FORESCOUT

Address the HIPAA Security Rule with ForeScout

Make HIPAA Security Rule Compliance a Reality with CounterACT®

Organizational Challenges

- Protect electronic information as mandated by HIPAA's Administrative, Physical and Technical safeguards
- Enable continuous monitoring and mitigation capabilities that leverage existing investments
- Ensure information protection through device and user access controls
- Facilitate streamlined network access and information sharing for trusted contractors, partners, patients and vendors
- Secure information from traditional systems (such as PCs, laptops) as well as Bring Your Own Device (BYOD) and Internet of Things (IoT), including network-connected medical devices

Technical Challenges

- Discover traditional, BYOD, rogue devices and medical IoT devices
- Control access to confidential and sensitive data
- Prevent infected or non-compliant devices from spreading malware or viruses across the network
- Defend against targeted attacks that can steal data or force network downtime
- Measure effectiveness of security controls and demonstrate compliance with HIPAA regulations

Security Standards for the Protection of Electronic Protected Health Information, commonly known as the Security Rule, were adopted to implement provisions of HIPAA relating to the information in electronic format.[1] This rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity.[1] Three parts of that rule: the Administrative, Physical and Technical safeguards, are addressed herein.

Administrative safeguards cover the administrative actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Physical Safeguards deal with implementing reasonable and appropriate physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Technical safeguards deal with implementing technology and the policy and procedures for its use that protect electronic health information and control access to it.

These controls should be part of the core understanding of any organization's defense and/or architecture that helps to protect the systems that are organizationally defined or established. ForeScout CounterACT® can be leveraged for this type of high-level, organization-wide control to track the devices and their users that connect to organizations' networks.

Protecting Healthcare Provider Organizations with ForeScout CounterACT

Many healthcare organizations today are unable to enforce cybersecurity policies across the enterprise, and consequently, find it difficult to protect electronic health records. A key reason for this is the fact that devices that lack security agents come and go from the network at will and are largely undetected by periodic, point-in-time vulnerability scans. Another reason is that many security systems work in silos and threats go undetected. This gap in security policy enforcement puts the entire network and the information it holds in jeopardy.

To make matters worse, IoT adoption is increasing network attack surfaces exponentially by opening up more entry points for stealing protected electronic health records.

In 2016, 450 healthcare breach incidents were reported and 27 million records were breached.[2] Many healthcare organizations were victims of ransomware attacks and had to pay cybercriminals to get their data back.[3]

ForeScout CounterACT can help prevent such attacks. It helps organizations build and maintain a secure network, drive a vulnerability management program, implement strong access control measures, monitor and test networks and maintain an information security policy. It can be leveraged for organization-wide control to track devices and their users within legacy, new and highly technical network infrastructure without reengineering the established network or disrupting services. The CounterACT platform provides administrators with the critical ability to see and monitor devices on the network, from endpoints such as PCs, laptops and printers, to IoT devices (including network-connected medical systems) and personally owned smartphones and tablets. CounterACT can also enforce network access policies across the network hierarchy, from switches to access and distribution layers.

Many medical IoT devices are especially vulnerable since they cannot host third-party security agents, run outdated or unsupported operating systems, cannot be patched and often lack even the most basic security features. ForeScout CounterACT helps overcome these limitations with its agentless approach and its support for heterogeneous systems.

In addition to playing a critical role in securing devices and networks, the CounterACT platform can also orchestrate and enable a variety of security tools to share information and work together. This orchestration allows enterprises to integrate and automate their security responses while also helping them to support compliance and standardization goals as well as preserving their investments in existing security tools. The bottom line is that CounterACT sees IP-addressable endpoints, manages those endpoints through policies and rule sets, and integrates with current security tools to help meet requirements for continuous monitoring, enable security procedures, and implement automated responses to secure and protect electronic health records.

ForeScout CounterACT and HIPAA Compliance

CounterACT supports the HIPAA Administrative, Technical and Physical safeguards as described below.

Administrative Safeguards

- **Security Management Process:** Enables creation of risk assessment policies and procedures to assess the potential impact of damage due to unauthorized access of information systems. Enables securing of less obvious sources of information such as BYOD and IoT devices. Enables application of appropriate sanctions, such as limiting or denying network access to workforce members and devices that fail to comply with the security policies and procedures of the covered entity. Enables implementation of procedures to allow for review of information system activity, such as audit logs, access reports and security incident tracking reports.

  CounterACT can continuously acquire, assess and take action on new information in order to identify vulnerabilities, remediate non-compliant or compromised devices and minimize the window of opportunity for attackers.

- **Workforce Security:** Enables implementation of policies and procedures to help ensure that authorized members of an organization's workforce and relevant devices have appropriate access to electronic protected health information while preventing unauthorized workforce members and devices from obtaining access to electronic protected health information.

- **Information Access Management:** Enables implementation of security policies and procedures, change control, monitoring and configuration changes, and access restrictions. Dynamic network segmentation capability enables creation and modification of policies and procedures that restrict access to the electronic health information within a subgroup or among subgroups. Isolating healthcare clearing house functions is an example of this segmentation. Enables implementation of policies and procedures that, based upon the entity's access authorization policies, establish and modify a user's right of access to a workstation, transaction, program or process. Employees can be dynamically assigned to Virtual Local Area Networks (VLANs) that are appropriate for their roles. An example of this is allowing only network administrators to access the networking infrastructure.

- **Security Incident Procedures:** Enables detection of malicious activity using CounterACT's threat protection engine. Can integrate with third-party advanced threat detection (ATD) and security information and event management (SIEM) systems. Insights gained through these processes can provide actionable threat information that CounterACT's policy manager can use to isolate or initiate remediation actions.

  Once CounterACT discovers a security problem on an endpoint, its sophisticated policy manager can automatically execute a range of responses depending on the severity of the problem. It can also prevent infected or non-compliant devices from spreading malware or viruses across the network by sending alerts to administrators, putting infected devices in quarantine, and repairing them. When repairs are complete, CounterACT can restore appropriate access and scan other endpoints for the same indicators of compromise (IOCs). Minor violations might result in a warning message sent to the end-user.

  CounterACT's remediation capabilities can be further extended with scripts that run on non-compliant hosts to fix violations. If a CounterACT scan finds that a device's operating system or key applications are missing critical patches, it can trigger an update by the patch management system. When repairs are complete, CounterACT can restore authorized access.

In the event of an incident, responders can analyze logs and other data collected on the endpoint's activities to assess security status, access records, assess patch level, assess installed applications and other information to provide context to the event, which can all assist the responder in determining and implementing the appropriate incident-response activities, including remediation and follow-up. This data can be found in the real-time contextual database of endpoint state and activity that CounterACT can build through its own device inspections and through its integrations with other management and security technologies.

Technical Safeguards

- **Access Control:** Enables limitation of access to healthcare information systems to authorized users, processes administered on behalf of authorized users or specified devices/information systems. Can integrate with a variety of third-party authentication systems to validate unique identity and users prior to providing role-based network access.

  For managed devices, CounterACT can identify the users currently logged in and their account types. It compares these with policies for the device and user. If discrepancies are found, CounterACT can restrict or deny access.

  CounterACT can facilitate streamlined network access and information sharing for trusted contractors, partners, patients and vendors. Employees and contractors who bring their own devices can be redirected to an automated onboarding portal. Serious violations could result in actions such as blocking or quarantining the device.

  When a remote device requests a network connection, CounterACT's initial scan can identify the type of connection and restrict or deny access if the endpoint posture is compromised. At the same time, it can evaluate the device configuration, installed software and patch levels for compliance with security policy.

  If a CounterACT scan finds that the operating system or key applications are missing critical patches, it can trigger an update by the patch management system. When repairs are complete, CounterACT can restore authorized access. If the device is non-compliant, CounterACT can deny access or quarantine it for remediation.

  CounterACT can also initiate an immediate vulnerability assessment (VA) of new network devices using its own scanning capabilities or those of partner solutions.

  As devices connect to an enterprise network, CounterACT collects a broad range of asset data as a basis for granting or denying access. These data include:

  - the type of device, including its operating system (Windows®, Macintosh®, Linux®, iOS® or Android™), whether the device is physical or virtual, and whether it's a non-user device such as a printer, Voice over Internet Protocol phone, security or manufacturing system, or medical or point-of-sale device;
  - the identity of the connecting user, allowing you to distinguish between employee, partner, contractor and guest devices;
  - whether the device is owned by the organization or the user;
  - where the device is connecting, and the connection type (wired, wireless, VPN); and
  - the device's IP address, MAC address, switch port, SSID and VLAN.

  CounterACT can actively manage (inventories, tracks and corrects) software on the network so that only authorized software is installed and executed while unauthorized and unmanaged software is found and prevented from installation or execution.

  CounterACT can install, update, re-start and re-configure various security and management agents such as those responsible for malware detection, encryption, firewall, DLP and patch management to enable data encryption and protection.

- **Audit Controls:** Enables enforcement of appropriate use policies for network and information systems. Enables implementation procedures to enable reviewing of information system activity, such as audit logs, access reports and security incident tracking reports. Enables organizations to audit information system use and validate standards compliance by producing documents and reports. When a device requests network access, the ForeScout platform's initial inspection can determine whether logging is enabled and how it is configured, including the chosen location for log storage.
- **Integrity:** Enables implementation of policies and procedures to protect electronic protected health information from improper alteration and destruction by limiting access to authorized users. CounterACT also protects data from inappropriate third-party modifications by facilitating streamlined network access and information sharing for trusted contractors, partners, patients and vendors.
- **Person or Entity Authentication:** Can address person, device and host identification and authentication, authenticator management, feedback and cryptographic authentication.

  CounterACT can facilitate streamlined network access and information sharing for trusted contractors, partners, patients and vendors. Employees and contractors who bring their own devices can be redirected to an automated onboarding portal. Serious violations could result in actions such as blocking or quarantining the device.

Just as CounterACT scans connecting endpoints to assess their configuration and inventories installed services, it can also conduct similar evaluations of network devices and network-based security infrastructure.

- **Transmission Security:** Enables creation of policies and procedures that reflect required standards and guidance that enforce monitoring and control communications at external and internal boundaries in the system.

Physical Safeguards

- **Workstation Use:** Enables implementation of policies to enable or disable access to specific workstations containing protected information from other systems or devices based on their roles. Can actively manage (inventories, tracks and corrects) all hardware devices on the network and their locations so that only authorized devices are given access, while unauthorized and unmanaged devices are found and prevented from gaining access.

  Enables the establishment, implementation and active management (tracks, reports on and corrects) of the security configurations of laptops, servers and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

- **Device and Media Controls:** To support a host-based backup protection security strategy, CounterACT can help ensure that relevant third-party protection software is installed, correctly configured and operational. Connecting devices can be evaluated as part of CounterACT's access inspection and non-conforming hosts can be quarantined or removed from the network until repaired. CounterACT can identify open ports, active protocols and services currently running, and compare that inventory with configuration policies for that host. It can also restrict or deny access for non-compliant devices and issue a user notification or remediation alert.

CounterACT Security Platform: Key Capabilities

The ForeScout CounterACT security platform provides real-time monitoring, control and policy-based remediation of managed, unmanaged and non-traditional devices to support your compliance efforts with HIPAA standards. Here's how:

See. Detects devices the instant they connect to the network without requiring agents. Profiles and classifies devices, users, applications and operating systems. Continuously monitors managed devices, BYOD devices and IoT endpoints.

Control. Allows, limits or denies network access based on device posture and security policies. Assesses and remediates malicious or high-risk endpoints. Helps to enforce compliance with industry mandates and regulations, including HIPAA standards.

Orchestrate. Shares contextual insights and data with IT security and management systems. Automates common workflows, IT tasks and security processes across systems. Accelerates system-wide response to quickly mitigate risks and data breaches.

FORESCOUT

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] https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html?language=es
[2] http://www.beckershospitalreview.com/Healthcare-information-technology/2016-averaged-1-healthcare-data-breach-per-day.html
[3] http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html