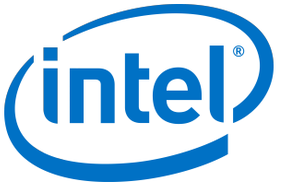


Health & Life Sciences Breach Security Assessment Report

For Star Healthcare

Fictitious organization and assessment data. For demo purposes only.

Contents

Reported On	Friday, 29 Apr 2016 09:22 PDT
Assessed On	Monday, 1 Feb 2016 11:18 PST
Organization	Star Healthcare Provider, United States
Account Manager	Kathy Trustworthy Senior Account Manager MindLeaf 123 456 7890 Kathy.Trustworthy@MindLeaf.com
Assessor	Joe Whitehat CISSP Senior Solutions Engineer MindLeaf Joe.Whitehat@MindLeaf.com
Assessments	8

Executive Summary

Breaches are the top privacy and security concern in Health & Life Sciences organizations, according to global Intel research conducted in 2015. This report highlights the results of an assessment of your organizations breach security capabilities. It also compares your breach security maturity, priorities across breach types, and your breach security capabilities with the rest of the Health & Life Sciences organizations that have also been assessed up to the time of this report. This is a pilot program running throughout 2016, led by Intel in collaboration with a broad range of partners working in the Health & Life Sciences Industry. We welcome your feedback both on the pilot program in general, and on this report.

This Health & Life Sciences breach security assessment is a high level survey of potential breach security issues and is intended to inform participants where they stand on selected security practices in relation to other similar participants in this study, and is not intended to replace participants other compliance or security due diligence activities. It is also different from and complementary to risk assessments that are required by several regulations and security standards. It provides an opportunity to look at gaps and next steps that can be taken to improve breach security posture. Improvements to breach security based on this assessment may also help with compliance with privacy and security regulations, data protection laws, and standards. Please consult publicly available information on your applicable regulations, laws and standards for further information.

42 breach security capabilities were assessed in this engagement. Star Healthcare has 75% of the capabilities in the Baseline maturity level (7% behind average), 46% in Enhanced (13% behind average), and 29% in Advanced (1% ahead of average). The breach security maturity level of Star Healthcare peaks in the Baseline level. See Breach Security Maturity for further details on the assessment of the breach security maturity level of Star Healthcare, and how this compares with the broader Health & Life Sciences Industry.

At Star Healthcare, Cybercrime Hacking, Malicious Insiders or Fraud, and Ransomware are considered High priority. Loss or Theft of Mobile Device or Media, Insider Accidents or Workarounds, Business Associates, and Insider Snooping are considered Medium priority. Improper Disposal is considered Low priority. 3 of these priorities are significantly different from the average priorities assigned by other Health & Life Sciences organizations to these

breach types. See Breach Type Priorities for further details on priorities assigned by Star Healthcare to various breach types, and how these priorities compare to the Health & Life Sciences Industry.

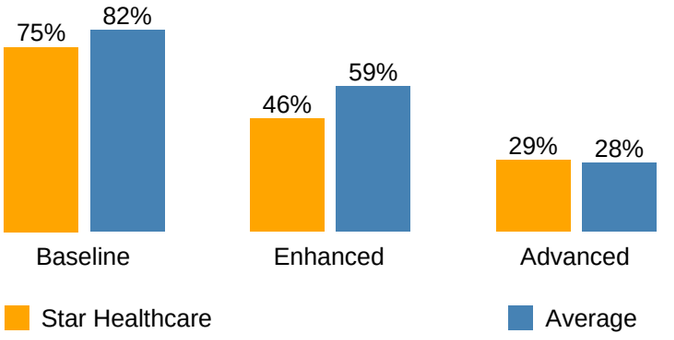
In the Baseline maturity level, Star Healthcare was behind the average in 7 capabilities: User Awareness Training, Mobile Device Management, Anti-Malware, Email Gateway, Web Gateway, Vulnerability Management, Patching and Backup and Restore. In the Enhanced maturity level, Star Healthcare was behind the average in 8 capabilities: Device Control, Penetration Testing, Vulnerability Scanning, Network Data Loss Prevention (Discovery Mode), Multi-Factor Authentication with Timeout, Secure Remote Administration, Network Intrusion Prevention System, Business Associate Agreements and Virtualization. In the Advanced maturity level, Star Healthcare was behind the average in 2 capabilities: Network Data Loss Prevention (Prevention Mode) and Security Information and Event Management. See Breach Security Maturity Model for how Star Healthcare was assessed across 42 breach security capabilities in the maturity model, and how this compares with the Health & Life Sciences Industry.

30 gaps in breach security capabilities were identified during this assessment. These capabilities represent new opportunities for improvements by Star Healthcare to improve its breach security posture and further mitigate risk of breaches. These capabilities may also improve usability, reduce cost, and improve efficiency of IT operations. For details on specific gaps and opportunities for improvement see Breach Security Gaps and Opportunities for Improvement . It is recommended that Star Healthcare review these opportunities and specific products, technologies and services that can help together with the account manager and assessor listed at the beginning of this report.

Thank you for participating in the Intel Health & Life Sciences Breach Security Assessment Program Pilot. We welcome any updates you may have on your breach security to ensure the accuracy of your assessment and this report. Please coordinate any such updates with your assessor. We also welcome your feedback on the overall process, as well as this report.

1. Breach Security Maturity

The percentage of breach security capabilities you have implemented at the various maturity levels. As your breach security posture improves, your assessment at all of these maturity levels will approach 100%. Important aspects to note in this result is what level your maturity peaks at, as well as how your Baseline, Enhanced, and Advanced maturity levels compare with the rest of the Health & Life Sciences Industry.



2. Breach Type Priorities

This assessment analyzed your level of concern or priority across six different types of breaches. These results enable you, for each breach type, to compare your level of concern or priority with the rest of the Health & Life Sciences Industry. For each of the following types of breaches the assessment results reflect the priority or level of concern you assigned to the given type of breach, compared to the Health & Life Sciences Industry. Relevant Capabilities Present shows for each type of breach the percentage of relevant security capabilities currently implemented at Star Healthcare. Readiness Percentile shows for each type of breach the percentile Star Healthcare falls within across all organizations assessed, based on the percentage of relevant capabilities present.

Star Healthcare Breach Type Priorities

#	Breach Type	Priority	Relevant Capabilities Present	Readiness Percentile	Alerts
2.1	Cybercrime Hacking	High	52%	14%	
2.2	Loss or Theft of Mobile Device or Media	Medium	58%	86%	
2.3	Insider Accidents or Workarounds	Medium	57%	43%	
2.4	Business Associates	Medium	65%	71%	⚠
2.5	Malicious Insiders or Fraud	High	53%	29%	⚠
2.6	Insider Snooping	Medium	53%	57%	
2.7	Improper Disposal	Low	67%	100%	⚠
2.8	Ransomware	High	55%	14%	

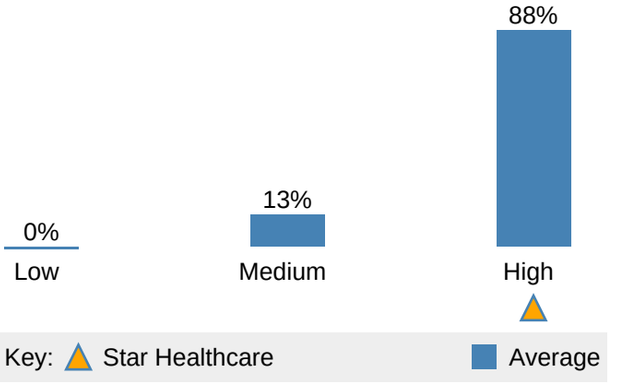
⚠ Star Healthcare priority differs significantly from Health & Life Sciences Industry average

2.1 Cybercrime Hacking

In this type of breach an external hacker accesses your organizations network and obtains unauthorized access to sensitive patient information. A common example of this type of breach starts with the hacker spear- phishing a worker in your organization, resulting in that worker clicking on a malicious link, and leading to drive-by download of malware. The malware then proliferates inside your intranet and key-logs the database administrator database credentials, at which point it turns into a bot that logs into your database containing sensitive patient data and exfiltrates this data "low and slow" to evade detection.

Percentage of relevant capabilities present: **52%**

Readiness percentile: **14%**

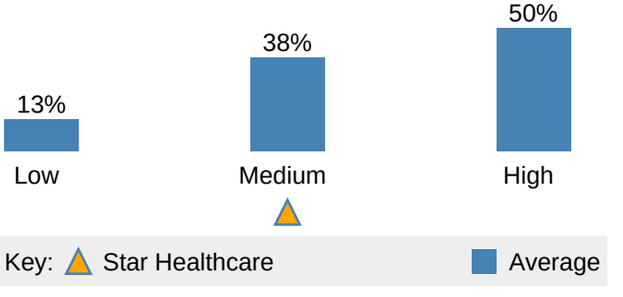


2.2 Loss or Theft of Mobile Device or Media

In this type of breach a worker either loses or has stolen a mobile device or media containing sensitive patient data, resulting in potential unauthorized access to that data and a breach.

Percentage of relevant capabilities present: **58%**

Readiness percentile: **86%**

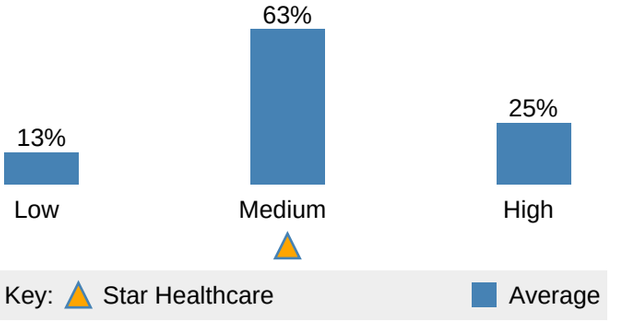


2.3 Insider Accidents or Workarounds

In this type of breach a worker performs a well-intentioned action that results in unauthorized access to sensitive patient information. A common example of this type of breach involves a worker emailing unsecured sensitive patient information, resulting in potential unauthorized access to this information, and a breach. This type of breach can involve the use of either corporate or BYOD devices by workers.

Percentage of relevant capabilities present: **57%**

Readiness percentile: **43%**

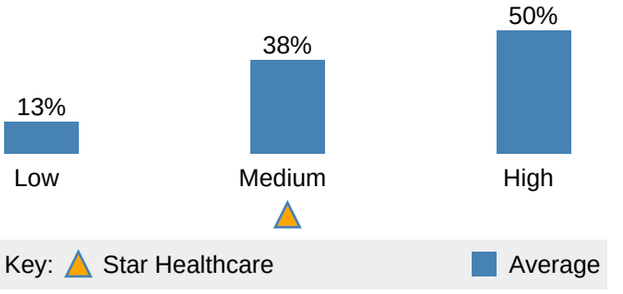


2.4 Business Associates

In this type of breach a third party organization contracted by your organization experiences a breach event involving unauthorized access to sensitive patient information. In this case the patient information impacted originates from your organization and was previously shared for the purpose of the third party organization fulfilling its contractual obligations. In the United States these entities are known as Business Associates, while in Europe they are typically referred to as Data Processors.

Percentage of relevant capabilities present: **65%**

Readiness percentile: **71%**

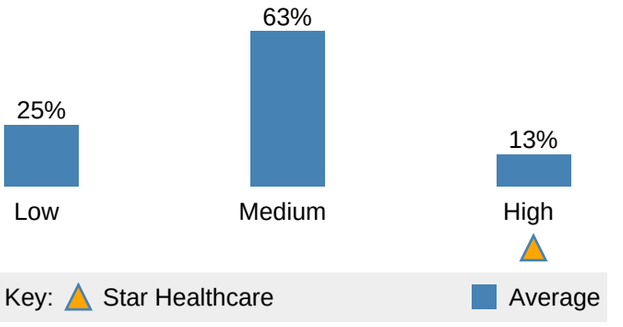


2.5 Malicious Insiders or Fraud

In this type of breach a worker performs a malicious action that results in unauthorized access to sensitive patient information. This could be a disgruntled worker, or done for the purpose of committing fraud. A common example of this type of this breach involves medical claims fraud where a worker files dishonest healthcare claims in order to turn a profit, or sells sensitive patient information on the black market. Prescription fraud and financial fraud are other examples of this type of breach.

Percentage of relevant capabilities present: **53%**

Readiness percentile: **29%**

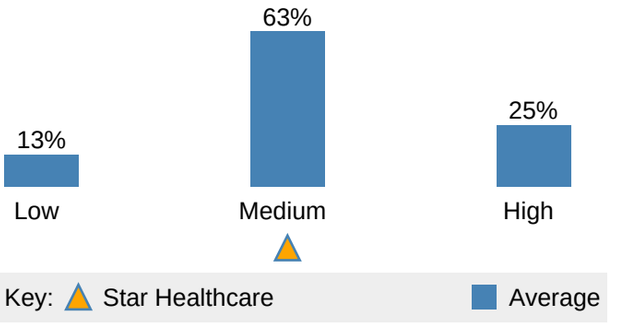


2.6 Insider Snooping

Insider snooping involves a worker accessing the records of patients of your organization without any legitimate need to do so, for example where a patient is not under the direct care of the worker.

Percentage of relevant capabilities present: **53%**

Readiness percentile: **57%**

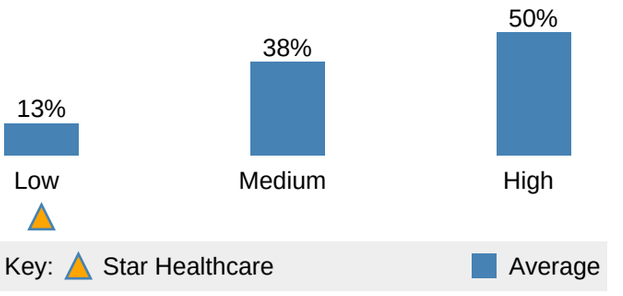


2.7 Improper Disposal

Improper disposal of electronic storage devices or media containing sensitive patient information. Examples of this could include dumping of paper based patient records in a dumpster, or selling electronic devices with stored patient records without first securely wiping them.

Percentage of relevant capabilities present: **67%**

Readiness percentile: **100%**

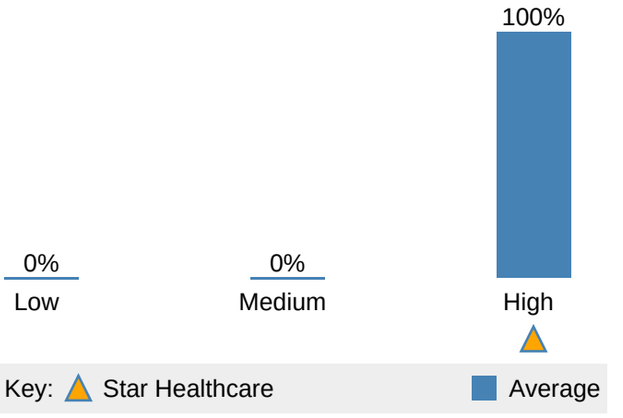


2.8 Ransomware

Ransomware breaches involve malware infections, often through spear phishing and drive by download, where the malware encrypts patient data in electronic form and the hackers behind it withold the decryption keys, typically demanding a ransom. This type of breach compromises the availability of the patient records, and can also involve unauthorized access to patient information, depending on the malware and hacker access to the internal network and data of the health and life sciences organization.

Percentage of relevant capabilities present: **55%**

Readiness percentile: **14%**



3. Breach Security Maturity Model

The capabilities in the maturity model below are directly relevant to mitigating risk of various types of breaches. Each capability is classified into the Baseline, Enhanced or Advanced breach security maturity levels. On the left of each breach security capability is a circle indicating whether this capability is currently present (🟢), partially present (🟡), or absent (🔴) at Star Healthcare respectively. (⚠) indicates a capability where Star Healthcare is significantly behind the Health & Life Sciences Industry average in implementing the capability.

Star Healthcare Breach Security Maturity

Baseline

- 🟢 Policy
- 🟢 Risk Assessment
- 🟢 Audit and Compliance
- 🟡 ⚠ User Awareness Training
- 🟡 Endpoint Device Encryption
- 🟡 ⚠ Mobile Device Management
- 🟢 Endpoint Data Loss Prevention (Discovery Mode)
- 🟡 ⚠ Anti-Malware
- 🟢 Single Factor Access Control
- 🟢 Firewall
- 🟡 ⚠ Email Gateway
- 🟡 ⚠ Web Gateway
- 🟡 ⚠ Vulnerability Management, Patching
- 🟢 Security Incident Response Plan
- 🟢 Secure Disposal
- 🟡 ⚠ Backup and Restore

Enhanced

- 🔴 ⚠ Device Control
- 🔴 ⚠ Penetration Testing, Vulnerability Scanning
- 🟢 Client Solid State Drive (Encrypted)
- 🟢 Endpoint Data Loss Prevention (Prevention Mode)
- 🔴 ⚠ Network Data Loss Prevention (Discovery Mode)
- 🟡 Anti-Theft: Remote Locate, Lock, Wipe
- 🔴 ⚠ Multi-Factor Authentication with Timeout
- 🔴 ⚠ Secure Remote Administration
- 🟡 Policy Based Encryption for Files and Folders
- 🟢 Server / Database / Backup Encryption
- 🟢 Network Segmentation
- 🟡 ⚠ Network Intrusion Prevention System
- 🟡 ⚠ Business Associate Agreements
- 🟡 ⚠ Virtualization

Advanced

- 🔴 Server Solid State Drive (Encrypted)
- 🔴 ⚠ Network Data Loss Prevention (Prevention Mode)
- 🟡 Database Activity Monitoring
- 🟡 Digital Forensics
- 🔴 ⚠ Security Information and Event Management
- 🟡 Threat Intelligence
- 🔴 Multi-Factor Authentication with Walk-Away Lock
- 🟡 Client Application Whitelisting
- 🟡 Server Application Whitelisting
- 🟡 De-Identification / Anonymization
- 🔴 Tokenization
- 🟡 Business Continuity and Disaster Recovery

(🟢 = present, 🟡 = partially present / in progress, 🔴 = not present / gap, ⚠ = Star Healthcare significantly behind Health & Life Sciences average in implementing capability)

4. Breach Security Gaps and Opportunities for Improvement

Security capabilities for which your implementation was assessed as either "No" (🔴) or "Partial" (🟡) are listed below together with the maturity level of the safeguard, its relevance across breach types, and whether your gap is significantly behind the rest of the Health & Life Sciences organizations assessed. Capabilities that are assessed as not present (🔴) will tend to appear higher on this list that ones assessed as partially present (🟡) . Capabilities that are relevant across more breach types (✓) will tend to appear higher on this list than ones relevant to fewer breach types. Capabilities relevant to breach types that you rated as higher priority will tend to appear higher on the list than those relevant to breach types that you rated as lower priority. Capabilities for which you assessed as significantly behind the Health & Life Sciences average (⚠) will tend to appear higher on the list than ones where your gap is typical across the Health & Life Sciences organizations assessed. This list is not intended to be prescriptive. Please consult your account manager and assessor for further guidance in interpreting these results.

Star Healthcare Breach Security Gaps

#	Security Capability	Assess	Breach Types Mitigated and Star Healthcare Priorities								Behind Industry
			Cybercrime Hacking	Loss or Theft	Insider Accidents	Business Associates	Malicious Insiders or Fraud	Insider Snooping	Improper Disposal	Ransomware	
			High	Medium	Medium	Medium	High	Medium	Low	High	
1	Network Data Loss Prevention (Prevention Mode)	🔴	✓		✓		✓	✓		✓	⚠
2	Secure Remote Administration	🔴	✓	✓	✓		✓	✓			⚠
3	Penetration Testing, Vulnerability Scanning	🔴	✓				✓	✓		✓	⚠
4	Security Information and Event Management	🔴	✓				✓	✓		✓	⚠
5	Device Control	🔴			✓		✓	✓		✓	⚠
6	User Awareness Training	🟡	✓	✓	✓	✓	✓	✓	✓	✓	⚠
7	Vulnerability Management, Patching	🟡	✓	✓	✓		✓	✓	✓	✓	⚠
8	Tokenization	🔴	✓	✓	✓	✓	✓	✓	✓		
9	Network Data Loss Prevention (Discovery Mode)	🔴			✓		✓	✓			⚠

10	Multi-Factor Authentication with Timeout	🔴		✓			✓	✓			⚠
11	Web Gateway	🟡	✓		✓		✓	✓		✓	⚠
12	Email Gateway	🟡	✓		✓		✓			✓	⚠
13	Mobile Device Management	🟡		✓	✓		✓	✓	✓		⚠
14	Backup and Restore	🟡	✓	✓			✓			✓	⚠
15	Digital Forensics	🟡	✓	✓	✓	✓	✓	✓	✓	✓	
16	Anti-Malware	🟡	✓		✓					✓	⚠
17	De-Identification / Anonymization	🟡	✓	✓	✓	✓	✓	✓	✓		
18	Multi-Factor Authentication with Walk-Away Lock	🔴		✓			✓	✓			
19	Server Solid State Drive (Encrypted)	🔴		✓			✓		✓		
20	Threat Intelligence	🟡	✓			✓	✓	✓		✓	
21	Client Application Whitelisting	🟡		✓	✓		✓	✓		✓	
22	Network Intrusion Prevention System	🟡	✓							✓	⚠
23	Server Application Whitelisting	🟡	✓				✓	✓		✓	
24	Policy Based Encryption for Files and Folders	🟡		✓	✓		✓	✓	✓		
25	Endpoint Device Encryption	🟡		✓			✓	✓	✓		
26	Business Continuity and Disaster Recovery	🟡	✓				✓			✓	
27	Database Activity Monitoring	🟡	✓				✓	✓			
28	Anti-Theft: Remote Locate, Lock, Wipe	🟡		✓			✓		✓		
29	Virtualization	🟡		✓							⚠

30	Business Associate Agreements	●	✓	⚠

(● = partially present / in progress, ● = not present / gap, ✓ = relevant to breach type, ⚠ = Star Healthcare significantly behind Health & Life Sciences average in implementing capability)

5. Breach Security Capabilities

This assessment evaluated the presence of 42 breach security capabilities in Star Healthcare . This section defines each capability and shows how Star Healthcare compares with the Health & Life Sciences Industry in implementing each capability.

5.1 Policy

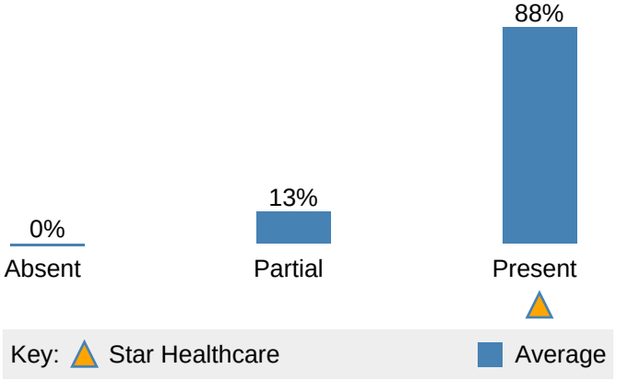
Accurate, complete and up to date security & privacy policy. This is the internal document used to govern employee responsibilities with regard to privacy and security of patient information.

More Info

Notes: Need to update for BYOD.

HIPAA: 45 CFR 164.308(a)

ISO: ISO/IEC 27001:2013 Section 5.2 Policy



5.2 Risk Assessment

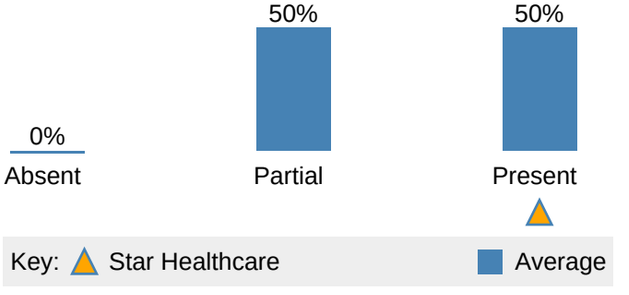
Documented risk assessments done annually.

More Info

Notes: Last one completed about 2 years ago. Not currently done regularly.

HIPAA: 45 CFR 164.308(a)(1)

ISO: ISO/IEC 27001:2013 Section 8.2 Information Security Risk Assessment



5.3 Audit and Compliance

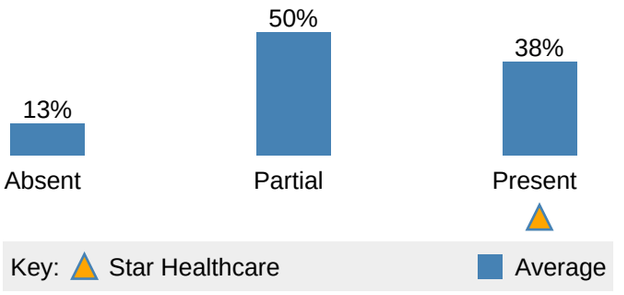
Audit and compliance technology and processes in place to detect and remedy non-compliance with policy.

More Info

Notes: Logging and regular audits done to verify compliance with policy.

HIPAA: 45 CFR 164.312(b)

ISO: ISO/IEC 27001:2013 Section 9.2 Internal Audit



5.4 User Awareness Training

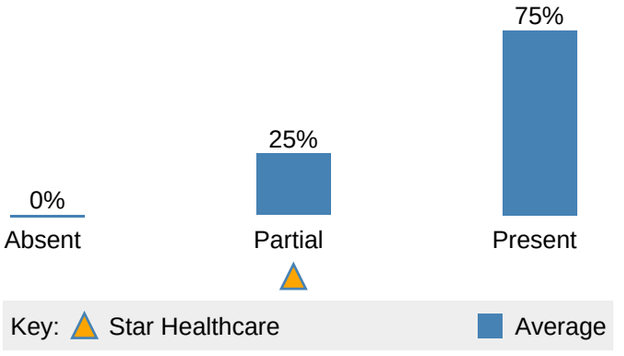
Training of Health & Life Sciences workers on security and privacy. May be implemented at time of hire, change of role, annually, or more frequently. May also be triggered by specific events. More advanced training may use gamified techniques, for example for spear-phishing, to help train Health & Life Sciences workers on the job.

More Info

Notes: New employees trained. Need training on role change and spear phishing.

HIPAA: 45 CFR 164.308(a)(5)

ISO: ISO/IEC 27002:2013 Section 7.2.2 Information Security Awareness, Education and Training



5.5 Endpoint Device Encryption

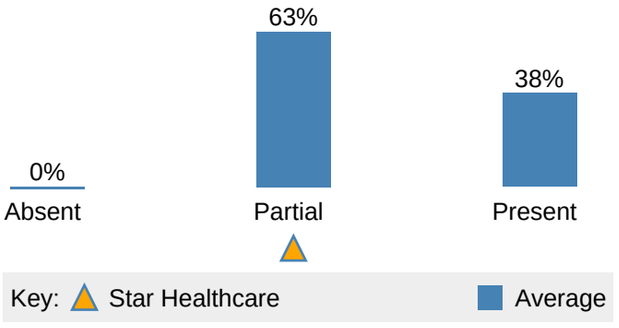
Client devices storing sensitive patient information have encryption of data at rest.

More Info

Notes: Laptops encrypted. Need encryption for smartphones and tablets.

HIPAA: 45 CFR 164.312

ISO: ISO/IEC 27002:2013 Section 10 Cryptography



5.6 Mobile Device Management

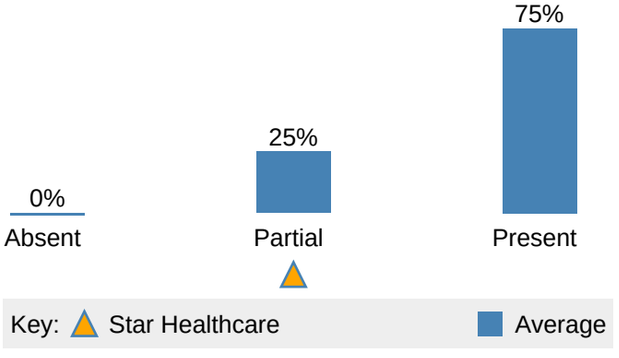
Management of mobile client devices including smartphones and tablets. Often used with BYOD devices. Functionality may include secure container for whitelisted business apps and data with access control and encryption, as well as remote management including remote lock and wipe.

More Info

Notes: Currently in place for BYOD smartphones. Need for corporate smartphones and tablets.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 6.2 Mobile Devices and Teleworking



5.7 Endpoint Data Loss Prevention (Discovery Mode)

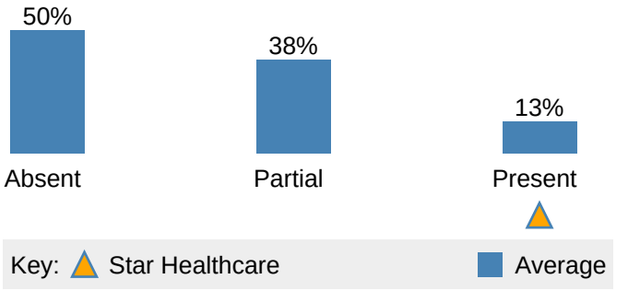
Data Loss Prevention ability to discover and possibly also classify sensitive patient data at rest on clients or servers.

More Info

Notes: Currently used to discover patient data stored on laptops etc.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 18.1.3 Protection of Records



5.8 Anti-Malware

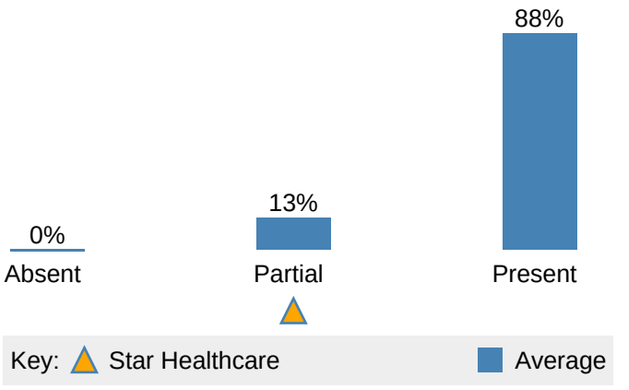
Ability to detect and remediate blacklisted executables. May be signature based or heuristics / behavior based. Remediation may include quarantine or removal of any malware detected.

More Info

Notes: Currently running on laptops. Need for smartphones and tablets as well.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 12.2 Protection from Malware



5.9 Single Factor Access Control

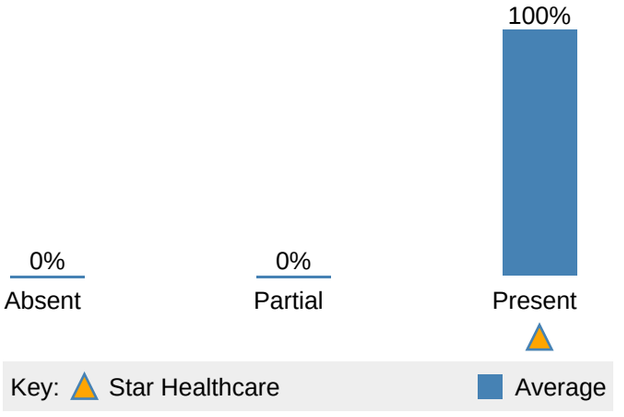
Access control using a single factor, either "what you know", "what you have" or "what you are" / biometrics. Username / password is a very common form of "what you know" single factor authentication. There may be multiple sets of credentials across different domains, applications and solutions. This capability includes both technology and processes covering full IAM (Identity and Access Management) lifecycle such as authentication and authorization / privilege management.

More Info

Notes: Microsoft Windows login, as well as logins across various applications.

HIPAA: 45 CFR 164.312

ISO: ISO/IEC 27002:2013 Section 9 Access Control



5.10 Firewall

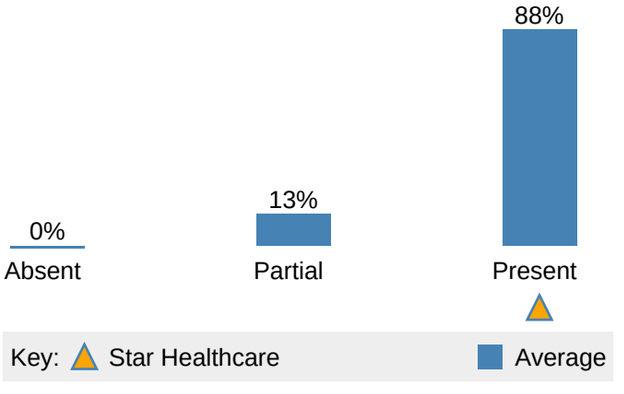
Provides network perimeter defense against unauthorized access to healthcare organizations systems and sensitive patient information. May also include host-based firewalls. Services may include provisioning / deployment, upgrade, patching, policy / configuration updates, network traffic monitoring, etc.

More Info

Notes: Currently have firewalls in place on perimeter of network, as well as endpoints.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 13.1.2 Security of Network Services



5.11 Email Gateway

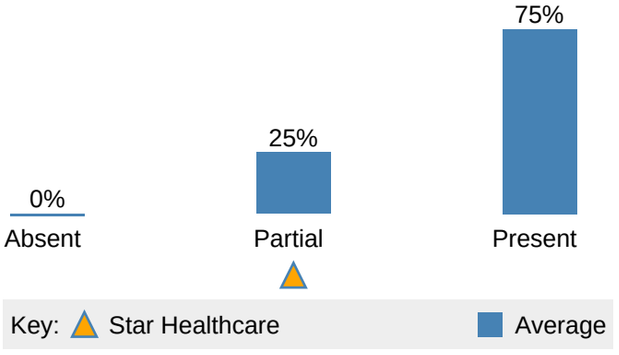
Safeguard for email and may include inbound threat protection, outbound encryption, compliance, data loss prevention, and administration.

More Info

Notes: We have the appliance in place but need to establish process to configure and monitor it.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 13.1 Network Security Management



5.12 Web Gateway

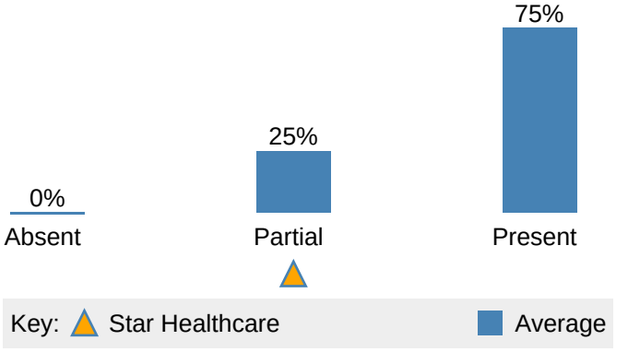
Safeguard for web requests and content returned in responses and may include analysis of the nature and intent of all content and code entering the network from requested web pages, to provide protection against malware and other hidden threats.

More Info

Notes: Appliance in place but need resources and process to monitor it to get full benefit.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 13.1 Network Security Management



5.13 Vulnerability Management, Patching

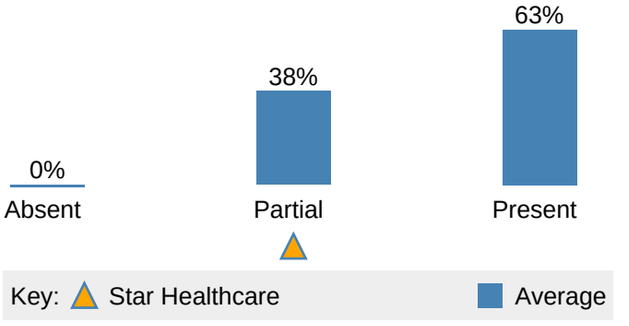
Ability (technology and processes) to manage vulnerabilities on endpoint devices through configuration updates, signature updates, patching, and so forth.

More Info

Notes: Currently PC's configured for automatic updates. Need to do more vulnerability management eg with client configuration.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 12.6 Technical Vulnerability Management



5.14 Security Incident Response Plan

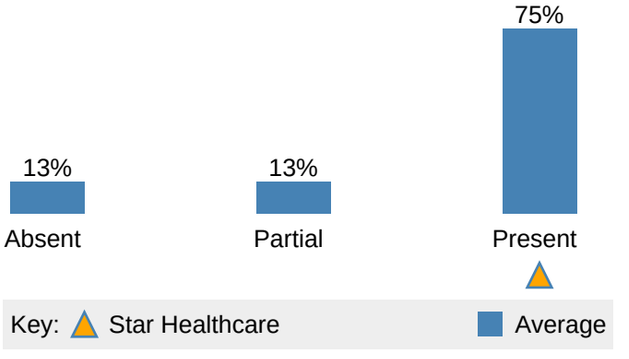
Plans in place covering what do to in the event of a suspected data security incident or breach.

More Info

Notes: Currently in place and tested. Good to go.

HIPAA: 45 CFR 164.308(a)(6)

ISO: ISO/IEC 27002:2013 Section 16 Information Security Incident Management



5.15 Secure Disposal

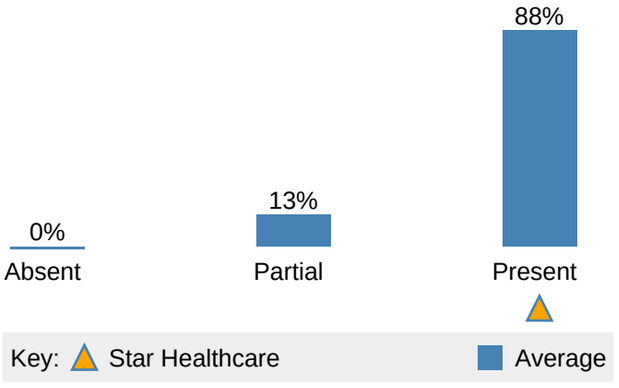
Technology and processes to securely dispose of devices and media containing sensitive healthcare information. This can include secure wipe of disk drives, shredding of paper records, and so forth.

More Info

Notes: Secure wipe for hard drives. Shredding for paper records.

HIPAA: 45 CFR 164.310(d)(2)(i)

ISO: ISO/IEC 27002:2013 Section 8.3.2 Disposal of Media, 11.2.7 Secure Disposal or Re-Use of Equipment



5.16 Backup and Restore

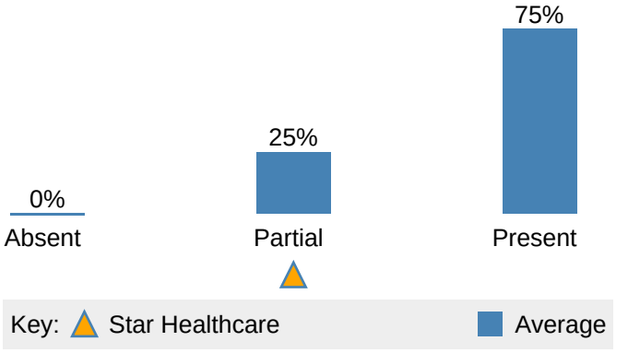
Ability to securely backup systems and data, store versioned backups in a secure managed backup system. This also includes the ability restore systems that become corrupt or infected. For this capability to be considered fully implemented it should be regularly tested through a full backup and restore cycle.

More Info

Notes: Some endpoints including smartphones and tablets not yet backed up.

HIPAA: Security Rule - Protect Availability - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 12.3 Backup



5.17 Device Control

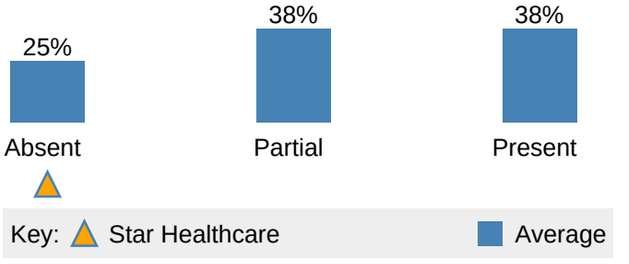
Ability to enforce the organizations policy regarding removable storage devices that may be connected by workers to endpoint client devices. Typically includes representation of policy rules, as well as technology and processes to enforce such rules. Examples include USB sticks or other removable storage.

More Info

Notes: Need to get this to prevent use of USB keys with laptops.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 8.3.1 Management of Removable Media



5.18 Penetration Testing, Vulnerability Scanning

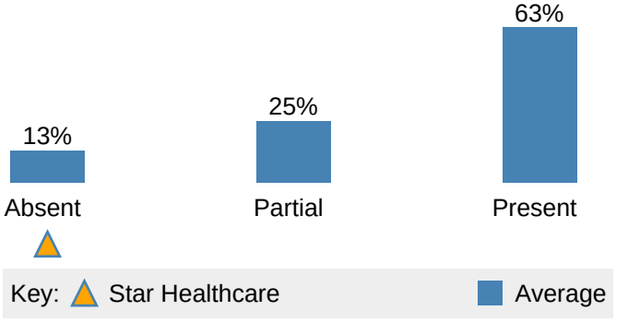
Penetration testing or vulnerability scanning has been conducted within the last year to discover vulnerabilities in a healthcare organizations IT infrastructure or applications.

More Info

Notes: Need to conduct this, especially on external network interfaces.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 18.2.3 Technical Compliance Review



5.19 Client Solid State Drive (Encrypted)

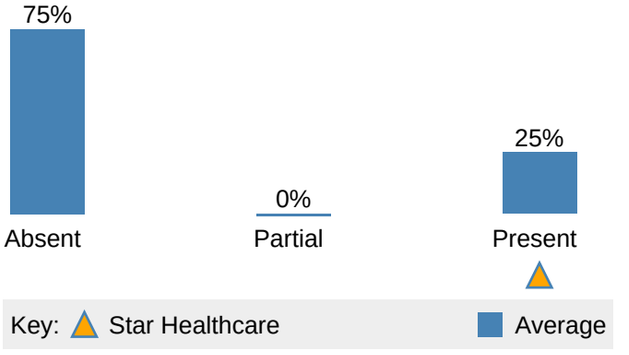
Self-encrypting solid state drives are used on client / endpoint devices to protect sensitive patient information at rest, with high performance.

More Info

Notes: Currently used in laptops.

HIPAA: 45 CFR 164.312

ISO: ISO/IEC 27002:2013 Section 10 Cryptography



5.20 Endpoint Data Loss Prevention (Prevention Mode)

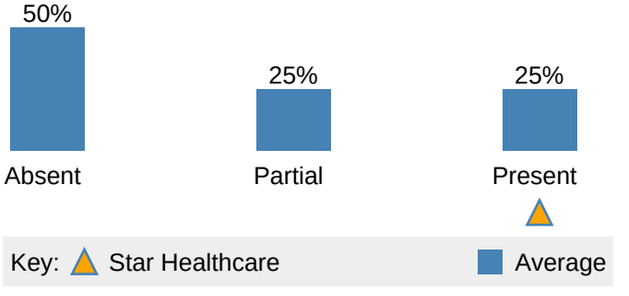
Data Loss Prevention for endpoint / client devices. Enforces rules derived from the policy of the healthcare organization that are intended to protect sensitive patient data. Includes capability to monitor user actions, detect potential non-compliance, and take action according to policy rules. Actions may include notifying the user, logging information in an audit log, preventing an action, or protecting data used in an action for example using encryption.

More Info

Notes: Working well as intended.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 18.1.3 Protection of Records



5.21 Network Data Loss Prevention (Discovery Mode)

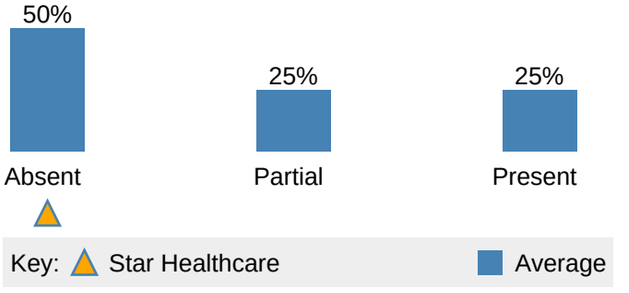
Network based Data Loss Prevention ability to monitor (scan and analyze) network traffic in real time, detect and classify sensitive patient data, and discover unknown risks.

More Info

Notes: We don't currently have a network DLP appliance.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 13.1 Network Security Management



5.22 Anti-Theft: Remote Locate, Lock, Wipe

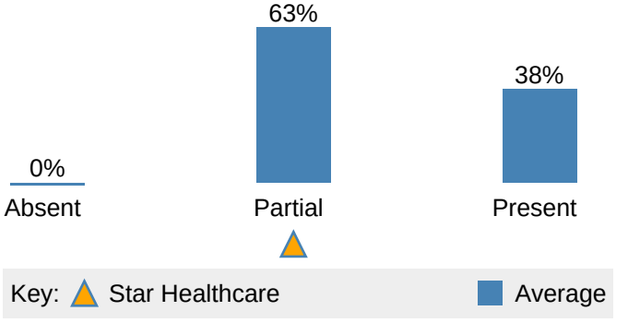
Ability for IT Administrators in healthcare organizations to remotely locate lost or stolen mobile client devices, lock them, or wipe them to remove sensitive patient data and thereby reduce risk of breach.

More Info

Notes: We have remote locate / lock / wipe only on smartphones and tablets, not on laptops currently.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 6.2 Mobile Devices and Teleworking



5.23 Multi-Factor Authentication with Timeout

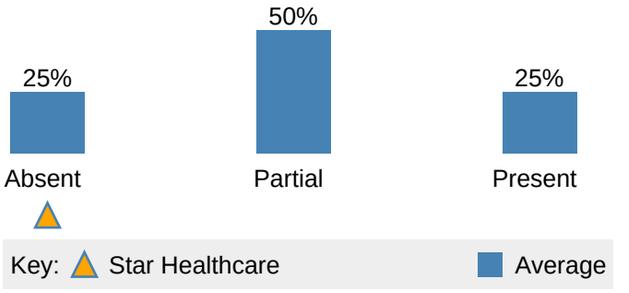
Access control with multiple factors: what you know (eg username / password), what you have (eg security hardware token), or what you are (biometrics). Timeout functionality automatically locks access after a policy defined period of inactivity, intended to reduce risk of an unauthorized access and breach that may result from an unauthorized person accessing an abandoned secure session.

More Info

Notes: We don't currently have MFA, but looking at Tap and Go prox cards.

HIPAA: 45 CFR 164.312

ISO: ISO/IEC 27002:2013 Section 9 Access Control



5.24 Secure Remote Administration

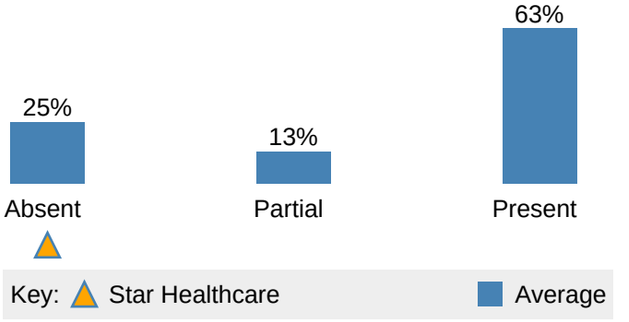
Ability for IT Administrator in healthcare organization to securely and remotely administer client devices containing sensitive patient information. This can include diagnostics, remediation of issues, patching, updates eg anti-malware signatures, configurations, upgrades, and so forth.

More Info

Notes: We don't currently have vPro laptops with Active Management Technology.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 12.6 Technical Vulnerability Management



5.25 Policy Based Encryption for Files and Folders

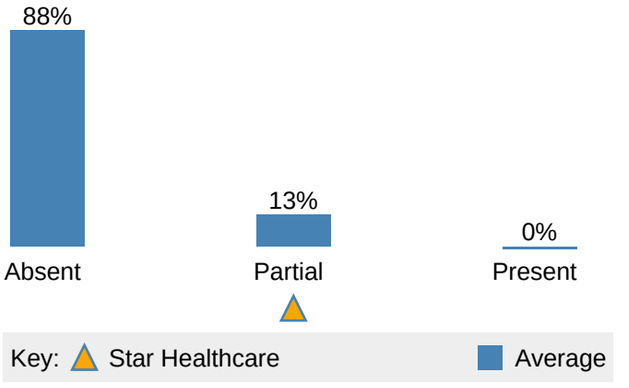
Encryption of specific files or folders based on policy of the healthcare organization, and classification of files, in order to ensure only authorized access to files and folders containing sensitive patient data, and thereby reduce risk of unauthorized access and mitigation of risk of breach.

More Info

Notes: X-Ray images are automatically encrypted per policy. Need to get this in place for other types of files.

HIPAA: 45 CFR 164.312

ISO: ISO/IEC 27002:2013 Section 10 Cryptography



5.26 Server / Database / Backup Encryption

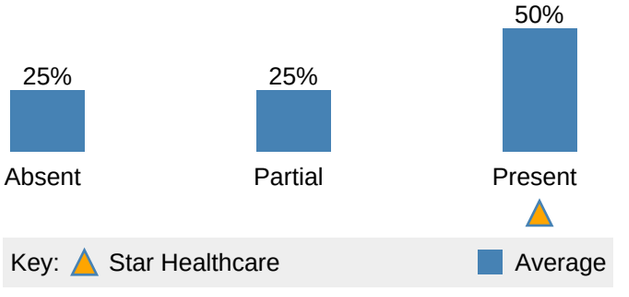
Encryption of servers, databases running on servers or SAN's, and encryption of backup archives.

More Info

Notes: Server filesystem encrypted. Database full disk encryption in place. Backups encrypted before going onto tape.

HIPAA: 45 CFR 164.312

ISO: ISO/IEC 27002:2013 Section 10 Cryptography



5.27 Network Segmentation

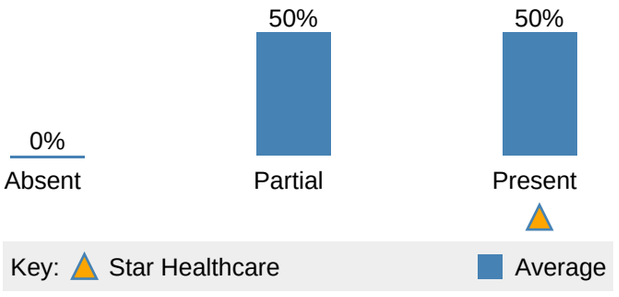
Network is segmented to protect critical assets. This can include use of guest network, medical devices network, or other segmentations to isolate vulnerabilities.

More Info

Notes: Currently have network segmented for Intranet, DMZ, Guest and Medical Devices.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 13.1.3 Segregation in Networks



5.28 Network Intrusion Prevention System

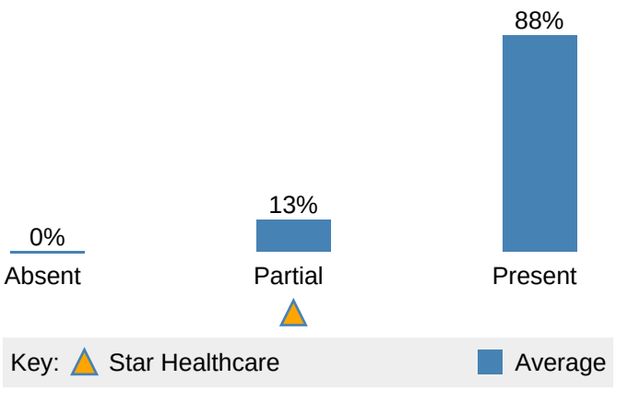
Technology and processes to detect and prevent intrusions the healthcare organizations network.

More Info

Notes: Needs better monitoring.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 13.1 Network Security Management



5.29 Business Associate Agreements

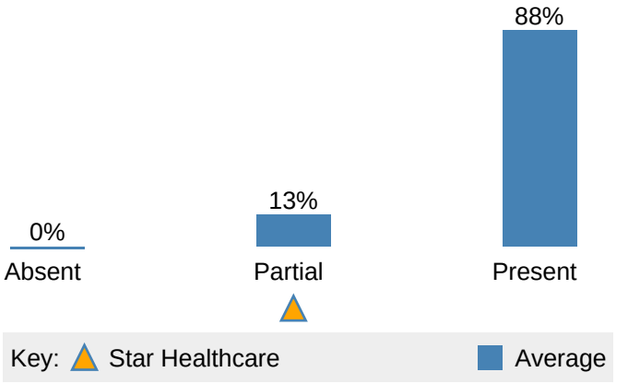
Contractual agreements covering the security and privacy of sensitive patient data with all third party sub-contractors or data processors that work with sensitive patient information.

More Info

Notes: Most of our contractors have signed a BAA. Working on getting others.

HIPAA: 45 CFR 164.308(b)(1)

ISO: ISO/IEC 27002:2013 Section 13.2.4 Confidentiality or Non-Disclosure Agreements



5.30 Virtualization

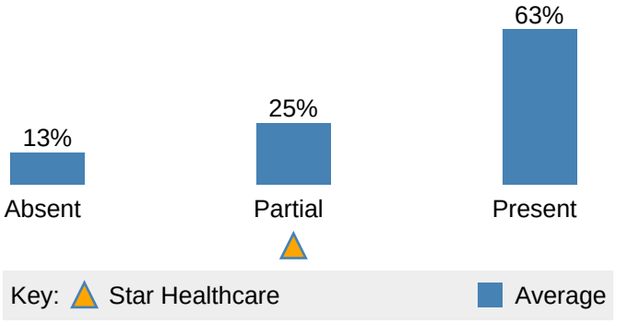
Virtualizing clients so that sensitive healthcare data exists only on strongly managed and secured servers, and not on clients and mobile devices that are at higher risk of loss or theft.

More Info

Notes: We have some VDI from zero client terminals, but we still have a significant portion of our endpoint PC's without VDI.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 11.2.1 Equipment Siting and Protection



5.31 Server Solid State Drive (Encrypted)

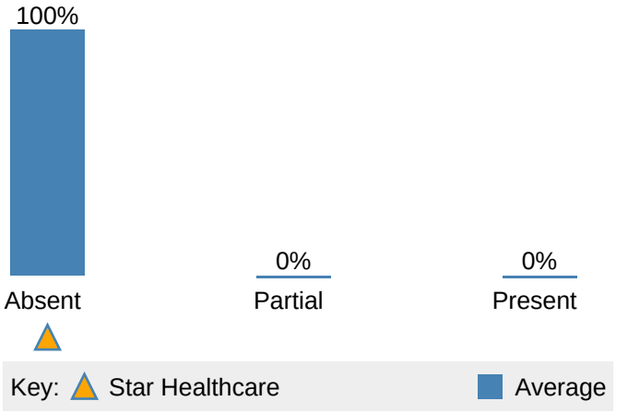
Solid state drives with encryption on servers for protection of sensitive patient data at rest on the drive.

More Info

Notes: We don't use any SSD's on the server at present.

HIPAA: 45 CFR 164.312

ISO: ISO/IEC 27002:2013 Section 10 Cryptography



5.32 Network Data Loss Prevention (Prevention Mode)

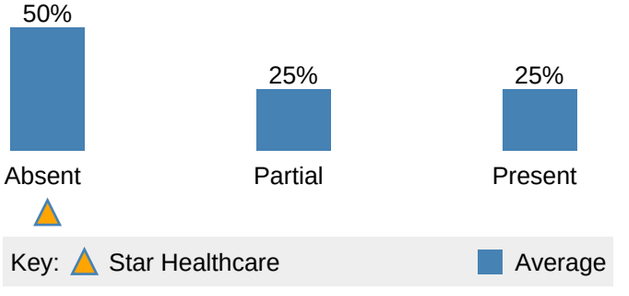
Network Data Loss Prevention ability to prevent non-compliance with the policy of the healthcare organization regarding network traffic. For example if a healthcare organization has a policy against sending patient information attached to emails NDLP can detect and block such emails and notify the sender to reduce risk of recurrence.

More Info

Notes: We don't currently have network DLP.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 13.1 Network Security Management



5.33 Database Activity Monitoring

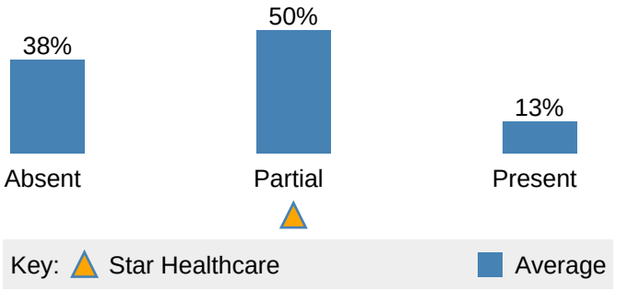
Monitoring of database activity in order to detect possible intrusion, for example in a case where database administrator credentials may have been compromised and used for covert unauthorized access to sensitive patient information in the database.

More Info

Notes: We currently only have this on some of our databases containing patient information.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 12.4 Logging and Monitoring



5.34 Digital Forensics

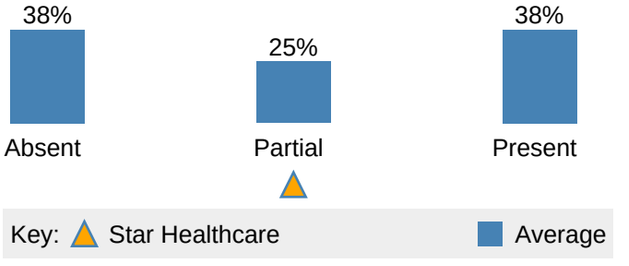
Ability to conduct forensic analysis of IT infrastructure, often in the event of a suspected security incident, to detect unauthorized access to sensitive patient information and establish whether breach occurred and if so characteristics such as timing and extent.

More Info

Notes: We contract an external organization for parts of this.

HIPAA: Incident Management - Forensics

ISO: ISO/IEC 27002:2013 Section 16.1.7 Collection of Evidence



5.35 Security Information and Event Management

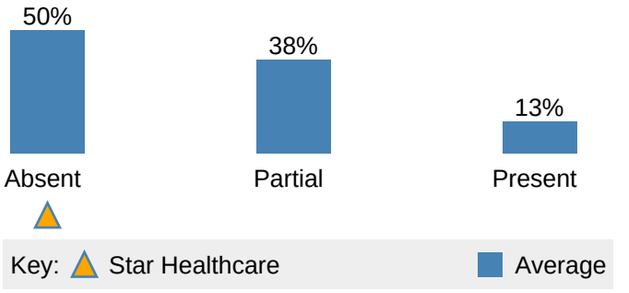
Security Information and Event Management includes real-time analysis of logs and security alerts generated by network hardware and applications.

More Info

Notes: We really need this to improve our detection capabilities.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 12.4 Logging and Monitoring



5.36 Threat Intelligence

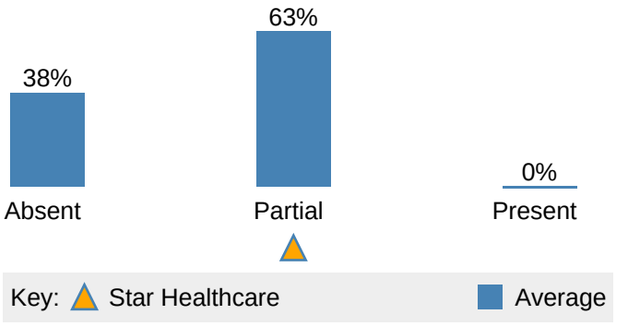
Acquisition of threat intelligence information such as where intrusions have occurred, the nature of the intrusions, appropriate safeguards and actions to mitigate, and sharing this information across security infrastructure near real time to improve defense and minimize recurrence / extent of future intrusions / breaches. Threat intelligence can include reputational information or information acquired through sandboxing and static or dynamic analysis of suspect executables.

More Info

Notes: We get updates on new threats from our security provider. We really need the ability to automate update of security controls based on this feed though.

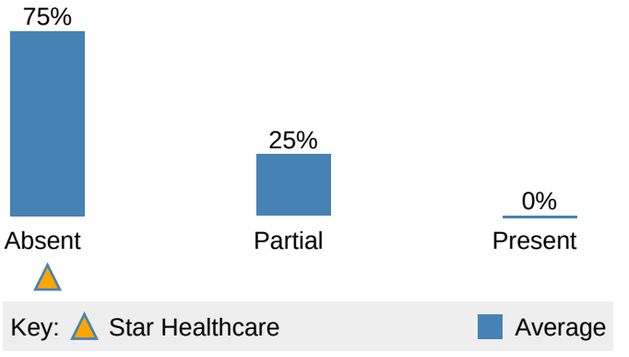
HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 12.6 Technical Vulnerability Management



5.37 Multi-Factor Authentication with Walk-Away Lock

Multi-Factor Authentication including multiple factors from: what you know (eg username / password), what you have (eg security hardware token), and what you are (eg biometrics). Walk away lock is ability to automatically lock a secure session the moment a healthcare worker walks away from the endpoint device running that terminal. Intended to mitigate risk of an unauthorized individual hijacking a secure session that an authorized user established and has abandoned (yet timeout lock has not yet occurred).



More Info

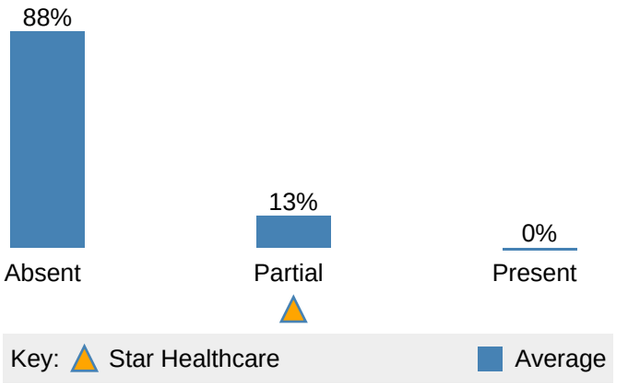
Notes: We don't currently have MFA. Once we have MFA we want to get this through Imprivata walk-away lock based on facial recognition.

HIPAA: 45 CFR 164.312

ISO: ISO/IEC 27002:2013 Section 9 Access Control

5.38 Client Application Whitelisting

Ability to control what applications run on a client device and block unauthorized applications from running. Typically signature based detection and enforcement. Includes secure processes for provisioning, managing, and updating whitelists.



More Info

Notes: We have this on some medical device machines. We need it on more.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 12.2.1 Controls Against Malware

5.39 Server Application Whitelisting

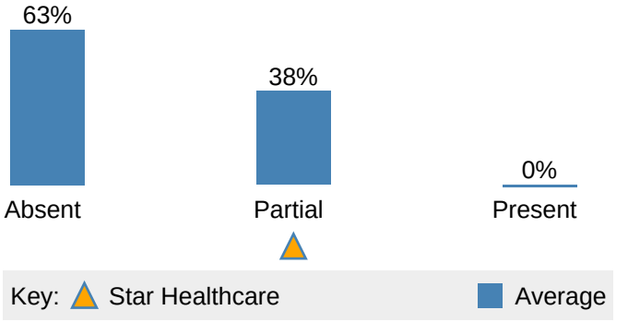
Ability to control what applications run on servers and block unauthorized applications from running. Typically signature based detection and enforcement. Includes secure processes for provisioning, managing, and updating whitelists.

More Info

Notes: Some servers associated with medical devices have this, but need it on all medical device servers.

HIPAA: Security Rule - Protect Confidentiality - Technical Safeguard

ISO: ISO/IEC 27002:2013 Section 12.2.1 Controls Against Malware



5.40 De-Identification / Anonymization

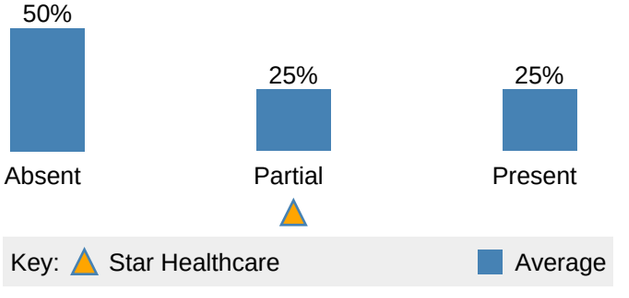
The ability to remove or mask personally identifiable fields in sensitive patient information to enable use while minimizing risk of breach.

More Info

Notes: We currently do this on data for research.

HIPAA: HHS Guidance

ISO: ISO/IEC 27002:2013 Section 9.4.1 Information Access Restriction



5.41 Tokenization

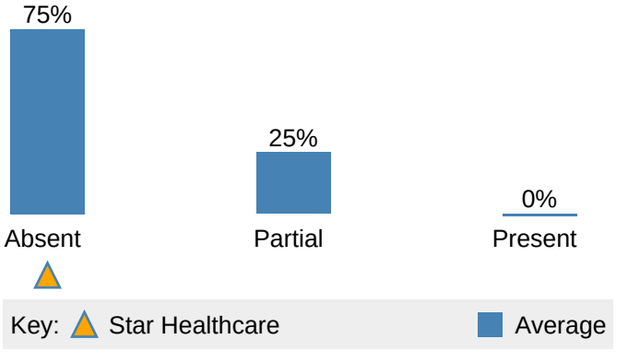
Replacing personally identifiable fields in sensitive patient records with opaque unique tokens and storing the mappings from these tokens back to the real data values in a secure access controlled database.

More Info

Notes: We don't do this but could use it for areas of our network that do payment processing and are subject to PCI DSS compliance.

HIPAA: HHS Guidance

ISO: ISO/IEC 27002:2013 Section 9.4.1 Information Access Restriction



5.42 Business Continuity and Disaster Recovery

People, process and technology to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster or disruption.

More Info

Notes: Some core / critical systems still need to be added.

HIPAA: Security Rule - Protect Availability

ISO: ISO/IEC 27002:2013 Section 11.1.4 Protecting Against External and Environmental Threats