HCLSoftware

HIPAA compliance Mapping Document

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) establishes national standards to protect individuals' electronic protected health information (ePHI) that is created, received, used, or maintained by covered entities. To ensure the confidentiality, integrity, and security of electronic patient health information, the HIPAA Security Rule outlines specific **administrative, physical, and technical safeguards** that organizations must implement.

HCL BigFix provides comprehensive solutions that align with the requirements of **the HIPAA Security Rule**. This document maps HCL BigFix's capabilities to HIPAA requirements, highlighting how HCL BigFix supports compliance and reinforces the protection of sensitive patient information.

HIPAA checklist Mapping Table

Administrative Safeguards

HIPAA Control Description	BigFix Capability
164.308(a)(1)(ii)(A) Risk Analysis Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	**Comprehensive Vulnerability Assessment** HCL BigFix assists with the assessment process by identifying and prioritizing vulnerabilities across endpoints. It leverages CyberFOCUS Security Analytics to integrate seamlessly with leading vulnerability scanners, allowing organizations to streamline vulnerability detection and enable efficient remediation to maintain a secure and compliant environment.
164.308(a)(1)(ii)(B) Risk Management Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	**Streamlined Risk Mitigation** HCL BigFix helps implement security measures by identifying and prioritizing vulnerabilities across systems. Leveraging CyberFOCUS Security Analytics and its integration with leading vulnerability scanners, BigFix facilitates efficient detection and remediation of vulnerabilities to enhance overall security posture.
164.308(a)(1)(ii)(D) Information System Activity Review Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	**Enhanced Audit Logging** HCL BigFix's audit logs provide detailed visibility into user activities, including login events, actions performed, targeted systems, and corresponding timestamps. Custom properties can also be configured and audited to support comprehensive activity reviews. HCL BigFix enables regular review of these records by capturing and logging all behavior within the product.
164.308(a)(3)(ii)(C) Termination procedures Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	BigFix integrates with enterprise CMDBs to support procedural workflows by identifying endpoints using assigned properties or custom tags. HCL BigFix enables the quarantine of targeted endpoints, thereby controlling network communication through the allowance or restriction of access. Additionally, BigFix has the capability to remotely wipe certain devices as a remote execution in line with an employee's termination.
164.308(a)(5)(ii)(A) Security reminders Periodic security updates.	**Automated Security Updates and Reminders** HCL BigFix automates the deployment of security patches and configuration updates, enabling faster remediation and reducing the time devices remain vulnerable. With one of the broadest catalogues of security updates, it allows for both manual and automated patch deployments.

HIPAA Control Description	BigFix Capability
164.308(a)(5)(ii)(B) Protection from malicious software Procedures for guarding against, detecting, and reporting malicious software.	**Proactive Threat Mitigation** HCL BigFix reduces the attack surface by enforcing endpoint compliance and integration with anti-malware platforms that provide an audit to verify if the platform is installed, updated, running, and fixed. HCL BigFix has checks in the HIPAA checklist that attempt to close multiple vulnerability paths used by malicious software to reduce the attack surface.
164.308(a)(5)(ii)(C) Log-in monitoring Procedures for monitoring log-in attempts and reporting discrepancies.	**Secure Authentication Practices** HCL BigFix enhances secure login protocols by enforcing robust login and logoff configurations as defined in the HIPAA checklist. It prevents malicious attempts by limiting invalid login attempts, implementing account lockout policies, and ensuring compliance with secure access standards. While HCL BigFix does not monitor failed logins in real-time, its enforcement of best practices strengthens overall security.
164.308(a)(5)(ii)(D) Password management Procedures for creating, changing, and safeguarding passwords	**Policy Enforcement for Password Security** HCL BigFix includes checks in the HIPAA checklist that supplement password management solutions by verifying password existence, enforcing age, expiration settings, controlling options like allowing or disallowing 'machine account password changes' and other related configurations.
164.308(a)(6)(i) Standard: Security incident procedures Implement policies and procedures to address security incidents.	**Visibility into Security Trends** HCL BigFix offers visibility into endpoint compliance trends, allowing organizations to monitor changes over time and identify potential security incidents. Through near real-time reporting and analysis, HCL BigFix enables organizations to investigate anomalies effectively, forming a key component of Security incident management runbooks.
164.308(a)(6)(ii) Implementation specification Response and reporting Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	**Effective Incident Response** HCL BigFix facilitates a swift response to security incidents by identifying vulnerable devices and enabling rapid configuration changes. Its ability to quarantine endpoints prevents further impact, while detailed reports provide actionable insights for remediation and documentation
164.308(a)(7)(i) Standard: Contingency plan Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	**Efficient System Restoration** HCL BigFix supports business continuity by enabling rapid restoration of systems through OS imaging and software deployment. It ensures compliance with security standards during recovery and provides visibility into endpoint classifications, such as encryption status, to aid in efficient recovery planning.

HIPAA Control Description	BigFix Capability
164.308(a)(7)(ii)(B) Disaster recovery plan Establish (and implement as needed) procedures to restore any loss of data.	**Backup System Integration** HCL BigFix can complement existing backup systems by tracking properties like the date and location of the last successful backup. This information provides a reliable starting point for recovery operations, helping organizations restore critical systems and maintain data integrity in line with HIPAA guidelines.
164.308(a)(7)(ii)(C) Emergency mode operation plan Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	**Hardware High Availability** HCL BigFix offers Business Continuity and Disaster Recovery capabilities to ensure high availability of your HCL BigFix Deployment. In the event of underlying hardware failure, the BigFix instances can be fully restored, preserving all settings and configurations for seamless recovery.
164.308(a)(7)(ii)(D) Testing and revision procedures Implement procedures for periodic testing and revision of contingency plans.	**Automated Testing of Contingency Plans** HCL BigFix allows organizations to test contingency plans through automation in test and development environments. Its scalable infrastructure and flexible Fixlet architecture empowers users to design, evaluate, and refine business continuity strategies effectively.
164.308(a)(8) Standard: Evaluation Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	**Security Evaluations** HCL BigFix supports ongoing evaluation of security policies and procedures by providing advanced automation tools for testing and refinement. Its flexible framework enables organizations to adapt to operational changes while maintaining robust compliance with HIPAA requirements.
164.308(a)(8) Standard: Evaluation Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	**Security Evaluations** HCL BigFix supports ongoing evaluation of security policies and procedures by providing advanced automation tools for testing and refinement. Its flexible framework enables organizations to adapt to operational changes while maintaining robust compliance with HIPAA requirements.

HIPAA checklist Mapping Table

Physical Safeguards

HIPAA Control Description	BigFix Capability
164.312(a)(1) **Access control** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	**Role-Based Access Control:** The HCL BigFix HIPAA checklist incorporates checks that ensure access and functionality are appropriately restricted based on each role, requiring an Administrator account for any actions that might compromise the security of protected health information.
164.312(a)(2)(i) **Unique user identification** Assign a unique name and/or number for identifying and tracking user identity.	**Securing User Identity** The HCL BigFix HIPAA checklist includes checks that enforces secure user identification by restricting logins to approved methods and requiring Network Level Authentication.
164.312(a)(2)(iii) **Automatic logoff** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	**Enforcing Automatic Logoff** HCL BigFix ensures compliance with automatic logoff requirements by implementing checks to enforce appropriate timeout and inactivity settings, terminating sessions after predefined periods of inactivity.
164.312(a)(2)(iv) **Encryption and decryption** Implement a mechanism to encrypt and decrypt electronic protected health information.	**Encryption and Decryption** HCL BigFix implements checks to enable encryption for data, traffic, and session security, which helps in the protection of Electronic Patient Health Information
164.312(b) **Audit controls** A covered entity or business associate must Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	**Facilitating Independent Audits** The HCL BigFix HIPAA checklist includes checks to ensure and enforce audits of account statuses, login events, service changes, group membership, and file share successes and failures.

HIPAA Control Description	BigFix Capability
164.308(a)(7)(ii)(B) Disaster recovery plan Establish (and implement as needed) procedures to restore any loss of data.	**Backup System Integration** HCL BigFix can complement existing backup systems by tracking properties like the date and location of the last successful backup. This information provides a reliable starting point for recovery operations, helping organizations restore critical systems and maintain data integrity in line with HIPAA guidelines.
164.312(c)(1) Integrity A covered entity or business associate must Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	**Ensuring Data Integrity** The HCL BigFix HIPAA checklist includes checks designed to mitigate risks to ensure data integrity. It automatically enforces policies that protect against threats to ePHI.
164.312(c)(2) Mechanism to authenticate Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	**Authenticating Data Integrity** The HCL BigFix HIPAA checklist includes checks to enforce network security settings, ensuring authentication is securely managed through LAN Manager and LDAP.
164.312(e)(1) Transmission security A covered entity or business associate must Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	**Securing Transmission of EPHI** The HCL BigFix HIPAA checklist includes checks to enforce cryptographic mechanisms, preventing unauthorized disclosure or modification of information requiring at-rest protection.
164.312(e)(2)(i) Integrity controls Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	**Ensuring Integrity of Transmitted EPHI** BigFix has checks in the HIPAA checklist that enforces digital encryption and signing of communications to ensure Electronic Protected Health Information is transmitted securely.
164.312(e)(2)(ii) Encryption Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	**Encryption for ePHI Protection** HCL BigFix supports BitLocker management to enable device encryption and implements checks to manage encryption of data, traffic, and session security, ensuring electronic protected health information is protected

Conclusion

By leveraging HCL BigFix's comprehensive endpoint compliance and security capabilities, healthcare organizations can effectively meet the HIPAA requirements. HCL BigFix offers the tools needed to continuously monitor, secure, and manage systems that handle ePHI, ensuring compliance with regulatory standards while mitigating the risk of data breaches. With its near real-time monitoring, automated patch management, and robust audit capabilities, HCL BigFix enables organizations to maintain a secure and compliant IT infrastructure in the face of evolving cybersecurity threats.

References:
1. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
2. https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

About HCLSoftware

HCL Software is a global leader in software innovation, dedicated to powering the Digital+ Economy. We develop, market, sell, and support transformative solutions across business and industry, intelligent operations, total experience, data and analytics, and cybersecurity. Built on a rich heritage of pioneering spirit and unwavering commitment to customer success, we deliver best-in-class software products that empower organizations to achieve their goals. Our core values of integrity, inclusion, value creation, people centricity, and social responsibility guide everything we do. HCL Software serves more than 20,000 organizations, including a majority of the Fortune 100 and almost half of the Fortune 500.