**$CLIENT$**

**Security Risk Analysis**

**Month, 202X**

Table of Contents

[Introduction 3](#_Toc434411357)

[Scope 3](#_Toc434411358)

[Methodology 3](#_Toc434411359)

[System Characterization 4](#_Toc434411360)

[Threat Identification 5](#_Toc434411361)

[Vulnerability Identification 8](#_Toc434411362)

[Control Analysis 9](#_Toc434411363)

[Likelihood Determination 13](#_Toc434411364)

[Impact Analysis 14](#_Toc434411365)

[Risk Determination 15](#_Toc434411366)

[Control Recommendations 21](#_Toc434411367)

[Revision History 23](#_Toc434411368)

# Introduction

In order to better protect our customers’ sensitive information, and to comply with the Health Insurance Portability and Accountability Act (HIPAA), $CLIENT$ (“$CLIENT$”) conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic protected health information it holds. This assessment was initially performed in $MONTH$ 2025 and will be updated regularly by $CLIENT$ personnel.

## Scope

This assessment covers all ePHI that $CLIENT$ creates, receives, maintains, or transmits.

## Methodology

The risk assessment was performed by Dotoreza with assistance from $CLIENT$. The participants used their knowledge of $CLIENT$’ operations, their expertise in the healthcare and technology fields, and interviews with employees to perform the risk assessment, following the methodology described in NIST Special Publication 800-30r1, “Guide for Conducting Risk Assessments”. Definitions of terms used in this document can be found in that document, or online at csrc.nist.gov.

System Characterization was done by manual review of data and system inventories.

Vulnerability information was taken from the National Vulnerability Database at the National Institute for Standards and Technology (NIST), at nvd.nist.gov.

Identifying threats, determining the likelihood of particular threats, and their impact on ePHI, was assessed on a qualitative Low-Medium-High scale assigned by the risk assessment team where no historical information existed. A threat that had occurred more than once in the past year was given a likelihood of “High”, and that had occurred once in the past two years was given a likelihood of “Medium”.

Control recommendations were made based on the prior analysis, taking into account best practices, resource constraints, and what controls would be reasonable and appropriate for the $CLIENT$ environment.

# System Characterization

* Business, clients, and ephi uses/processed.
* 100% remote / physical description
* Workforce members, organization.
* The asset inventory that contains ePHI is:
  + Amazon Web Services (AWS),
* Other important systems, that do not contain ePHI, are:
* Engineering and risk management processes
* Data backup
* Workstations and mobile devices.
* Third party management
* Remote access is provided by the AWS Console interface to the systems hosted there, and to Google Workspace systems via the web interface. No on-premises systems are in use at $CLIENT$.

# Threat Identification

The below table documents the threats facing $CLIENT$’ ePHI.

| **#** | **Threat Type** | **Threat-Source** | **Threat Action** |
| --- | --- | --- | --- |
| 1 | Natural | Severe Weather (Thunderstorm, Hurricane, Tornado, Snow, Ice) | Power Outage  Communications Outage |
| 2 | Natural | Flood (Of any kind) | Power Outage  Communications Outage  Physical Damage to Systems |
| 3 | Natural | Fire | Power Outage  Communications Outage  Physical Damage to Systems |
| 4 | Human | Snooping Insider | Data Leakage  Data Tampering  Privilege Elevation  Unauthorized Access |
| 5 | Human | Careless Insider | Data Leakage  Denial of Service  Installation of Malicious Code  Data Tampering  Encryption compromise |
| 6 | Human | Malicious Insider | Cracking  Social Engineering  Denial of Service  Defacing  Data Tampering  Data Theft  Resource Poaching  Installation of Malicious Code  Encryption compromise |
| 7 | Human | Snooping 3rd Party (A 3rd party has logical and/or physical access to our information, but is not an employee) | Data Leakage  Data Tampering  Privilege Elevation  Unauthorized Access |
| 8 | Human | Careless 3rd Party | Data Leakage  Denial of Service  Installation of Malicious Code  Data Tampering  Encryption compromise |
| 9 | Human | Malicious 3rd Party | Cracking  Social Engineering  Denial of Service  Defacing  Data Tampering  Data Theft  Resource Poaching  Installation of Malicious Code  Encryption compromise |
| 10 | Human | External Attacker | Cracking  Social Engineering  Denial of Service  Defacing  Data Tampering  Data Theft  Installation of Malicious Code  Encryption compromise |
| 11 | Human | Malware (Non-human external attacker) | Cracking  Denial of Service  Defacing  Data Tampering  Data Theft  Resource Poaching  Installation of Malicious Code  Encryption compromise |
| 12 | Human | Careless Service Provider | Data Leakage  Denial of Service  Data Tampering  Encryption compromise  Service Outage |
| 13 | Environmental | Electrical Failure | Power Outage  Electrical Damage to Systems |
| 14 | Environmental | Telecommunications Failure | Network Outage |
| 16 | Environmental | Hardware Failure | Physical Damage to Systems  System Shut-down |

# Vulnerability Identification

The below list of vulnerabilities was taken from the NIST National Vulnerability Database, and the knowledge of the personnel performing the risk assessment.

| **#** | **Type** | **Vulnerability** | **Identifying Source** |
| --- | --- | --- | --- |
|  | People | Key person | Risk Assessment process |
|  | People | Careless employees | Risk Assessment process |
|  | People | Vulnerabilities in 3rd parties | Risk Assessment process |
|  | People | Weak passwords | NIST NVD |
|  | Processes | Insufficient system change controls | NIST NVD |
|  | Processes | Lost or stolen laptops | Risk Assessment process |
|  | Processes | Weak or absent security policies | NIST NVD |
|  | Technology – application | Excessive user permissions | NIST NVD |
|  | Technology – application | Un-validated data | NIST NVD |
|  | Technology – network | Open or unneeded network ports | NIST NVD |
|  | Technology – network | Single points of failure – network | NIST NVD |
|  | Technology – network | Weak or missing encryption of data in motion | NIST NVD |
|  | Technology - O/S | Flawed software without a patch | NIST NVD |
|  | Technology - O/S | Unpatched software | NIST NVD |
|  | Technology - O/S | Weak or missing encryption of data at rest on laptops | Risk Assessment process |
|  | Technology – physical | Electrically unshielded equipment | NIST NVD |
|  | Technology – physical | Insufficient physical security | NIST NVD |
|  | Technology - physical | Insufficient power capability | NIST NVD |
|  | Technology - physical | Misconfigured hardware or software | NIST NVD |
|  | Technology - physical | Poor plumbing | NIST NVD |
|  | Technology - physical | Single points of failure – hardware | NIST NVD |

# Control Analysis

The below table documents the preventative, detective, and compensating controls in place to minimize the likelihood or impact of ***any*** threat’s exercising a particular vulnerability.

| **#** | **Vulnerability** | **Preventative Controls** | **Detective Controls** | **Compensating Controls** |
| --- | --- | --- | --- | --- |
|  | Key person |  |  | * Business Associates provide the vast majority of support for their systems. |
|  | Careless employees |  |  |  |
|  | Vulnerabilities in 3rd parties | * Business Associates are contractually obligated to use reasonable and appropriate safeguards to prevent unauthorized use or disclosure of ePHI. * Business Associates are contractually obligated to implement administrative, physical, and technical safeguards in accordance with the HIPAA Security Rule. * No other third parties have access to ePHI. | * Business Associates are contractually obligated to notify $CLIENT$ of any unauthorized use or disclosure of ePHI. |  |
|  | Weak passwords |  |  | * Workstations do not contain ePHI. |
|  | Insufficient system change controls | * Cloud providers perform their own changes to the systems hosted there. * Workstations change infrequently. |  | * Workstations do not contain ePHI. * The hosted nature of cloud systems provides redundancy and availability of information from any system. |
|  | Lost or stolen laptops |  |  | * Workstations do not contain ePHI. |
|  | Weak or absent security policies |  |  |  |
|  | Excessive User Permissions |  |  |  |
|  | Un-validated data |  |  |  |
|  | Open or unneeded network ports | * The local firewall on laptops would block most hostile or unneeded network traffic. |  |  |
|  | Single points of failure – network |  |  | * The hosted nature of cloud systems provides redundancy and availability of information from any location. |
|  | Weak or missing encryption of data in motion | * Transmissions to and from $CLIENT$ are encrypted with HTTPS. |  |  |
|  | Flawed Software without a patch |  |  |  |
|  | Unpatched Software |  |  | * The hosted nature of cloud systems limits the impact of local software vulnerabilities to the affected system. |
|  | Weak or missing encryption of data at rest on laptops |  |  | * Laptops do not contain ePHI. |
|  | Electrically Unshielded Equipment |  |  | * The hosted nature of cloud systems provides redundancy and availability of information from any location. |
|  | Insufficient physical security |  |  | * ePHI is not stored on local systems. |
|  | Insufficient power capability |  |  |  |
|  | Misconfigured hardware or software | * Workstations are configured infrequently. |  | * Local systems do not contain ePHI. * The hosted nature of cloud systems provides redundancy and availability of information from any system. |
|  | Poor plumbing |  |  | * The hosted nature of cloud systems provides redundancy and availability of information from any location. |
|  | Single points of failure – hardware |  |  | * The hosted nature of cloud systems provides redundancy and availability of information from any system. |

# Likelihood Determination

The likelihood rating of a particular threat exercising a potential vulnerability within our environment was determined based on four factors:

* Historical information, where available;
* Threat-source motivation and capability;
* Nature of the vulnerability; and
* Existence and effectiveness of current controls.

Where historical information was not available, the Risk Assessment team used their professional knowledge to estimate the other three factors. The likelihood that a potential vulnerability could be exercised by a given threat-source was described as high, medium, or low:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Historical Record** | **Threat Motivation** | **Vulnerability Nature** | **Current Controls** |
| **Likelihood** |
| *High* | The threat has exploited the vulnerability at least once in the past year. | The threat is specifically targeting us. | The vulnerability requires no particular skill or coincidence to exploit. | There are no controls in place against the threat/vulnerability pair. |
| *Medium* | The threat has exploited the vulnerability at least once in the past 2 years. | The threat is opportunistic. | The vulnerability requires some skill or coincidence to exploit. | There is at least one type of control  in place against the threat/vulnerability pair. |
| *Low* | The threat has not exploited the vulnerability in the past 2 years. | The threat is unmotivated or non-human. | The vulnerability requires expertise to exploit. | There is more than one type of control in place against the threat/vulnerability pair. |

For ease of reading, the results of the likelihood determination are documented in the section “Risk Determination”, below.

# Impact Analysis

To analyze the impact of a threat exercising a particular vulnerability, the Risk Assessment team used the matrix below.

|  |  |
| --- | --- |
| **Impact Level** | **Impact Definition** |
| ***High*** | The threat/vulnerability pair would impair our ability to deliver care, fulfill regulatory mandates, be a reportable breach of unsecured ePHI, or seriously impact operations. |
| ***Medium*** | The threat/vulnerability pair would require a good deal of time and effort to recover from, or open additional vulnerabilities in our infrastructure. |
| ***Low*** | The threat/vulnerability pair would not meet either of the criteria above. |

For ease of reading, the results of the impact analysis are documented in the section “Risk Determination”, below.

# Risk Determination

The determination of risk for a particular threat/vulnerability pair was expressed as a function of:

* The magnitude of the impact should a threat-source successfully exercise the vulnerability, determined in the Impact Analysis phase; and
* The likelihood of a given threat-source’s attempting to exercise a given vulnerability, determined in the Likelihood Determination phase.

(Recall that Likelihood Determination includes the control environment in place). Threat/Vulnerability pairs that were judged to be so unlikely as to not merit analysis or controls were rated “negligible” and not included in the written analysis.

The risk was calculated as below:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Impact** | | |
| **Likelihood** | ***High*** | ***Medium*** | ***Low*** |
| ***High*** | High | High | Medium |
| ***Medium*** | High | Medium | Low |
| ***Low*** | Medium | Low | Low |

Below find the documented risks, sorted by risk rating:

| # | Threat | Vulnerability | Likelihood | Impact | Risk Rating |
| --- | --- | --- | --- | --- | --- |
|  | External Attacker | Careless employees | L | H | M |
|  | External Attacker | Excessive user permissions | L | H | M |
|  | External Attacker | Flawed software without a patch | L | H | M |
|  | External Attacker | Insufficient physical security | L | H | L |
|  | Electrical Failure | Insufficient power capability | L | H | L |
|  | Fire | Insufficient power capability | L | H | L |
|  | Flood | Insufficient power capability | L | H | L |
|  | Severe Weather | Insufficient power capability | L | H | L |
|  | External Attacker | Lost or stolen laptops | L | H | L |
|  | External Attacker | Misconfigured hardware or software | L | H | L |
|  | External Attacker | Open or unneeded network ports | L | H | L |
|  | External Attacker | Rogue devices | L | H | L |
|  | Careless 3rd Party | Single points of failure – network | L | H | L |
|  | Careless Insider | Single points of failure – network | L | H | L |
|  | Careless Service Provider | Single points of failure – network | L | H | L |
|  | External Attacker | Single points of failure – network | L | H | L |
|  | Fire | Single points of failure – network | L | H | L |
|  | Flood | Single points of failure – network | L | H | L |
|  | Severe Weather | Single points of failure – network | L | H | L |
|  | Telecom. Failure | Single points of failure – network | L | H | L |
|  | External Attacker | Unpatched software | L | H | L |
|  | External Attacker | Un-validated data | L | H | L |
|  | External Attacker | Vulnerabilities in 3rd parties | L | H | L |
|  | Careless 3rd Party | Weak or missing encryption of data at rest on laptops | L | H | L |
|  | Careless Insider | Weak or missing encryption of data at rest on laptops | L | H | L |
|  | External Attacker | Weak or missing encryption of data at rest on laptops | L | H | L |
|  | Malicious 3rd Party | Weak or missing encryption of data at rest on laptops | L | H | L |
|  | Malicious Insider | Weak or missing encryption of data at rest on laptops | L | H | L |
|  | Snooping 3rd Party | Weak or missing encryption of data at rest on laptops | L | H | L |
|  | Snooping Insider | Weak or missing encryption of data at rest on laptops | L | H | L |
|  | External Attacker | Weak or missing encryption of data in motion | L | H | L |
|  | External Attacker | Weak passwords | L | H | L |
|  | Electrical Failure | Electrically unshielded equipment | L | L | L |
|  | Severe Weather | Electrically unshielded equipment | L | L | L |
|  | Severe Weather | Key person | L | L | L |
|  | Flood | Poor plumbing | L | L | L |
|  | Electrical Failure | Single points of failure – hardware | L | L | L |
|  | External Attacker | Single points of failure – hardware | L | L | L |
|  | Fire | Single points of failure – hardware | L | L | L |
|  | Hardware Failure | Single points of failure – hardware | L | L | L |
|  | Careless 3rd Party | Careless employees | L | M | L |
|  | Careless Insider | Careless employees | L | M | L |
|  | Malicious 3rd Party | Careless employees | L | M | L |
|  | Malicious Insider | Careless employees | L | M | L |
|  | Malware | Careless employees | L | M | L |
|  | Snooping 3rd Party | Careless employees | L | M | L |
|  | Snooping Insider | Careless employees | L | M | L |
|  | Careless Service Provider | Electrically unshielded equipment | L | M | L |
|  | Careless 3rd Party | Excessive user permissions | L | M | L |
|  | Careless Insider | Excessive user permissions | L | M | L |
|  | Malicious 3rd Party | Excessive user permissions | L | M | L |
|  | Malicious Insider | Excessive user permissions | L | M | L |
|  | Malware | Excessive user permissions | L | M | L |
|  | Snooping 3rd Party | Excessive user permissions | L | M | L |
|  | Snooping Insider | Excessive user permissions | L | M | L |
|  | Careless Service Provider | Flawed software without a patch | L | M | L |
|  | Malware | Flawed software without a patch | L | M | L |
|  | Careless 3rd Party | Insufficient physical security | L | M | L |
|  | Careless Insider | Insufficient physical security | L | M | L |
|  | Careless Insider | Insufficient power capability | L | M | L |
|  | Careless Service Provider | Insufficient power capability | L | M | L |
|  | Careless 3rd Party | Insufficient system change controls | L | M | L |
|  | Careless Insider | Insufficient system change controls | L | M | L |
|  | Careless Service Provider | Insufficient system change controls | L | M | L |
|  | External Attacker | Insufficient system change controls | L | M | L |
|  | Malicious Insider | Insufficient system change controls | L | M | L |
|  | Careless Insider | Key person | L | M | L |
|  | Malicious Insider | Key person | L | M | L |
|  | Snooping Insider | Key person | L | M | L |
|  | Careless 3rd Party | Lost or stolen laptops | L | M | L |
|  | Careless Insider | Lost or stolen laptops | L | M | L |
|  | Malicious 3rd Party | Lost or stolen laptops | L | M | L |
|  | Malicious Insider | Lost or stolen laptops | L | M | L |
|  | Snooping 3rd Party | Lost or stolen laptops | L | M | L |
|  | Snooping Insider | Lost or stolen laptops | L | M | L |
|  | Careless Service Provider | Misconfigured hardware or software | L | M | L |
|  | Careless Service Provider | Open or unneeded network ports | L | M | L |
|  | Malware | Open or unneeded network ports | L | M | L |
|  | Careless Service Provider | Poor plumbing | L | M | L |
|  | Severe Weather | Poor plumbing | L | M | L |
|  | Malicious 3rd Party | Rogue devices | L | M | L |
|  | Malicious Insider | Rogue devices | L | M | L |
|  | Careless 3rd Party | Single points of failure – hardware | L | M | L |
|  | Careless Insider | Single points of failure – hardware | L | M | L |
|  | Careless Service Provider | Single points of failure – hardware | L | M | L |
|  | Flood | Single points of failure – hardware | L | M | L |
|  | Careless Service Provider | Unpatched software | L | M | L |
|  | Malware | Unpatched software | L | M | L |
|  | Careless 3rd Party | Un-validated data | L | M | L |
|  | Careless Insider | Un-validated data | L | M | L |
|  | Careless Service Provider | Un-validated data | L | M | L |
|  | Malicious 3rd Party | Un-validated data | L | M | L |
|  | Malicious Insider | Un-validated data | L | M | L |
|  | Careless 3rd Party | Vulnerabilities in 3rd parties | L | M | L |
|  | Careless Insider | Vulnerabilities in 3rd parties | L | M | L |
|  | Careless Service Provider | Vulnerabilities in 3rd parties | L | M | L |
|  | Malicious 3rd Party | Vulnerabilities in 3rd parties | L | M | L |
|  | Malicious Insider | Vulnerabilities in 3rd parties | L | M | L |
|  | Malware | Vulnerabilities in 3rd parties | L | M | L |
|  | Snooping 3rd Party | Vulnerabilities in 3rd parties | L | M | L |
|  | Snooping Insider | Vulnerabilities in 3rd parties | L | M | L |
|  | Malicious Insider | Weak or absent security policies | L | M | L |
|  | Snooping 3rd Party | Weak or absent security policies | L | M | L |
|  | Snooping Insider | Weak or absent security policies | L | M | L |
|  | Careless 3rd Party | Weak or missing encryption of data in motion | L | M | L |
|  | Careless Insider | Weak or missing encryption of data in motion | L | M | L |
|  | Malicious 3rd Party | Weak or missing encryption of data in motion | L | M | L |
|  | Malicious Insider | Weak or missing encryption of data in motion | L | M | L |
|  | Snooping 3rd Party | Weak or missing encryption of data in motion | L | M | L |
|  | Snooping Insider | Weak or missing encryption of data in motion | L | M | L |
|  | Malicious 3rd Party | Weak passwords | L | M | L |
|  | Malicious Insider | Weak passwords | L | M | L |
|  | Snooping Insider | Weak passwords | L | M | L |

# Control Recommendations and Remediation Plan

For each High and Medium risk, and selected Low risks, the Risk Assessment team considered if additional controls were reasonable and appropriate around the associated vulnerability. The agreed-upon controls are listed below.

| **#** | **Vulnerability** | **Additional Control** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Revision History

This Risk Assessment will be reviewed and updated annually. The Review History is below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Reviewer** | **Updates Made** |
|  |  | Initial draft |
|  |  |  |