**$CLIENT$**

**Security Risk Analysis**

**Month, 202X**

**Contents**

[Executive Summary 3](#_Toc459988689)

[Assessment Methodology 4](#_Toc459988690)

[Gap Assessment 5](#_Toc459988691)

[*Administrative Safeguards* 5](#_Toc459988692)

[*Physical Safeguards* 10](#_Toc459988693)

[*Technical Safeguards* 13](#_Toc459988694)

[*Documentation* 15](#_Toc459988695)

[*HITECH Act* 16](#_Toc459988696)

# Executive Summary

**Background and Scope**

Dotoreza was engaged by $CLIENT$ (“$CLIENT$”) to assess the state of $CLIENT$’ compliance with the HIPAA Security Rule (45 CFR Part 164, Subpart C), and with the revisions to the Security Rule that were passed into law by the HITECH Act of 2009. In 3Q 202X, we reviewed the administrative, physical, and technical safeguards around the electronic personal health information (PHI) that $CLIENT$ uses, stores, and transmits. Our specific observations on $CLIENT$’ compliance are matched to the individual safeguards that the HIPAA Security Rule details and are provided in the body of this report.

**Key Findings**

* $CLIENT$ is a new company with immature processes and a lack of documentation, as typical for companies of its size and age. While the existing documentation is sufficient for a company with only two co-founders, more processes should be documented as new workforce members are on-boarded.
* $CLIENT$ relies on third parties for many supporting services, such as X, Y, and Z. Many of the HIPAA safeguards are implemented by these third parties, which are industry leaders with the resources to implement them in a far more mature and thorough manner than $CLIENT$.

# Assessment Methodology

This analysis was limited to a review of documents provided by $CLIENT$ and detailed interviews with $CLIENT$ personnel. Limited sampling was performed on configuration and log files, and other artifacts, where available.

Compliance with the individual specific safeguards of the HIPAA Security Rule was scored using the following rating criteria:

|  |  |  |
| --- | --- | --- |
| $CLIENT$ Compliance | | Description |
| ⚫ | Full | $CLIENT$ appears to have implemented the safeguard adequately. |
| ⚫ | Partial | $CLIENT$ appears to have partially implemented the safeguard; however, improvements may be readily made. |
| ⚫ | Minimal | HIPAA safeguards are not implemented, or have only minimal compliance |
| ⚫ | N/A | Not applicable for the stated reason. |

For each control, supporting evidence was sought to confirm the observation made and to demonstrate the safeguards in place at $CLIENT$.

“Full” $CLIENT$ Compliance is only given to safeguards that both meet the HIPAA requirement and that produce supporting evidence of some sort, such as a document, report, or communication.

“Partial” $CLIENT$ Compliance was given to controls that a) were asserted by $CLIENT$ personnel, but not supported by sufficient evidence or b) partially met the HIPAA standard, due to lack of complete coverage of $CLIENT$ operations, outdated-ness, or some other flaw.

Controls that received a rating of “Minimal” or “N/A” Compliance either fall short of the standard, or are not applicable for some (noted) reason.

For the Source of Findings, an answer of “None” meant no supporting evidence was available within $CLIENT$; an answer of “N/A” meant that the control was out of the scope of this assessment.

Where a safeguard is labeled (Required), it is required by the Security Rule; those labeled (Addressable) are deemed “addressable” by the Security Rule. Those safeguards not labeled as either are Required. Where a HIPAA standard gave implementation specifications, those were reviewed; where no implementation specifications were given, compliance with the standard was reviewed.

# Gap Assessment

| HIPAA Clause | HIPAA Safeguard | Observations | Source of findings | Compliance |
| --- | --- | --- | --- | --- |
| Administrative Safeguards | | | | |
| **164.308 (a)(1)(ii)(A) Security Management Process** | Risk analysis (Required): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI held by the covered entity. | Concurrent with this Gap Analysis, Dotoreza performed a Security Risk Analysis. | $CLIENT$ Security Risk Analysis, v09-2024 | • |
| **164.308 (a)(1)(ii)(B) Security Management Process** | Risk management (Required): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. | The Security Risk Analysis produced a list of recommendations to better manage security risk. | $CLIENT$ Security Risk Analysis, v09-2024 | • |
| **164.308 (a)(1)(ii)(C) Security Management Process** | Sanction policy (Required): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. |  |  | • |
| **164.308 (a)(1)(ii)(D) Security Management Process** | Information system activity review (Required): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. |  |  | • |
| **164.308(a) (2) Assigned Security Responsibility.** | Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. |  |  | • |
| **164.308(a)(3)(ii) (A) Workforce Security** | Authorization and/or supervision (Addressable) Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. |  |  | • |
| **164.308(a)(3)(ii) (B) Workforce Security** | Workforce clearance procedures (Addressable): Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. |  |  | • |
| **164.308(a)(3)(ii) (C) Workforce Security** | Termination procedures (Addressable): Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (Addressable)(3)(ii)(B) of this section. |  |  | • |
| **164.308(a)(4)(ii) (A) Information Access Management** | Isolating healthcare clearinghouse functions (Required): If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the EPHI of the clearinghouse from unauthorized access by the larger organization. |  |  | • |
| **164.308(a)(4)(ii) (B) Information Access Management** | Access authorization (Addressable): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. |  |  | • |
| **164.308(a)(4)(ii) (C) Information Access Management** | Access establishment and modification (Addressable): Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. |  |  | • |
| **164.308(a)(5)(ii) (A) Security Awareness and Training** | Security reminders (Addressable): Implement periodic security updates. |  |  | • |
| **164.308(a)(5)(ii) (B) Security Awareness and Training** | Protection from malicious software (Addressable): Implement procedures for guarding against, detecting, and reporting malicious software. |  |  | • |
| **164.308(a)(5)(ii) (C) Security Awareness and Training** | Login monitoring (Addressable): Implement procedures for monitoring log-in attempts and reporting discrepancies. |  |  | • |
| **164.308(a)(5)(ii) (D) Security Awareness and Training** | Password management (Addressable): Implement procedures for creating, changing, and safeguarding passwords. |  |  | • |
| **164.308(a)(6)(ii) Security Incident Procedures** | Response and Reporting (Required): 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; and document security incidents and their outcomes. |  |  | • |
| **164.308(a)(7)(ii) (A) Contingency Plan** | Data backup plan (Required): Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. |  |  | • |
| **164.308(a)(7)(ii) (B)Contingency Plan** | Disaster recovery plan (Required): Establish (and implement as needed) procedures to restore any loss of data. |  |  | • |
| **164.308(a)(7)(ii) (C) Contingency Plan** | Emergency mode operation plan (Required). 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. | As $CLIENT$’ ePHI is not critical for care, an emergency mode operation plan is not in place. | Interview with $CLIENT$ personnel. | • |
| **164.308(a)(7)(ii) (D) Contingency Plan** | Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans. |  |  | • |
| **164.308(a)(7)(ii) (E) Contingency Plan** | Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components. |  |  | • |
| **164.308(a)(8) Evaluation** | Perform a periodic technical and non-technical evaluation to ensure that standards continue to be met in response to operational and environmental changes. |  |  | • |
| **164.308(b)(1)(4)**  **Business Associate Contracts and Other**  **Arrangements** | Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b) (1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a). |  |  | • |

| HIPAA Clause | HIPAA Safeguard | Observations | Source of findings | Compliance |
| --- | --- | --- | --- | --- |
| Physical Safeguards | | | | |
| **164.310(a)(2)(i) Facility Access Controls** | Contingency operations (Addressable). Establish (and implement as needed) 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. |  |  | • |
| **164.310(a)(2)(ii) Facility Access Controls** | Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. |  |  | • |
| **164.310(a)(2)(iii) Facility Access Controls** | Access control and validation procedures (Addressable). Implement 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. |  |  | • |
| **164.310(a)(2)(iv) Facility Access Controls** | Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks). |  |  | • |
| **164.310(b) Workstation Use** | Implement policies and procedures 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 workstation that can access electronic protected health information. |  |  | • |
| **164.310(c) Workstation Security** | Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. |  |  | • |
| **164.310(d)(2)(i) Device and Media Controls** | Disposal (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. |  |  | • |
| **164.310(d)(2)(ii) Device and Media Controls** | Media re-use (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use. |  |  | • |
| **164.310(d)(2)(iii) Device and Media Controls** | Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore. |  |  | • |
| **164.310(d)(2)(iv) Device and Media Controls** | Data backup and storage (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. |  |  | • |

| HIPAA Clause | HIPAA Safeguard | Observations | Source of findings | $CLIENT$ Compliance |
| --- | --- | --- | --- | --- |
| Technical Safeguards | | | | |
| **164.312(a)(2)(i) Access Control** | Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity. | There are no shared user IDs within $CLIENT$ systems. | Interview with $CLIENT$ personnel. | • |
| **164.312(a)(2)(ii) Access Control** | Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | As $CLIENT$’ ePHI is not critical for care, an emergency access procedure is not in place. | N/A | • |
| **164.312(a)(2)(iii) Access Control** | Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. |  |  | • |
| **164.312(a)(2)(iv) Access Control** | Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. |  |  | • |
| **164.312(b)**  **Audit Controls** | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. |  |  | • |
| **164.312(c)(2)**  **Integrity** | Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | $CLIENT$ relies on the integrity checking mechanisms of its filesystems to ensure/ verify the integrity of data at rest, and on TLS to ensure/verify the integrity of data in motion. | Interview with $CLIENT$ personnel. | • |
| **164.312(d)**  **Person or Entity Authentication** | Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | All persons and entities must first authenticate themselves via username and password before access is granted to any ePHI stored on $CLIENT$ systems. | Interview with $CLIENT$ personnel. | • |
| **164.312(e)(1)(i) Transmission Security** | Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | All transmissions to and from $CLIENT$’ system are encrypted with TLS 1.3, which also ensures integrity. | Interview with $CLIENT$ personnel. | • |
| **164.312(e)(1)(ii) Transmission Security** | Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | All transmissions to and from $CLIENT$’ system are encrypted with TLS 1.3. | Interview with $CLIENT$ personnel. | • |

| HIPAA Clause | HIPAA Safeguard | Observations | Source of findings | Compliance |
| --- | --- | --- | --- | --- |
| Documentation | | | | |
| **164.316(a)**  **Policies and Procedures** | Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications or other requirements of the law. | $CLIENT$ has the reasonable and appropriate policies and procedures for a company of its size and maturity. | Interview with $CLIENT$ personnel. | • |
| **164.316(b)(1)(i)**  **Documentation** | Maintain the policies and procedures in written form, which may be electronic. | Policies are maintained in $. | Interview with $CLIENT$ personnel. | • |
| **164.316(b)(1)(ii)**  **Documentation** | If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment. | BAAs and security incidents and their outcomes are stored in $.  Grants of user access are documented in $ | Interview with $CLIENT$ personnel. | • |
| **164.316(b)(2)(i) Documentation** | Retain the documentation for six years from the date of its creation or the date when it last was in effect, whichever is later. | Policies are maintained indefinitely. | Interview with $CLIENT$ personnel. | • |
| **164.316(b)(2)(ii) Documentation** | Make documentation available to those individuals responsible for implementing the procedures to which the documentation pertains. | Policies are accessible to all workforce members. | Interview with $CLIENT$ personnel. | • |
| **164.316(b)(2)(iii) Documentation** | Review the documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of EPHI. | Policies are updated as needed. | Interview with $CLIENT$ personnel. | • |

| HITECH Clause | HITECH Requirement | Observations | Source of findings | $CLIENT$ Compliance |
| --- | --- | --- | --- | --- |
| HITECH Act | | | | |
| **13402(a)**  **Breach Notification** | A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach. | No such notice has been needed to date. | Interview with $CLIENT$ personnel. | • |
| **13405(e)**  **Access to Certain Information in Electronic Format** | In applying section 164.524 of title 45, Code of Federal Regulations, in the case that a covered entity uses or maintains an electronic health record with respect to protected health information of an individual—  (1) the individual shall have a right to obtain from such covered entity a copy of such information in an electronic format and, if the individual chooses, to direct the covered entity to transmit such copy directly to an entity or person designated by the individual, provided that any such choice is clear, conspicuous, and specific; and  (2) notwithstanding paragraph (c)(4) of such section, any fee that the covered entity may impose for providing such individual with a copy of such information (or a summary or explanation of such information) if such copy (or summary or explanation) is in an electronic form shall not be greater than the entity’s labor costs in responding to the request for the copy (or summary or explanation). | N/A. $CLIENT$ does not maintain an EHR. | N/A | • |
| **13408**  **Business Associate Contracts Required for Certain Entities.** | Each organization, with respect to a covered entity, that provides data transmission of protected health information to such entity (or its business associate) and that requires access on a routine basis to such protected health information, such as a Health Information Exchange Organization, Regional Health Information Organization, E prescribing Gateway, or each vendor that contracts with a covered entity to allow that covered entity to offer a personal health record to patients as part of its electronic health record, is required to enter into a written contract (or other written arrangement) described in section 164.502(e)(2) of title 45, Code of Federal Regulations and a written contract (or other arrangement) described in section 164.308(b) of such title, with such entity and shall be treated as a business associate of the covered entity for purposes of the provisions of this subtitle and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of the date of enactment of this title. | N/A. $CLIENT$ does not provide such services. | N/A | • |