HIPAA
Compliance report

Be Software International
Pty Ltd

Report Issue Date: 04/20/2021
Testing Dates: 02/01/2021 to 04/16/2021
Assessor: Raul E Lopez

Scope

At the request of Be Software International Pty Ltd, the information security assessor performed a security assessment against the supporting services and assets of Be Software International Pty Ltd and the application to the HIPAA Security Rule to electronic personal health information that is created, received, used, or maintained.

The HIPAA Security Rule establishes US national standards to protect individuals electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

This document reports the results and conclusions of the security assessment engagement.

Objectives

The main purpose of this assessment is to validate the compliance of the HIPAA security rule that states as follows in the Electronic Code of Federal Regulations (e-CFR) Title 45 - Public Welfare Subtitle A - Department of Health and Human Services SUBCHAPTER C - ADMINISTRATIVE DATA STANDARDS AND RELATED REQUIREMENTS PART 164 - SECURITY AND PRIVACY Subpart C - Security Standards for the Protection of Electronic Protected Health Information § 164.306 Security standards: General rules section a:

(a) General requirements. Covered entities and business associates must do the following:
(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
(4) Ensure compliance with this subpart by its workforce.

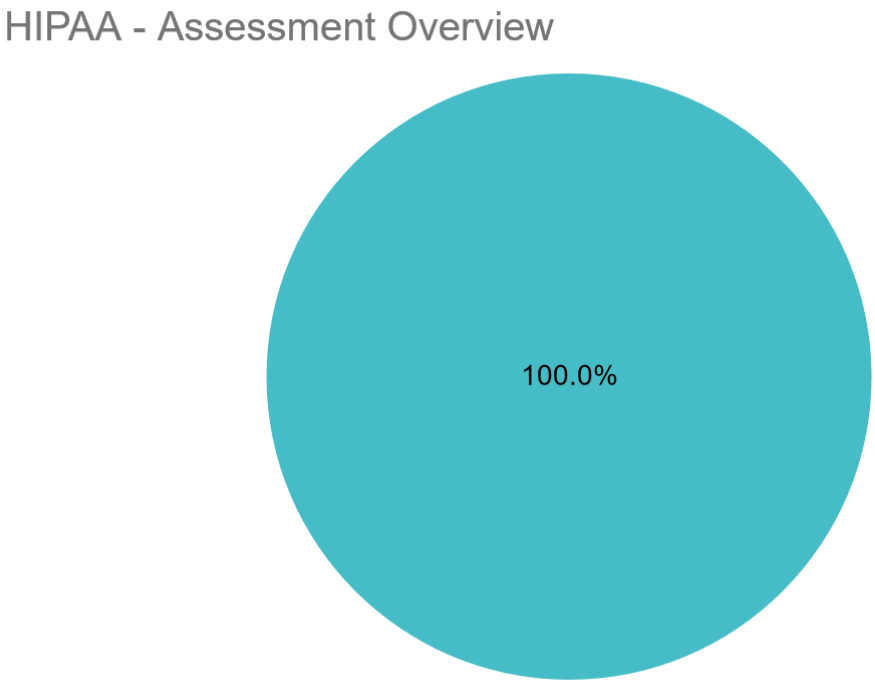
Assessment Resources

A set of interviews and sessions was performed in order to validate compliance and as part of the assessment it was presented and shared the following documentation

- Asset inventory version 2.6
- Network Diagram version 1.0
- Dataflow register for personal health information version 2.0
- Penetration test latest reports (2020)
- Third party and service providers list version 1.0
- Risk assessment version 1.9
- Incident management procedure version 3.2
- Software change and development procedure version 1.9
- Access Control policies and procedures
- Operational procedures
- Information security standards version 3.1
- BCP/DRP Plan version 2.2

Executive Summary

Based on the control evaluation performed Be Software International Pty Ltd have provided evidence that support 100% of compliance based on the list of controls applicable based on the suite of HIPAA Administrative Simplification Regulations, this can be found at 45 CFR Part 160, Part 162, and Part 164



Control summary	Count
Not Requested	0
Requested	0
Under review	0
Amendment to process required	0
Non Compliant	0
Compliant	150

Detailed Report

Based on the control evaluation performed Be Software International Pty Ltd have provided evidence that support 100% of compliance based on the list of controls applicable based on the suite of HIPAA Administrative Simplification Regulations, this can be found at 45 CFR Part 160, Part 162, and Part 164

The detail of controls applicable to this assessment and the evaluation criteria of “Compliance” can be verified as follows:

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.308a1iiA	Has a Risk Analysis been completed to identify potential threats & vulnerabilities and likelihood of impact, including management, operational, and technical issues (such as outlined in NIST SP 800-30), for all systems that store, process or transmit ePHI?	Yes	Compliant
HIPAA	164.308a1iiA	Have you identified potential threats and vulnerabilities and ranked them based on their likelihood and impact should they happen (to prevent them from happening)?	Yes	Compliant
HIPAA	164.308a1iiA	Have you conducted penetration testing?	Yes	Compliant
HIPAA	164.308a1iiB	Do you have a Risk Management procedures in place that requires a Risk Assessment be completed to evaluate compliance with the HIPAA Security Rule?	Yes	Compliant
HIPAA	164.308a1iiB	Has a Risk Management & Risk Mitigation process been completed (such as outlined in NIST Guidelines NIST 800-30) to reduce risks & vulnerabilities, including documentation of corrective actions taken?	Yes	Compliant

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.308a1iiB	Do you have a policy in place requiring users to get approval for use of any new and updated hardware and/or software (e.g. putting in networks, systems, desktops,)?	Yes	Compliant
HIPAA	164.308a1iiB	Do you have a process in place/ controls to deal with remaining (residual) risk after other controls have been applied?	Yes	Compliant
HIPAA	164.308a8	Do you perform periodic technical and non technical evaluations of the standards under this rule and in response to environmental or operational changes affecting the security of ePHI?	Yes	Compliant
HIPAA	164.308a7i	Do you have P&Ps in place to respond to emergencies that damage systems containing ePHI?	Yes	Compliant
HIPAA	164.308a7i	Do you maintain a copy of the plans on & offsite?	Yes	Compliant
HIPAA	164.308a7i	Have you assigned responsibility for implementing and maintaining the P&P? If yes, who is responsible?	Yes	Compliant
HIPAA	164.308a7iiB	Have you established and implemented procedures to restore any loss of ePHI data that is stored electronically?	Yes	Compliant
HIPAA	164.308a7iiC	Have you established and implemented procedures to enable continuation of critical business processes for protection of ePHI while operating in the emergency mode?	Yes	Compliant
HIPAA	164.308a7iiC	Does the plan include all critical systems containing ePHI such as the EHR, patient accounting systems, digital recordings of diagnostic images, electronic test results, etc. as well as all supplies & service providers to support the plan?	Partial	Compliant

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.308a7iiC	Do you have any environmental controls? Any alarms/paging used for temperature and/or fire? Fire suppression system? Fire extinguishers? Does insurance cover sprinkler malfunctioning? 4) Install a cooling system	Partial	Compliant
HIPAA	164.308a7iiC	Do you have a UPS? Are there any warning lights or alarms? Generator?	Partial	Compliant
HIPAA	164.308a7iiC	Are redundant power supplies monitored and tested (UPS and/or Generator)?	Partial	Compliant
HIPAA	164.308a7iiC	Are the contingency plans distributed to the appropriate personnel and readily available in the event of an emergency?	Yes	Compliant
HIPAA	164.308a7iiD	Have you implemented procedures for periodic testing and revision of contingency plans?*	Yes	Compliant
HIPAA	164.308a7iiE	Have you assessed the relative criticality of specific applications and data in support of other contingency plan components?*	Yes	Compliant
HIPAA	164.308a7iiE	Do you have a list of servers, model & serial #s, software, locations, use/role, interdependencies, and warranty information? Where is this located?	Yes	Compliant
HIPAA	164.308a7iiE	Do you have a list of all workstations and portable media/mobile devices that may be used to access, store, and transmit ePHI (i.e. computers, laptops, smart phones, flash drives, etc.). Does this include where they are located, purpose of their use, who uses them, and where to get backup systems for emergencies? Where is this maintained?	Partial	Compliant
HIPAA	164.308a7iiE	Do you have a network diagram of all servers, systems, interfaces, etc.? Where is this located?	Yes	Compliant

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.308a7iiE	Do you have a data inventory list (which may include more than what is stored/transmitted in key ePHI applications) in your current criticality list?	Yes	Compliant
HIPAA	164.310a2i	Have you established and implemented procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency?*	Partial	Compliant
HIPAA	164.312a2ii	Have you established and implemented procedures for obtaining necessary ePHI during an emergency?	Yes	Compliant
HIPAA	164.308a7iiA	Have you established and implemented procedures to create and maintain retrievable exact copies of ePHI?	Yes	Compliant
HIPAA	164.308a7iiA	What types of backups are performed of your servers (look at log, rotation schedule offsite storage, & testing backups)?	Yes	Compliant
HIPAA	164.310d1	Have you implemented P&Ps that define how hardware and media may be moved into and out of each facility?	Partial	Compliant
HIPAA	164.310d2iii	Do you have and follow a policy to maintain a record of the movements of hardware and electronic media and the person responsible for its movement?*	Partial	Compliant
HIPAA	164.310d2iv	Do you have and follow a plan to create a retrievable, exact copy of ePHI, when needed, before moving equipment on which it is stored?*	Partial	Compliant

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.308a1iiD	Have you implemented procedures to regularly review records of information system activity such as audit logs, access reports, and security incident tracking in all systems that contain or transmit ePHI?	Yes	Compliant
HIPAA	164.308a5iiC	Do you have procedures for monitoring log-in attempts and reporting discrepancies?*	Yes	Compliant
HIPAA	164.312b	Have you implemented hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI (Audit Controls)?	Yes	Compliant
HIPAA	164.312b	What security auditing capabilities are in place for systems that contain or transmit ePHI (to monitor for unauthorized users)? Is access limited to specific users?	Yes	Compliant
HIPAA	164.312b	Are there security audit logging capabilities for the servers? If yes, to what degree can users be audited in each server?	Yes	Compliant
HIPAA	164.312b	Are there any audit storage space constraints?	Yes	Compliant
HIPAA	164.308a5iiB	Do you have written procedures for guarding against, detecting, and reporting malicious software (virus, Trojan horse, or worms)?*	Yes	Compliant
HIPAA	164.308a5iiB	Are anti-virus/malware updates on the *servers* active and current, and how are they verified?	Yes	Compliant
HIPAA	164.308a5iiB	Are anti-virus/malware updates on the *workstations (computers, laptops, etc.)* active and current, and how are they verified?	Yes	Compliant
HIPAA	164.308a5iiB	Are anti-virus/malware updates on third party *medical devices* active and current, and how are they verified?	No	N/A

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.308a5iiB	Do you have systems in place to inspect and control all places where data comes into and leaves your system (such as a firewall, proxy, anti-spam, etc.)?	Yes	Compliant
HIPAA	164.308a5iiB	Are *server* patches current and how are they verified?	Yes	Compliant
HIPAA	164.308a5iiB	Are *workstation* patches current and how are they verified?	Yes	Compliant
HIPAA	164.308a5iiB	Are *portable devices* (i.e. smart phones, laptops, etc.) patches current and how are they verified?	Yes	Compliant
HIPAA	164.308a5iiB	Are *third party medical device* patches current and how are they verified?	No	N/A
HIPAA	164.306a	Is this included in a HIPAA Oversight Policy and/or in the Standards of Conduct: Our organization is dedicated to maintaining the confidentiality, integrity, and availability of PHI and protecting against any reasonably anticipated threats, hazards, and/or inappropriate uses or disclosure?	Yes	Compliant
HIPAA	164.306b	Do you have formal or informal policy and procedures to evaluate how to reasonably and appropriately implement the HIPAA Security Rule by taking into account 1) The size, complexity, and capabilities of the covered entity; 2) The CE's technical infrastructure, hardware, and software security capabilities; 3) The costs of security measures; 4) The probability and criticality of potential risks to ePHI	Yes	Compliant
HIPAA	164.306c	Requirement 1 of HI-HT-048	Yes	Compliant
HIPAA	164.306d1-2	Requirement 2 of HI-HT-048	Yes	Compliant
HIPAA	164.306d3	Requirement 3 of HI-HT-048	Yes	Compliant

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.306d3	Requirement 4 of HI-HT-048	Yes	Compliant
HIPAA	164.306e	Have you implemented P&Ps to continuously monitor security P&Ps as well as security measures in place and update them as needed to protect ePHI?	Yes	Compliant
HIPAA	164.306e	Do you have a process in place to identify new laws and regulations with IT security implications?	Yes	Compliant
HIPAA	164.308a2	Have you identified the security official who is responsible and has the enforcement authority for the development, implementation, & communication of the P&Ps required by the Security Rule (responsible and enforcement authority for identifying, reducing, & preventing threats) and have a job description for the position?	Yes	Compliant
HIPAA	164.308a2	Have you provided training for the Security Official so they are knowledgeable about their responsibilities and how to fulfill them?	Yes	Compliant
HIPAA	164.316a	Training material used on the Security Official training	Yes	Compliant
HIPAA	164.316b1	Do you maintain all P&Ps, assessments, and all other documentation (such as risk analyses, risk management decisions, moving media, hardware disposal, job descriptions, training, etc.) required by the Security Rule?	Yes	Compliant
HIPAA	164.316b2i	Do you maintain all required documentation for at least 6 years from the date of creation, or date when last in effect, whichever is later?	Yes	Compliant

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.316b2ii	Are your P&Ps readily available to those individuals in your organization required to follow and implement them?	Yes	Compliant
HIPAA	164.316b2iii	Have you implemented P&Ps to periodically review, identify, document, and mitigate reasonably anticipated threats to ePHI?	Yes	Compliant
HIPAA	164.308a5i	Do you have a security awareness training program in place requiring a training program for all workforce members?	Yes	Compliant
HIPAA	164.308a5i	When is training provided?	Yes	Compliant
HIPAA	164.308a5i	Do you document that training was provided?	Yes	Compliant
HIPAA	164.308a5iiA	Do you provide periodic information security reminders?*	Yes	Compliant
HIPAA	164.308a1i	Is this included in a HIPAA Oversight Policy and/or in the Standards of Conduct: Our organization is dedicated to preventing, detecting, containing, and correcting security violations?	Yes	Compliant
HIPAA	164.308a6i	Do you have a P&P in place to address security incidents?	Yes	Compliant
HIPAA	164.308a6ii	Do you have procedures to identify and respond to suspected or known security incidents; mitigate to the extent possible harmful effects of known security incidents; and document incidents and their outcomes?	Yes	Compliant

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.308a1iiC	Do you have a policy and procedures in place to apply sanctions against workforces who fail to comply with security P&Ps?	Yes	Compliant
HIPAA	164.308a1iiC	Do you consistently enforce the sanctions policy?	Yes	Compliant
HIPAA	13402(e) (164.408)	Do you have a policy and procedure in place requiring reporting of breaches of "unsecured PHI" and sending of notifications to the Secretary?	Yes	Compliant
HIPAA	13402a (164.404)	Do you have a policy and procedure in place requiring reporting of breaches of "unsecured PHI" and sending of notifications to individuals?	Yes	Compliant
HIPAA	13402b	Do you include breach reporting requirements in your organization's BAA? If you are a BA, do you have a policy and procedure requiring reporting of breaches of unsecured PHI to the other entity?	Yes	Compliant
HIPAA	13406 (164.406)	Do you have a policy and procedure in place requiring reporting of breaches of "unsecured PHI" and sending of notifications to the media?	Yes	Compliant
HIPAA	164.308a3i	Do you have different levels of access to ePHI for different types/categories of users for each system/application (to support minimum necessary requirements)?	Yes	Compliant
HIPAA	164.308a3iiA	Have you implemented procedures for the authorization and/or supervision of workforces who work with ePHI or in locations where it might be accessed (e.g. identified lines of authority & workforce are aware of them)?*	Yes	Compliant

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.308a3iiB	Have you implemented procedures to determine that the access of a user to ePHI is appropriate (such as role based access) and the minimum necessary (least privilege)?*	Yes	Compliant
HIPAA	164.308a3iiB	Are types of roles clearly documented and access provided based on these types of roles so that access is the minimum necessary for each user?	Yes	Compliant
HIPAA	164.308a4i	Have you implemented P&Ps to determine who can be authorized to have access to ePHI in systems, servers, workstations, and portable devices?	Yes	Compliant
HIPAA	164.308a4i	Have you implemented procedures to do background checks on workforce members prior to employment and on a regular basis thereafter?	Yes	Compliant
HIPAA	164.308a4i	Do you require workforce members and contractors to sign confidentiality agreements before allowing them to work?	Yes	Compliant
HIPAA	164.308a4iiB	Have you implemented procedures for granting access to ePHI, for example, through access to a workstation, laptop, transaction, program, process, or other mechanism?*	Yes	Compliant
HIPAA	164.308a4iiB	How are access rights requested, approved, and granted to servers containing ePHI?	Yes	Compliant
HIPAA	164.308a4iiB	How are access rights requested, approved, and granted to system users?	Yes	Compliant
HIPAA	164.312a1	Do you have P&Ps in place that allow only authorized access to systems/applications that contain and/or transmit ePHI?	Yes	Compliant

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.308a4iiC	Have you implemented policies and procedures that are based upon your access authorization policies, establish, document, review, and *modify* a user's right of access to a workstation, transaction, program, or process?*	Yes	Compliant
HIPAA	164.308a4iiC	How and when are access rights modified to *servers* containing ePHI (what procedures are in place)?	Yes	Compliant
HIPAA	164.308a4iiC	How and when are access rights modified for *system users* (what procedures are in place)?	Yes	Compliant
HIPAA	164.308a4iiC	How and when are access rights reviewed and revalidated (what procedures are in place)?	Yes	Compliant
HIPAA	164.308a3iiC	Have you implemented procedures to *terminate* access to ePHI when a workforce member leaves your organization, and/or with role changes?*	Yes	Compliant
HIPAA	164.308a3iiC	How and when are access rights terminated for *servers* containing ePHI?	Yes	Compliant
HIPAA	164.308a3iiC	How and when are access rights terminated for *system* users?	Yes	Compliant
HIPAA	164.312a2iii	Have you implemented procedures that automatically terminate system access after a predetermined time of inactivity so that unauthorized users do not access ePHI on unattended workstations?*	Yes	Compliant
HIPAA	164.312a2iii	Are automatic logoffs activated for all systems containing or that transmit ePHI? If yes, for what timeframe is it set (e.g. 10 minutes)?	Yes	Compliant

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.308a5iiD	Are users trained to lock or log off workstations and systems so that other users may not use their sessions to access ePHI?	Yes	Compliant
HIPAA	164.308a4iiA	If you are a clearinghouse that is part of a larger organization, have you implemented P&Ps to protect ePHI from the larger organization (e.g. prevent access to hardware, software, & ePHI; separate physical space)?	No	N/A
HIPAA	164.308a5iiD	Do you have procedures for creating, changing, and safeguarding passwords and are these trained to all users?*	Yes	Compliant
HIPAA	164.308a5iiD	Do you train your users to not share passwords with others and not write them down so they can be accessed by others?	Yes	Compliant
HIPAA	164.308a5iiD	What are your password security requirements to access workstations (strength, frequency of change, sharing, …)?	Yes	Compliant
HIPAA	164.308a5iiD	What are your password security requirements to access systems that contain/ transmit ePHI (strength, frequency of change, sharing, …)?	Yes	Compliant
HIPAA	164.308a5iiD	What are your server password security requirements (strength, frequency of change, sharing …)?	Yes	Compliant
HIPAA	164.312a2i	Have you assigned a unique name and/or number to each system user and can the identifier be used to track user identity in systems that contain ePHI?	Yes	Compliant
HIPAA	164.312d	Have you implemented (Person or Entity Authentication, such as unique usernames & passwords) procedures to verify that a person or entity seeking access to ePHI is the one claimed?	Yes	Compliant

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.310b	Have you implemented P&Ps that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access ePHI?	Yes	Compliant
HIPAA	164.310c	What physical safeguards have you put in place for all workstations that access ePHI to restrict access to authorized users (workstation screen viewability, laptop mobility, monitored for theft, etc.)?	Partial	Compliant
HIPAA	164.310c	How are portable devices secured/safeguarded?	Partial	Compliant
HIPAA	164.310c	Do you have any other measures in place to restrict access to those who do not need access to ePHI?	Yes	Compliant
HITECH	13404	If your organization is a BAA, do you have procedures in place to require your workforce to follow all HITECH requirements as required by the contractual relationship with that organization?	No	N/A
HITECH	13408	Are BAAs in place with vendors that provide data transmission of PHI to your organization (HIEO, RHIO, E-prescribing Gateway)?	Yes	Compliant
HITECH	13401a	If you are a BA, do you have policies indicating that you follow the Security Rule (i.e. follow the security rule while performing BA responsibilities)?	Yes	Compliant
HIPAA	164.308b1-b3	Have you implemented a P&P to obtain BAAs as required by the Security Rule, Privacy Rule & HITECH (including specific individuals responsible for oversight of third parties and BAs and to obtain, track, and update BAAs)?	Yes	Compliant

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.308b4	Do you obtain signed BAAs with language compliant with the Security Rule, Privacy Rule & HITECH and maintain them for 6 years after the contracts have expired?	Yes	Compliant
HIPAA	164.314a1	Does your BAA include the required language? Do you have a reporting & investigation process in place with BAs?	Yes	Compliant
HIPAA	164.314a2i	Does your BAA include the required language including termination of the contract if the BA violated a material term of the contract? Do you have a reporting & investigation process in place with BAs?	Yes	Compliant
HIPAA	164.314a2ii	Are you a governmental entity and have BAAs that are also governmental entities? If yes, do you require they sign a memorandum of understanding or reliance on law or regulation that requires equivalent actions of the BAA?	No	N/A
HIPAA	164.310a	Have you implemented P&Ps to limit physical access to information systems and the facilities where they are housed to those authorized to access them?	Partial	Compliant
HIPAA	164.310a2ii	Have you implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft?*	Yes	Compliant
HIPAA	164.310a2ii	What types of facility access controls are used to control exterior and interior doors (key, key code, badge. cameras)? Where are they used?	Yes	Compliant
HIPAA	164.310a2ii	Do you have a current inventory of keys, access cards, and individuals with key codes?	Yes	Compliant

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.310a2ii	Is there an alarm system?	Yes	Compliant
HIPAA	164.310a2ii	Do you restrict who can be in certain areas of the facility(s)? If yes, what areas and how? Are the workforce trained to report suspicious behavior?	Yes	Compliant
HIPAA	164.310a2ii	How do you secure hardcopy PHI (i.e. medical records, printed reports, encounter forms, etc.)?	No	N/A
HIPAA	164.310a2ii	How is access to servers and phones secured? Are there keypad entry codes, keys, or other access controls utilized to access them?	Partial	Compliant
HIPAA	164.310a2ii	Who has access to the server rooms and is the access periodically audited?	No	N/A
HIPAA	164.310a2iii	Have you implemented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision?*	Yes	Compliant
HIPAA	164.310a2iv	Have you implemented P&Ps to document repairs and modifications to the building or facility, which are related to security (for example, hardware, walls, doors, and locks)?*	Partial	Compliant
HIPAA	164.310a2iv	Do you have a process in place to approve facility changes and verify they improve (not reduce) ePHI safeguarding measures before making them (or building a new facility)?	Partial	Compliant

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.310d2i	Have you implemented P&Ps to destroy ePHI on hardware or electronic media you are no longer using?	Partial	Compliant
HIPAA	164.310d2i	What disposal procedures are in place for servers?	No	N/A
HIPAA	164.310d2i	What disposal procedures are in place for hard drives, portable devices, and other electronic media containing ePHI?	No	Compliant
HIPAA	164.310d2ii	Have you implemented procedures for removal of ePHI from electronic media before the media are available for reuse (internally and externally)?	Partial	Compliant
HIPAA	164.312e1	Have you implemented measures to prevent unauthorized access to ePHI during transmission over electronic communication networks (e.g. email, texting, paging, Internet, private or point-to-point networks, internal transmission, etc.)	Yes	Compliant
HIPAA	164.312a2iv	Have you implemented a mechanism to encrypt and decrypt ePHI?*	Yes	Compliant
HIPAA	164.312a2iv	Is ePHI stored on workstations, laptops/tablets?	No	N/A
HIPAA	164.312a2iv	Is ePHI at rest encrypted on workstations, laptops/tablets ?	No	N/A
HIPAA	164.312a2iv	Is ePHI stored on or other portable media (devices, thumb drives, & backup tapes, smart phones, etc.)?	No	N/A
HIPAA	164.312a2iv	Is ePHI at rest encrypted on other portable media (devices, thumb drives, & backup tapes, smart phones, etc.)?	No	N/A

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.312a2iv	Is ePHI at rest encrypted on servers?	Yes	Compliant
HIPAA	164.312e2ii	Have you implemented a mechanism to encrypt ePHI whenever deemed appropriate (transmissions such as emails, paging, texting, internet transmissions, virtual private networks (VPNs), etc.)? If not, what measures do you have in place to ensure the protection of this ePHI?*	Yes	Compliant
HIPAA	164.312e2ii	Do you have encrypted: email, VPN, Citrix, etc.?	No	N/A
HIPAA	164.312e2ii	What type of Internet connection(s) do you have?	Yes	Compliant
HIPAA	164.312e2ii	Are there data jacks in every room? Are they enabled?	No	N/A
HIPAA	164.312e2ii	Type of Wireless access point (WEP, WPA or WPA2)?	Yes	Compliant
HIPAA	164.312e2ii	Is your wireless SSID (service set identifier) broadcasted (i.e. icon in taskbar/internet access search)?	Yes	Compliant
HIPAA	164.312c1	Have you implemented P&Ps to prevent ePHI from being changed or destroyed improperly?	Yes	Compliant
HIPAA	164.312c2	Have you implemented electronic mechanisms to confirm that ePHI has not been altered or destroyed in an unauthorized manner?*	Yes	Compliant
HIPAA	164.312e2i	Have you implemented security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of?*	Yes	Compliant

Regulatory Source	Regulatory Requirement	Assessment Question	In Scope	Current Status
HIPAA	164.314b1-b2	Do you sponsor a health plan (i.e. have a self-insured health plan for your employees)? If yes, do you have measures in place to follow the HIPAA Security Rule and is this included in the plan documents? Does the plan document specify reporting security incidents to the group health plan?	No	N/A
HITRUST	Control Reference: 10.m Control of Technical Vulnerabilities	Do you perform periodic vulnerability scans on critical systems that process, transmit or store ePHI?	Yes	Compliant
HITRUST	Control Reference: 09.y On-line Transactions	Do you have some measure of protection against unauthorized intrusions via IDS/IPS on the Web server(s) that receive online transactions in a data warehouse?	Yes	Compliant

Non applicable controls justification

Control Number	Regulatory Source	Regulatory Requirement	Assessment Question	Current Status	Justification
HI-HT-041	HIPAA	164.308a5iiB	Are anti-virus/malware updates on third party *medical devices* active and current, and how are they verified?	N/A	No medical devices under scope
HI-HT-046	HIPAA	164.308a5iiB	Are *third party medical device* patches current and how are they verified?	N/A	No medical devices under scope
HI-HT-095	HIPAA	164.308a4iiA	If you are a clearinghouse that is part of a larger organization, have you implemented P&Ps to protect ePHI from the larger organization (e.g. prevent access to hardware, software, & ePHI; separate physical space)?	N/A	BSI is not a clearinghouse nor part of a larger organization
HI-HT-107	HITECH	13404	If your organization is a BAA, do you have procedures in place to require your workforce to follow all HITECH requirements as required by the contractual relationship with that organization?	N/A	BSI is not a BAA
HI-HT-114	HIPAA	164.314a2ii	Are you a governmental entity and have BAAs that are also governmental entities? If yes, do you require they sign a memorandum of understanding or reliance on law or regulation that required equivalent actions of the BAA?	N/A	BSI is not a governmental entity

Control Number	Regulatory Source	Regulatory Requirement	Assessment Question	Current Status	Justification
HI-HT-121	HIPAA	164.310a2ii	How do you secure hardcopy PHI (i.e. medical records, printed reports, encounter forms, etc.)?	N/A	BSI does not manage hard copy PHI
HI-HT-123	HIPAA	164.310a2ii	Who has access to the server rooms and is the access periodically audited?	N/A	Risk transferred to AWS
HI-HT-128	HIPAA	164.310d2i	What disposal procedures are in place for servers?	N/A	Risk transferred to AWS
HI-HT-129	HIPAA	164.310d2i	What disposal procedures are in place for hard drives, portable devices, other electronic media containing ePHI?	N/A	Risk transferred to AWS
HI-HT-133	HIPAA	164.312a2iv	Is ePHI stored on workstations, laptops/tablets?	N/A	No ePHI is stored on workstations, laptops/tablets
HI-HT-134	HIPAA	164.312a2iv	Is ePHI at rest encrypted on workstations, laptops/tablets ?	N/A	No ePHI is stored on workstations, laptops/tablets
HI-HT-135	HIPAA	164.312a2iv	Is ePHI stored on or other portable media (devices, thumb drives, & backup tapes, smart phones, etc.)?	N/A	No portable media used to store ePHI
HI-HT-136	HIPAA	164.312a2iv	Is ePHI at rest encrypted on other portable media (devices, thumb drives, & backup tapes, smart phones, etc.)?	N/A	No portable media used to store ePHI
HI-HT-139	HIPAA	164.312e2ii	Do you have encrypted: email, VPN, Citrix, etc.?	N/A	No ePHI transmitted outside secure data flow
HI-HT-141	HIPAA	164.312e2ii	Are there data jacks in every room? Are they enabled?	N/A	Risk transferred to AWS

Control Number	Regulatory Source	Regulatory Requirement	Assessment Question	Current Status	Justification
HI-HT-147	HIPAA	164.314b1-b2	Do you sponsor a health plan (i.e. have a self-insured health plan for your employees)? If yes, do you have measures in place to follow the HIPAA Security Rule and is this included in the plan documents? Does the plan document specify reporting security incidents to the group health plan?	N/A	BSI does not have access to ePHI/PHI, it is a service provider

Compliance status

Based on a comprehensive assessment executed between February 2021 and April 2021 on Be Software International Pty Ltd technologies and assets used to transmit, process and store electronic Protected Health Information (ePHI) and in order to validate the compliance of the HIPAA security rule located in the Electronic Code of Federal Regulations (eCFR) Title 45 - Public Welfare Subtitle A - Department of Health and Human Services SUBCHAPTER C - ADMINISTRATIVE DATA STANDARDS AND RELATED REQUIREMENTS PART 164 - SECURITY AND PRIVACY Subpart C - Security Standards for the Protection of Electronic Protected Health Information § 164.306 it has been verified that:

Be Software International Pty provides appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

Raul E Lopez
CDP, LCSPC, CPTE, CySA+, Pentest+
Information Security Consultant
April 20, 2021

---------- END OF DOCUMENT ----------