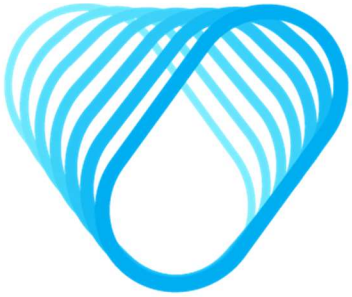

VIBRANT

ACTIVATE ▪ RESET ▪ LIVE

HIPAA

COMPLIANCE REPORT

with the Security Rule

As of January 30, 2022

VIBRANT
ACTIVATE ▪ RESET ▪ LIVE

Table of Contents

Document Management

Rev.	Written By	Date	Change Description	Signature
01	Cyber-EX – Gil Rueknstain	01/2022	Released	Gil Rukenstain

Introduction, Purpose, and Scope

Vibrant pioneered the Self-Activation Solution™, an innovative non-drug system for chronic constipation.

The orally administered capsule synchronizes the Biological Clock-Bowel connection, enabling an effective treatment, predictable bowel movements, and improved quality of life.

The treatment includes an app helping patients monitor their progress and enables the physician to remotely monitor the treatment for optimal results.

The purpose of this document is to assess the compliance of Vibrant implemented security controls with the Healthcare Insurance Portability and Accountability Act (HIPAA) Security Rule.

This assessment was performed by Mr. Gil Rueknstain, a privacy and information security consultant with more than ten years of experience in privacy and information security in the healthcare and medical sector.

Mr. Rukenstain holds the following certifications:

- CISM (Certify Information Security Manager) issued by ISACA.
- CISO (Chief Information Security Officer) issued by the Israeli Technion Institution.
- CHP (Certify HIPAA Professional) issued by the Ecfirst HIPAA Academy.
- CIPM (Certify Information Privacy Manager) issued by the IAPP.

VIBRANT
ACTIVATE • RESET • LIVE

HIPAA Security Rule Requirements and controls

Administrative Safeguard

ID	Standards	Specifications	R/A	Related question	Existing controls
1	Security Management Process §164.308(a)(1)	Risk Analysis	R	Is a Risk Analysis process used to ensure that cost-effective security measures are used to mitigate expected losses? If yes, is the Risk Analysis process documented?	The company procedure, ISP 02- Information Security Risk Management Procedure, requires a security risk assessment and treatment process. During the audit, a security risk assessment was presented to the auditors. The assessment includes information asset identification, the associated security risks, the possible attack vectors, probability, severity, and risk level, the implemented controls to mitigate risk level, and the additional controls required for risk mitigation.
2	Security Management Process §164.308(a)(1)	Risk Management	R	Are security measures implemented to reduce risks and vulnerabilities to an appropriate level for the organization?	The company implements administrative, physical, and technical security controls to reduce security risks and vulnerabilities to acceptable risk levels, according to ISP 02- Information Security Risk Management Procedure.
3	Security Management	Sanction Policy	R	Do documented policies and procedures exist regarding disciplinary actions	ISP 05- Human Resource Security Procedure includes a sanction policy.

ID	Standards	Specifications	R/A	Related question	Existing controls
	Process §164.308(a)(1)			(stipulations for misuse or misconduct)? Have they been communicated to all employees?	This issue is communicated to the employees in annual awareness training.
4	Security Management Process §164.308(a)(1)	Information System Activity Review	R	Are audit logs reviewed? If yes, how often? Is there a responsible entity? Is this effort documented? Is audit logging for communications-enabled?	The Vibrant web application and all other information systems used by the company to store PHI stores security logs about user login, failed login, account lockout, and admin activities. The system production environment in AWS is monitored by AWS services and configured to alert according to predefined rules.
5	Assigned Security Responsibility §164.308(a)(2)	No Implementation Specifications	R	Has the security responsibility for the organization been assigned to an individual or group? If yes, is it documented?	Mr. Boaz Yekutieli was assigned as the company HIPAA officer.
6	Workforce Security §164.308(a)(3)(i)	Authorization and/or Supervision	A	Are there procedures in place to ensure personnel performing technical system maintenance activities are supervised by authorized/knowledgeable individuals and that operational personnel is appropriately authorized to access systems? Are these procedures documented?	According to the company procedures (ISP 07- Access Control Procedure and ISP 09- Application Security Procedure), access to the production environment, Vibrant application, and PHI databases are restricted, granted only on a need-to-know basis audited by the DPO periodically.
7	Workforce Security §164.308(a)(3)(i)	Workforce Clearance Procedures	A	Are personnel clearance procedures established and maintained? Are these procedures documented?	Reference in ISP 05- Human Resource Security Procedure.

ID	Standards	Specifications	R/A	Related question	Existing controls
8	Workforce Security §164.308(a)(3)(i)	Workforce Clearance Procedures	A	Does the organization follow personnel clearance procedures to verify access privileges before admission? Are these procedures documented?	The company follows personnel clearance procedures to verify access privileges. Reference in ISP 05- Human Resource Security Procedure and in ISP 07- Access Control Procedure.
9	Workforce Security §164.308(a)(3)(i)	Termination Procedures	A	Are access lists updated in a timely manner when employee access authorizations change? If yes, are they documented and updated consistently?	An access list that is managed by the HIPAA officer was presented. The HIPAA Officer is responsible for updating the list when necessary.
10	Workforce Security §164.308(a)(3)(i)	Termination Procedures	A	Does the organization follow termination procedures that include checklists for collecting access-providing materials? If yes, are these procedures followed consistently? Are these termination procedures documented?	The company has termination procedures for employees and 3rd parties—reference in ISP 05- Human Resource Security Procedure.
11	Workforce Security §164.308(a)(3)(i)	Termination Procedures	A	Does the organization follow procedures for changing combinations and locking mechanisms? Are these procedures documented?	N/A. Access is terminated logically to all information systems that stores PHI.
12	Workforce Security §164.308(a)(3)(i)	Termination Procedures	A	Does the organization have documented termination checklists, which include procedures for removing user account(s) in a timely manner?	The company uses onboarding and termination checklists.
13	Information Access Management §164.308(a)(4)(i)	Isolating Healthcare Clearinghouse Function	R	If the organization includes a healthcare clearinghouse, what policies and procedures are there in place to isolate the clearinghouse electronic Protected	N/A

ID	Standards	Specifications	R/A	Related question	Existing controls
				Healthcare Information from the rest of the organization?	
14	Information Access Management §164.308(a)(4)(i)	Access Authorization	A	Are there rules established to determine the initial level of access an individual may have? Are these rules documented?	Access permissions are granted on a need-to-know basis only, described in ISP 07- Access Control Procedure.
15	Information Access Management §164.308(a)(4)(i)	Access Establishment and Modification	A	Does the organization follow procedures for governing access to information on a need-to-know basis? If yes, who is responsible for maintaining documentation of these procedures?	Yes. As described in ISP 07- Access Control Procedure.
16	Information Access Management §164.308(a)(4)(i)	Access Establishment and Modification	A	Does the organization have different levels of access to health information/data? Are there rules established for granting access and authorization? If yes, are these rules documented?	Access to data in the Vibrant application is upon user roles. Internal user's access is managed in the access matrix according to ISP 07- Access Control Procedure.
17	Information Access Management §164.308(a)(4)(i)	Access Establishment and Modification	A	Are there rules established for the modification of individual access authorizations? If yes, are these rules documented?	Yes. As described in ISP 07- Access Control Procedure.
18	Security Awareness and Training §164.308(a)(5)(i)	Security Reminders	A	Are periodic security reminders issued to all employees? If yes, are these reminders documented, and do you feel that it is effective?	Annual awareness training.
19	Security Awareness and Training §164.308(a)(5)(i)	Security Reminders	A	Is formal information security awareness training conducted for all employees, agents, and contractors? If yes, how often is it performed, and is periodic re-attendance	Annual awareness training to employees. All employees' attendance is required.

ID	Standards	Specifications	R/A	Related question	Existing controls
				required? Is the security awareness training program documented?	The training was done based on a dedicated learning system – HIPAA to BAA.
20	Security Awareness and Training §164.308(a)(5)(i)	Security Reminders	A	Does the organization conduct customized training sessions based on job responsibilities that focus on issues regarding the use of health information? Does the organization include the employee's responsibilities regarding confidentiality and security?	Vibrant is a small company. All employees are required to participate in annual training that comprehends all the topics relevant to all the roles.
21	Security Awareness and Training §164.308(a)(5)(i)	Protection from Malicious Software	A	If Security Awareness Training is conducted, does it include (at a minimum): (A) Virus protection, (B) Importance of monitoring login success/failure, and (C) Password management? Are these minimal requirements for Security Awareness Training documented?	Initial training was done based on a dedicated learning system – HIPAA to BAA.
22	Security Awareness and Training §164.308(a)(5)(i)	Protection from Malicious Software	A	Are there procedures in place to make sure virus checking software is installed and running on all computer systems within the organization?	The AWS production environment is monitored for viruses by AWS services. Organization networks and computers use Eset anti-virus managed by the IT.
23	Security Awareness and Training §164.308(a)(5)(i)	Protection from Malicious Software	A	Do these procedures include the requirement that virus definitions be consistently updated? If yes, what procedure do you use to update them, and how often?	Virus signatures are automatically updated when the software connects to the internet. The user is unable to change any anti-virus configurations. The settings are controlled by IT.

ID	Standards	Specifications	R/A	Related question	Existing controls
24	Security Awareness and Training §164.308(a)(5)(i)	Protection from Malicious Software	A	Do the procedures call for periodic scanning for viruses? How often is the virus software configured to scan for viruses?	The software is configured for online and weekly scans. The user is unable to change any anti-virus configurations. The settings are controlled by IT.
25	Security Awareness and Training §164.308(a)(5)(i)	Login monitoring	A	Are procedures implemented that provide for monitoring of failed login attempts in an organization's servers?	The vibrant application stores security logs about user login, failed login, account lockout, and admin activities. The system production environment in AWS is monitored by AWS services and configured to alert according to predefined rules.
26	Security Awareness and Training §164.308(a)(5)(i)	Login monitoring	A	What procedures are there in place to ensure failed login attempts are reported to the proper authority?	The application stores security logs about user login, failed login, account lockout, and admin activities. The system production environment in AWS is monitored by AWS services and configured to alert according to predefined rules.
27	Security Awareness and Training §164.308(a)(5)(i)	Password Management	A	What password guidelines exist, and what procedures are followed to ensure the user makes a good selection?	A strong and complex password policy is enforced in user login to network resources, AWS production environment, and web application. AWS management console and admin accounts in the web application require 2FA.

ID	Standards	Specifications	R/A	Related question	Existing controls
28	Security Awareness and Training §164.308(a)(5)(i)	Password Management	A	Do users sign a security statement when issued a password?	Internal users in the company sign an "Acceptable use of assets" policy.
29	Security Awareness and Training §164.308(a)(5)(i)	Password Management	A	What are password guidelines in place to protect the integrity of administrator-type accounts?	Administrator's accounts must use strong and complex passwords and MFA.
30	Security Incident Procedures §164.308(a)(6)(i)	Response and Reporting	R	Is there a formal process in place to allow the reporting of security breaches? If yes, to whom are these breaches reported, and are these processes documented?	ISP 10- Incident Response and Breach Notification Procedure include a reference for this requirement. Employees are trained about this procedure as part of the annual security awareness training.
31	Security Incident Procedures §164.308(a)(6)(i)	Response and Reporting	R	Are formal procedures followed for responding to incidents? If yes, which entity is responsible, and are they handled in a timely manner? Are these procedures documented?	ISP 10- Incident Response and Breach Notification Procedure include a reference for this requirement. The company management will handle an incident in cooperation with the professional, relevant entities, and the customers.
32	Security Incident Procedures §164.308(a)(6)(i)	Response and Reporting	R	Are procedures followed for mitigating incidents that may occur? Do the procedures also identify a team assigned to handle these incidents?	ISP 10- Incident Response and Breach Notification Procedure include a reference for this requirement.
33	Security Incident Procedures §164.308(a)(6)(i)	Response and Reporting	R	At the conclusion of an incident, are procedures followed to document the outcome of the incident investigation? Are	ISP 10- Incident Response and Breach Notification Procedure include a reference for this requirement.

ID	Standards	Specifications	R/A	Related question	Existing controls
				the results maintained in a historical file for subsequent review?	The HIPAA officer is required to document the incident, the investigation, and corrective actions.
34	Contingency Plan §164.308(a)(7)(i)	Data Backup Plan	R	Has a Data Backup Plan been implemented and followed within the organization? If yes, is the Data Backup Plan documented?	According to the company backup and restoration test procedure, PHI is stored in the application production environment on AWS and backed up at the AWS environment. Access to PHI databases and their backups is restricted to authorized personnel only, granted on a need-to-know basis, and periodically audited by the HIPAA officer.
35	Contingency Plan §164.308(a)(7)(i)	Data Backup Plan	R	Does the Data Backup Plan contain procedures for testing and revision? If so, are these procedures documented?	Testing and revision (if necessary) are done annually and documented.
36	Contingency Plan §164.308(a)(7)(i)	Data Backup Plan	R	Does the organization follow Data Backup Plan procedures that allow for an exact copy of the information to be retrieved? If yes, are Data Backup Plan policies and procedures formally documented?	According to the backup and restoration described in the ISP 09- Application Security Procedure.
37	Contingency Plan §164.308(a)(7)(i)	Data Backup Plan	R	What type of backups does the Data Backup plan call for? Full or incremental?	Full backups According to ISP 09- Application Security Procedure
38	Contingency Plan §164.308(a)(7)(i)	Data Backup Plan	R	Where is backup media stored? For how long?	At AWS, According to ISP 09- Application Security Procedure.
39	Contingency Plan §164.308(a)(7)(i)	Data Backup Plan	R	What physical protection mechanisms exist for local and remote copies of backups? What handling instructions are in place?	According to AWS policies.

ID	Standards	Specifications	R/A	Related question	Existing controls
40	Contingency Plan §164.308(a)(7)(i)	Disaster Recovery Plan	R	Has a Disaster Recovery Plan been developed? If yes, is the Disaster Recovery Plan document?	According to the description ISP 09- Application Security Procedure.
41	Contingency Plan §164.308(a)(7)(i)	Emergency Mode Operation Plan	R	Has an Emergency Mode Operation Plan been tested to determine continual operations? If yes, is the Emergency Mode Operation Plan documented?	Reference in ISP 07- Access Control Procedure.
42	Contingency Plan §164.308(a)(7)(i)	Emergency Mode Operation Plan	R	Does the emergency mode operation plan and disaster recovery plan address physical access to appropriate personnel? Is the emergency mode operations plan and procedures formally documented?	Reference in ISP 07- Access Control Procedure.
43	Contingency Plan §164.308(a)(7)(i)	Testing and Revision Procedure	A	Is the Disaster Recovery Plan periodically tested to ensure adequacy? If yes, is the testing documented? What types of testing are accomplished?	Yes. At AWS, According to ISP 09- Application Security Procedure.
44	Contingency Plan §164.308(a)(7)(i)	Applications and Data Criticality Analysis	A	Have Critical Systems been identified within your organization and documented within the Contingency Plan?	N/A
45	Contingency Plan §164.308(a)(7)(i)	Applications and Data Criticality Analysis	A	What are other types of mechanisms in place to allow for mission-critical hosts or systems to property shutdown?	N/A
46	Evaluation §164.308(a)(8)	No Implementation Specifications	R	Has an internal or external entity performed an assessment on any network or individual system(s) within the network to determine if they meet a pre-specified set of security standards? If yes, has any such assessment been documented?	The company intends to do a system penetration test when applicable.

ID	Standards	Specifications	R/A	Related question	Existing controls
47	Evaluation §164.308(a)(8)	No Implementation Specifications	R	Does the organization maintain a history of Technical Evaluations for the computer system(s) and network(s)?	The company intends to do a system penetration test when applicable.
48	Business Associate Contracts and Other Arrangements §164.308(b)(1)	Written Contract or Other Arrangement	R	Has an inventory of all electronic data exchanges with third parties, vendors, or business partners taken place? If yes, has a Business Associate agreement been executed? Are the inventory and agreement documented?	Yes. For now, there are no electronic data exchanges with third parties. Business associate agreements are signed when relevant.
49	Business Associate Contracts and Other Arrangements §164.308(b)(1)	Written Contract or Other Arrangement	R	Are you aware of any trusted internal or external business connections or any third-party connections or accesses? What are they?	For now, there are no trusted internal or external business connections or any third-party connections or accesses.
50	Facility Access Controls §164.310(a)(1)	Contingency Operations	A	Have procedures been implemented that provide for facility access and other business functions during contingency operations?	N/A.
51	Facility Access Controls §164.310(a)(1)	Facility Security Plan	A	Does the organization have a facility security plan? Is the facility security plan formally documented?	There is no PHI stored in the company offices. Logical access to PHI is restricted to authorized personnel according to ISP 07- Access Control Procedure.
52	Facility Access Controls §164.310(a)(1)	Facility Security Plan	A	Has the organization implemented procedures within the facility to sign in visitors and provide escorts, if appropriate? Are there formally documented procedures for visitor escort and sign-in?	Yes. ISP 06- Physical Security Procedure.

ID	Standards	Specifications	R/A	Related question	Existing controls
53	Facility Access Controls §164.310(a)(1)	Access Control and Validation Procedures	A	What procedures are there in place to ensure that maintenance personnel has proper access and authorization? Are these procedures documented?	N/A.
54	Facility Access Controls §164.310(a)(1)	Maintenance Records	A	Does the organization retain system maintenance records? Is there formal documentation for this procedure?	N/A.
56	Facility Access Controls §164.310(a)(1)	Maintenance Records	A	Does the organization maintain access authorization records? If so, how long are these records retained? Are these authorizations documented?	Yes. In the Access control matrix (presented).

Physical Safeguards

ID	Standards	Specifications	R/A	Related question	Cardlatch existing controls
1	Facility Access Controls §164.310(a)(1)	Contingency Operations	A	Have procedures been implemented that provides for facility access and other business functions during contingency operations?	N/A for the Vibrant systems or PHI databases. PHI is stored in AWS data centers according to AWS physical security procedures. The company does have a physical security procedure ISP-06 Rev.1.0 - that covers relevant physical security aspects.
2	Facility Access Controls §164.310(a)(1)	Facility Security Plan	A	Does the organization have a facility security plan? Is the facility security plan formally documented?	N/A for the Vibrant medical system or PHI databases.
3	Facility Access Controls §164.310(a)(1)	Facility Security Plan	A	Has the organization implemented procedures within the facility to sign in visitors and provide escorts, if appropriate? Are there formally documented procedures for visitor escort and sign-in?	Yes. ISP 06- Physical Security Procedure
4	Facility Access Controls §164.310(a)(1)	Access Control and Validation Procedures	A	What procedures are there to ensure that maintenance personnel has proper access and authorization? Are these procedures documented?	N/A for the company medical system or PHI databases.
5	Facility Access Controls §164.310(a)(1)	Maintenance Records	A	Does the organization retain system maintenance records? Is there formal documentation for this procedure?	N/A for the company medical system or PHI databases.

ID	Standards	Specifications	R/A	Related question	Cardlatch existing controls
6	Facility Access Controls §164.310(a)(1)	Maintenance Records	A	Does the organization retain facility maintenance records? Is there formal documentation for this procedure?	N/A for the company medical system or PHI databases.
7	Facility Access Controls §164.310(a)(1)	Maintenance Records	A	Does the organization maintain access authorization records? If so, how long are these records retained? Are these authorizations documented?	N/A for the company medical system or PHI databases.
8	Workstation Use §164.310(b)	No Implementation Specifications	R	Does the organization follow procedures for defined acceptable workstation use? Are there documented guidelines that outline proper functions?	Yes. Reference in ISP 03- Network & Computers Security Procedure and ISP 06- Physical Security Procedure. Also mentioned in the acceptable use of assets policy
9	Workstation Security §164.310(c)	No Implementation Specifications	R	Has the organization implemented physical safeguards to eliminate or minimize unauthorized access/viewing of health information on workstations?	Yes. Access permissions, strong authentication, computer lockdown after 15 minutes of unuse, Bitlocker hard drive encryption.
10	Workstation Security §164.310(c)	No Implementation Specifications	R	Does the organization implement console lock features?	AWS admin center/web application auto log off after 1 hour of unuse
11	Device and Media Controls §164.310(d)(1)	Disposal	R	Does the organization follow procedures for the final disposition of electronic data (including PHI) and the hardware that it resides on? Are these procedures documented?	Yes. Reference in ISP 04- Disposal of old computing equipment Procedure.
12	Device and Media Controls §164.310(d)(1)	Media Re-use	R	Have procedures been developed for removing electronic Protected Health	As a principal, PHI is not stored in employees computer local hard drives. However, the company

ID	Standards	Specifications	R/A	Related question	Cardlatch existing controls
				Information from media before it is scheduled for re-use?	have a procedure for disposal of old computing equipment Reference in ISP 04- Disposal of old computing equipment Procedure.
13	Device and Media Controls §164.310(d)(1)	Accountability	A	Does the organization follow procedures for taking hardware and software into or out of a facility? Are these procedures documented? Who is accountable for the movement of media?	As a principal PHI is not stored in employees computer local hard drives. However, the company guides the employees on the proper use of laptops outside the office. Those instructions are included in the "acceptable use of assets" document that every new employee signs.
.14	Device and Media Controls §164.310(d)(1)	Data Backup and Storage	A	Does the organization follow data storage procedures for electronic retention of individual health care information? Are there formally documented policies and procedures?	PHI stored in the AWS production environment on AWS and backed up at the AWS environment according to the company backup, and restoration test described in ISP 09- Application Security Procedure

Technical Safeguards

ID	Standards	Specifications	R/A	Related question	Cardlatch existing controls
1	Access Control §164.312(a)(1)	Unique User Identification	R	Are unique user ID(s) in place/use (network and application)? If yes, for which systems and are they governed by written security procedures?	Yes. Access to PHI is with a unique username only (AWS admin center/Direct SSH connections/ web application).
2	Access Control §164.312(a)(1)	Unique User Identification	R	Are there any shared IDs or non-unique IDs in use?	No. there are no shared IDs with access permissions to PHI.
3	Access Control §164.312(a)(1)	Unique User Identification	R	Do all end-users of network resources have a unique user ID?	Yes. Access to PHI is with a unique username only.
4	Access Control §164.312(a)(1)	Emergency Access Procedures	R	Is an emergency access procedure documented and followed?	Reference in ISP 07- Access Control Procedure.
5	Access Control §164.312(a)(1)	Automatic Logoff	A	Are controls in place and configured to allow for automatic logoffs (network and application)?	Web application logs off automatically after 1 hour of non-use.
6	Access Control §164.312(a)(1)	Automatic Logoff	A	Are there controls in place to ensure that data has not been altered or destroyed during transmission?	Data in transit is encrypted with SSL 1.2
7	Access Control §164.312(a)(1)	Encryption and Decryption	A	Is encryption currently in use with any access control solutions that are in place? If yes, how?	Data in transit is encrypted with SSL 1.2. Databases are encrypted with AWS standard encryption.
8	Access Control §164.312(a)(1)	Encryption and Decryption	A	Are access controls or encryption technologies used to secure the	Data in transit is encrypted with SSL 1.2

ID	Standards	Specifications	R/A	Related question	Cardlatch existing controls
				transmission of sensitive information? If yes, what and for which systems?	
9	Access Control §164.312(a)(1)	Encryption and Decryption	A	Are encryption technologies used to secure data at rest? If yes, for which systems?	Databases are encrypted with AWS standard encryption.
10	Audit Controls §164.312(b)	No Implementation Specifications	R	Are networked systems configured to allow event reporting? If yes, which types of systems?	The Vibrant application stores security logs about user login, failed login, account lockout, and admin activities. The system production environment in AWS is monitored by AWS services and configured to alert according to predefined rules
11	Audit Controls §164.312(b)	No Implementation Specifications	R	Are auditing capabilities enabled for file/record accesses, modifications, or deletions? If yes, for which systems and what activities are audited?	The Vibrant application stores security logs about user login, failed login, account lockout, and admin activities. The system production environment in AWS is monitored by AWS services and configured to alert according to predefined rules
12	Audit Controls §164.312(b)	No Implementation Specifications	R	Are there software or hardware solutions in place that will provide notification of abnormal conditions that may occur in a networked system?	The system production environment in AWS is monitored by AWS services and configured to alert according to predefined rules
13	Integrity §164.312(c)(1)	Mechanism to Authenticate EPHI	A	What process exists to determine who will have the authority to change or	According to user's role and permissions in the application.

ID	Standards	Specifications	R/A	Related question	Cardlatch existing controls
				manipulate health information? Is this process documented?	
14	Person or Entity Authentication §164.312(d)	No Implementation Specifications	R	How is the signature on the document/data verified as trust-worthy? Is online or offline validation as well as entity or non-entity certificate used?	User authentication. Admin authenticates with MFA.
15	Transmission Security §164.312(e)(1)	Integrity Controls	A	What policies, procedures, and technical mechanisms are in place to protect health information as it is transmitted across internal and external networks? Are these policies, procedures, and technical mechanisms documented?	Data in transit is encrypted with SSL 1.2 over HTTPS.
16	Transmission Security §164.312(e)(1)	Integrity Controls	A	What technical and administrative processes and mechanisms are in place to ensure the secure storage of health information? Are these processes documented?	Databases are encrypted with AWS standard encryption. See reference in ISP 09- Application Security Procedure
17	Transmission Security §164.312(e)(1)	Encryption	A	Is the message encrypted, signed, or signed and encrypted? What practices are in place for the storage of private (secret) keys?	The encryption keys are stored and maintain in AWS-KMS.
18	Transmission Security §164.312(e)(1)	Encryption	A	What cryptographic methods and parameters are used to ensure that the integrity of the message during transmission is unaltered?	Data in transit is encrypted with SSL 1.2 over HTTPS.

Organizational Requirements

ID	Standards	Specifications	R/A	Related question	Cardlatch existing controls
1	Business Associate Contracts and Other Arrangements §164.314(a)(1)	Business Associate Contracts	R	Are Business Associate contracts in place between the organization and any business associate that might come in contact with the organization's electronic Protected Health Information?	Not relevant at the moment. The company has a business associate agreement template to be used with relevant suppliers.
2	Business Associate Contracts and Other Arrangements §164.314(a)(1)	Other Arrangements	R	Are both the organization and the business associate a government agency? If yes, does a memorandum of understanding exist between the organization and the business associate that requires the business associate to implement reasonable and appropriate administrative, physical, and technical safeguards to protect electronic Protected Health Information?	N/A
3	Business Associate Contracts and Other Arrangements §164.314(a)(1)	Other Arrangements	R	Is the business associate required by law to perform a function or activity on behalf of the organization? If yes, describe what steps the organization has taken to ensure the business associate complied with the provisions of the HIPAA security rule.	N/A

ID	Standards	Specifications	R/A	Related question	Cardlatch existing controls
4	Requirements for Group Health Plans §164.314(b)(1)	Plan Documents	R	Does the organization have a group health plan? If yes, do the plan documents require the plan sponsor reasonably and appropriately safeguard electronic Protected Health Information?	N/A

Policies, Procedures, and Documentation Requirements

ID	Standards	Specifications	R/A	Related question	Cardlatch existing controls
1	Policy and Procedures §164.316(a)	No Implementation Specifications	R	Does the organization have formal documented and approved information security policy statements that encompass information values, information protection, and an overall organizational commitment?	ISP 01 - information security policy
2	Policy and Procedures §164.316(a)	No Implementation Specifications	R	Does the organization have a process for developing, approving, and publishing formal security policies?	
3	Documentation §164.316(b)(1)	Time Limit	R	Are documents related to electronic Protected Health Information maintained for the time period proscribed by this rule?	PHI retention is determined according to applicable regulatory requirements.
4	Documentation §164.316(b)(1)	Availability	R	Is this documentation available to those persons responsible for implementing the various procedures required by the HIPAA security rule?	Yes.
5	Documentation §164.316(b)(1)	Updates	R	Are the policies and procedures reviewed periodically to ensure adequacy and timeliness?	Annual review.

Conclusion

Vibrant LTD has completed the HIPAA Compliance exercise and has implemented all necessary controls and protections for all information collections.

Complying with HIPAA regulations is an ongoing process. This report is valid for the day it was provided.

The company will finish and verify the implemntation of relevant security measures such as system penetration test when it will be applicable.