incomplete and incorrect, because the effectiveness of these systems is typically limited to monitoring corporate-owned devices that have functioning agents. As a result, security teams typically have little to no visibility into the existence, let alone the security posture, of employee-owned devices, including:

- Personal laptops
- Smartphones
- Tablet computers
- Smart printers (those containing embedded operating systems)
- USB memory sticks and other peripheral devices
- Medical equipment

Forescout CounterACT is a network security appliance that provides IT organizations with the unique ability to see devices, such as computers, switches, VoIP phones, printers, personal smartphones, rogue wireless access points and USB drives and devices the instant they connect to the network. It delivers the most granular host interrogation engine in the industry, giving healthcare IT and clinical engineering teams the endpoint information and configuration details they need to consistently secure information and comply with regulations. CounterACT automatically builds a profile on each endpoint that includes:

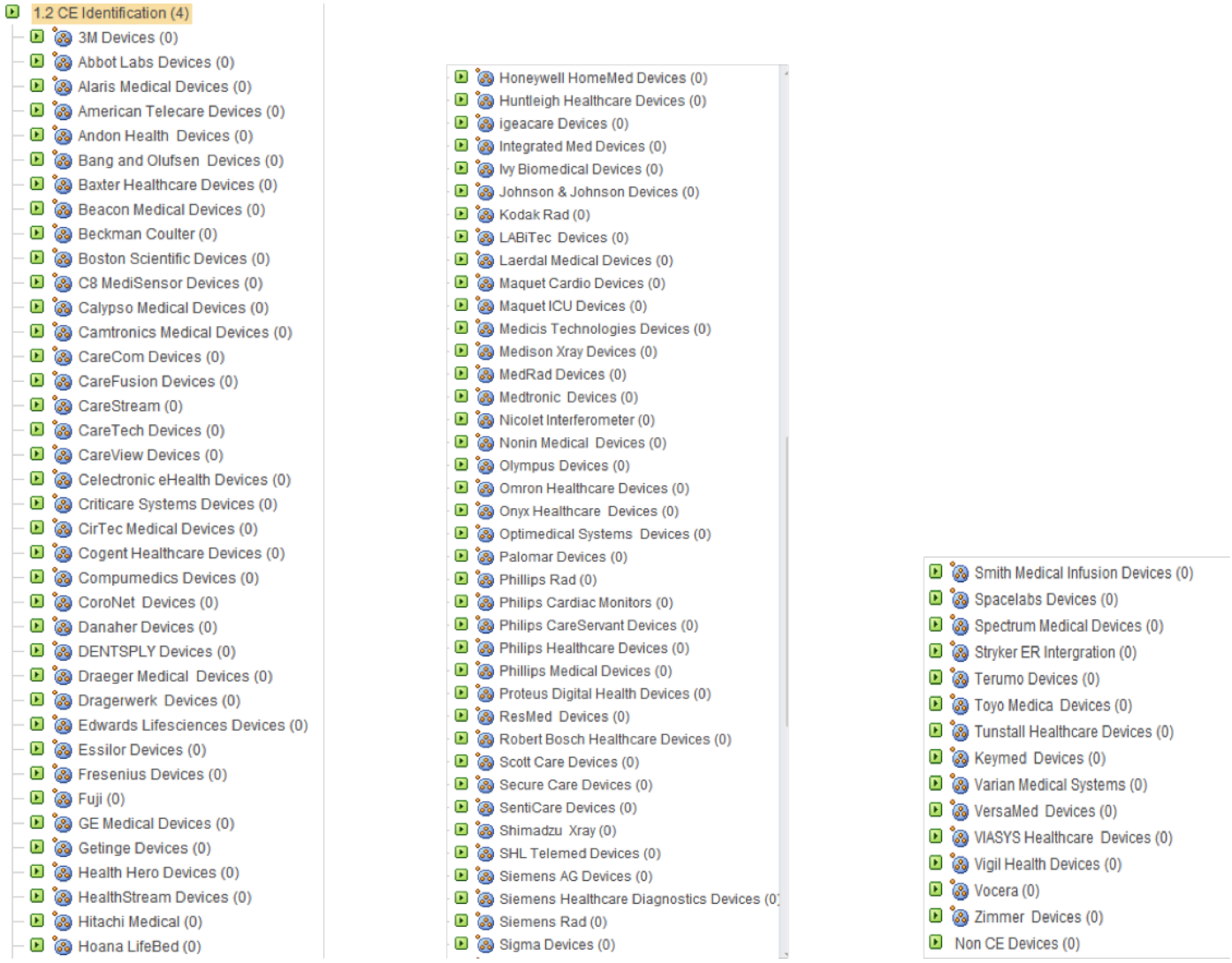
- Identity of the person who logged on (user id)
- User's behavior once logged in to the system
- Operating system of the device
- Applications running on the device
- Patch levels for software on the device
- Status of security agents (running or not running) on the device
- Endpoint-connected devices, such as USB drives
- Network-connected mobile devices, such as smart phones

Identification of Clinical Engineering Devices

As noted earlier, clinical engineering devices pose a special challenge to healthcare organizations. The good news is that the custom policy engine of CounterACT not only makes it possible to identify devices based on any known characteristic, it also identifies thousands of the most frequently deployed medical devices from nearly 100 manufacturers. This makes identification of most medical devices automatic and provides clinical engineering teams the data they need, when they need it, to see what devices are connected to the network for inventory tracking and remediation purposes.

New device classes are being added all the time, saving healthcare IT teams valuable time by providing them an accurate, real-time inventory of medical devices in accordance with FDA and HIPAA requirements.

Here's a sampling of some of the clinical devices CounterACT can quickly and accurately inventory:



Identification of Unpatched and Unsupported Software

Forescout CounterACT can identify non-compliant devices and users, revealing where they are and how they are in violation of the healthcare organization's security policies. A few examples of security posture information that CounterACT can evaluate are:

- Anti-malware agent status (installed/running)
- Anti-malware signature version
- Patch management agent status (installed/running)
- Operating system vulnerabilities
- Firewall status (installed/running)
- Processes and services installed or running
- Registry and configuration
- Applications installed/running
- P2P/IM clients installed/running
- Peripheral devices (type, make, model)
- Malicious traffic (worm propagation, device spoofing, intrusion and spam)
- Rogue NAT/DHCP behavior

Healthcare organizations can leverage CounterACT's ability to monitor compliance of all devices connected to the network, and then, if desired, automatically take action to remediate non-compliant systems. Forescout CounterACT enables a wide range of corrective actions, ranging from the light touch of a user notification email to a more aggressive action, such as restricting access to network resources or programmatically installing patches. CounterACT features also aid in other areas of compliance, including data segmentation and peer-to-peer/acceptable use enforcement.

Enforcement, Remediation and Auditing of Encryption and other Security Policies

The CounterACT policy engine provides deep visibility into healthcare environments, allowing healthcare IT and clinical device teams to compare security policy baselines to the actual state of the system. This real-time visibility identifies systems below established baselines and can offer a wide range of remediation options, from simple alerts to fully automatic remediation of those systems.

For example, many of Forescout's healthcare customers utilize a CounterACT policy to ensure encryption standards are being met. This protects the organization with "Safe Harbor," in case of a breach, in that if a device is lost or stolen, the ability to prove the data on said device was unusable allows the healthcare organization to avoid costly breach disclosure notifications.

The policy example below shows how CounterACT is able to detect whether encryption software is properly deployed on an endpoint, as well as confirm the device is encrypted and compliant. Devices found not to be compliant can be remediated by installing the encryption software programmatically or notifying support personnel that there is an issue that needs attention.

CounterACT has other compliance policies to further aid with the identification of malfunctioning agents, such as those used by patch management and antivirus applications, to help healthcare organizations understand and mitigate the risks to their network and patient information and records. Additionally, CounterACT can provide controls to validate password-aging policies and auto-login PCs that may be used in some clinical environments.

To learn more about how the Forescout CounterACT solution can improve your healthcare organization's security and regulatory compliance, please contact Forescout today.

About Forescout

Forescout Technologies, Inc. is transforming security through visibility. Forescout offers Global 2000 enterprises and government organizations the unique ability to see devices, including non-traditional devices, the instant they connect to the network. Equally important, Forescout lets you control these devices and orchestrate information sharing and operation among disparate security tools to accelerate incident response. Unlike traditional security alternatives, Forescout achieves this without requiring software agents or previous device knowledge. The company's solutions integrate with leading network, security, mobility and IT management products to overcome security silos, automate workflows and enable significant cost savings. As of October 2015, more than 2,000 customers in over 60 countries improve their network security and compliance posture with Forescout solutions.

Learn more at
www.Forescout.com

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591

1 http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm080235.htm
2 http://www.fda.gov/RegulatoryInformation/Guidances/ucm077812.htm
3 http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm
4 http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
5 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cignetcmp.html
6 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/alaska-agreement.html
7 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/wellpoint-agreement.html
8 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/bcbstagrmnt.html
9 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/affinity-agreement.html
10 http://www.hhs.gov/about/news/2015/09/02/750,000-dollar-hipaa-settlement-emphasizes-the-importance-of-risk-analysis-and-device-and-media-control-policies.html
11 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/isu-agreement.html
12 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/shasta-agreement-press-release.html
13 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf