Privacy and Security
Risk Assessment Report

Organization Name

ICHOR Health and Wellness Center

Submitted by

Robert Taylor Martin, Jr.

Submitted to

Professor Tennille Gifford MSN, RN, RN-BC, CPHIMS

Directions

This is a privacy and security risk assessment report template. Refer to the desk audits you conducted in modules 2, 3, and 4 as you work on this document, as they contain the information you need to complete this template.

The Privacy and Security Risk Assessment Report Template includes sections for you to complete and supporting information and instructions to assist you in understanding the federal requirements for privacy and security in health care. Once you have filled in all of the information needed in this template, you will have created a Privacy and Security Assessment Report. Completion of this assessment for an organization meets one of the requirements for Meaningful Use standards and attestation.

The areas in this template that you need to complete will be indicated as text boxes or tables to type in your content. Follow the directions in each section to meet the template.

*This template is based on the following, which may be used as references.

- Office for Civil Rights ("OCR") HIPAA Security Standards: Guidance on Risk Analysis Requirements under the HIPAA Security Rule – https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
- Dept. of Health and Human Service (HHS) HIPAA Security Series: Basics of Risk Analysis and Risk Management - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf

Things to Consider

The following is a general overview of things to consider when creating a Privacy and Security Risk Assessment Report.

1. **Identify the scope of the analysis.** It would help if you considered all ePHI (electronic patient health information) created, received, maintained, or transmitted by the organization. Electronic media could range from a single workstation in a small practice to networks in organizations with multiple locations.
2. **Gather data.** Gather information about how the ePHI is stored, received, maintained, or transmitted. For example, solo practice with paper medical records may identify its ePHI by analyzing how it uses its billing software. Be sure to consider any portable electronic media used by the organization, such as an iPhone or iPad.
3. **Identify and document potential threats and vulnerabilities.** First, list natural, environmental, and human threats, with the latter probably being of most significant concern. Potential human hazards include employees (the most common source), ex-employees, and visitors to hackers and criminals. Anyone

who has the access, knowledge, and motivation "to cause an adverse impact" on your practice can act as a threat. Then, note the practice's vulnerabilities to the hazards you have identified. The practice's vendors may be able to help you determine system vulnerabilities.

4. **Assess current security measures.** These can be both technical and non-technical. Technical measures are part of information systems hardware and software, such as access controls, identification, authentication, encryption methods, automatic logoff, and audit controls. Nontechnical measures are management and operational controls, such as policies, procedures, standards, guidelines, accountability and responsibility, and physical and environmental security measures.
5. **Determine the likelihood of threat occurrence.**
6. **Determine the potential impact of threat occurrence.** The most common outcomes include, but are not limited to, unauthorized access to or disclosure of ePHI, permanent loss or corruption of ePHI, temporary loss or unavailability of ePHI, or loss of cash flow.
7. **Determine the level of risk**. Use what you wrote down for steps 5 and 6 to do this step. You might create a risk level matrix using a high, medium, and low rating system. For example, a threat likelihood value of "high" combined with an impact value of "low" may equal a risk level of "low." Or, a threat likelihood value of "medium" combined with an impact value of "medium" may equal a risk level of "medium."
8. **Identify security measures and finalize documentation.** Keep in mind the HIPAA Security Rule (see https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html) does not require a specific format for your analysis. When you use this template, you will provide a summary. In that summary report, you will outline your analysis process, record the result of each step, and identify needed security measures. Implementation of the identified security measures is a separate process from the risk analysis.

Part I: Executive Summary

This section will provide a one- to a two-paragraph summary of the organization's HIPAA Privacy and Security Risk Assessment and Mitigation Plan. You do not need to provide extensive detail, as executive summaries are brief and to the point and give an overview of the assessment and next steps.

Following the standards set forth under federal and state statutory requirements (hereafter referred to as regulatory requirements), ICHOR Health and Wellness Center is committed to ensuring all protected health information's confidentiality, integrity, and availability (PHI/ePHI), confidential. Sensitive data (hereafter referred to as covered information) creates, receives, maintains, and transmits at a reasonable and appropriate level with the associated classification level, regardless of format (i.e., electronic, paper, voice, etc.).

The purpose of this procedure is to define ICHOR Health and Wellness Center's information security risk management program. This policy outlines the scope, responsibilities, and processes associated with risk identification, assessment/analysis, mitigation, acceptance, continuous monitoring, and revalidation.

Part II: Scope

In this section, indicate the scope of the assessment with one paragraph or more. Indicate the setting assessed during the audits and where ePHI/ PHI data is stored.

The principal goal of the ICHOR Health and Wellness Center information security risk management program is to identify and mitigate risks to the confidentiality, integrity, and availability of covered information, including the people, processes, and technology that use, support, or manage covered information. The information security risk management program is not a technical function carried out exclusively Information and Technology Services (ITS), but rather a business process that requires involvement from many different people (e.g., senior leadership, middle management, ITS, People and Culture, Legal, Privacy, etc.) in the organization.

The risk management program's objective is to assess continually, control, monitor, and respond to the risks to ICHOR Health and Wellness Center's assets, clients, workforce, and covered information that ICHOR Health and Wellness Center is entrusted with and required protection. Additionally, risk management ensures that controls/safeguards are not applied unnecessarily. Risk is evaluated based on likelihood and impact from a loss of confidentiality, integrity, and availability of covered information and associated assets.

Part III: Risk Assessment and User Access

Risk Assessment Methodology

In this section, indicate how the assessment occurred. Was it conducted onsite, as a desk audit, or a combination of the two? This section is less than a paragraph and provides the reader with a brief understanding of how the assessment was carried out.

> **Risk analysis is an integral part of the risk management program. Without risk analysis, the program cannot be successful. This procedure describes several risk analysis approaches ICHOR Health and Wellness Center utilizes to meet the specific situation. The remainder of this procedure describes each of the following core risk management program processes:**
>
> - **Risk Assessment/Analysis**
> - **Risk Mitigation**
> - **Risk Acceptance**
> - **Continuous Monitoring**
> - **Revalidation**

Security Officer

Indicate who the organization's privacy and security officers are. Include their title in the organization. Many organizations have a privacy and security officer role that one person holds.

> **The term "risk management team" refers to individuals who are knowledgeable about the covered entity's HIPAA Privacy, Security and HITECH policies, procedures, training program, computer system set up and technical security controls, and who are responsible for the risk management process and methods outlined in this Policy. ICHOR Health and Wellness Center's risk management team includes but is not limited to:**
>
> - **Chief Compliance Officer**
> - **Senior Director for IT**
> - **HIPAA Privacy Officer(s)**
> - **HIPAA Security Officer or designee**
> - **Information Security Officer**
> - **Other designated subject matter experts**

Inventory

Identify how ePHI is created, stored, received, or transmitted. This includes identifying internal sources (e.g., servers, desktop computers, etc.) and external sources of ePHI, such as vendors or consultants who create, receive, maintain or transmit ePHI. Also,

indicate if there is a documented process for updating the inventory. Include how paper-based documents containing PHI are managed and disposed of.

ICHOR Health and Wellness Center respects the right to privacy for all individuals. It protects the confidentiality, integrity, and availability of data that contain electronically protected health information (ePHI) as required by HIPAA Security Rule, Contingency Plan, Data Backup Plan. 45CFR § 164.308(a)(7)

The term "backup" refers to the process of making an electronic copy of data stored in a computer system. Examples of backups include:

- **Whole/complete backup (backup/image of all (selected) data, programs, files on the system)**
- **Incremental backup (backup that only contains files that have changed since the most recent backup, either total or cumulative)**
- **Snap-shot back-up/image backup (process to restore/recover the system at a particular state, at a specific point in time)**
- **If a system does not allow for an electronic backup, the department will develop an alternative method to create a copy of the ePHI contained on that system.**

The units of the PCC HCC and each individual or unit within ICHOR Health and Wellness Center that is a business associate of a covered entity (hereafter collectively referred to as "departments") will protect the confidentiality, integrity, and availability of ePHI by implementing sound data management and backup practices that include, but are not limited to, the activities described in this Policy below. The department establishes and implements procedures to create and maintain retrievable exact backup copies of electronically protected health information (ePHI) as required by 45 CFR § 164.308(a)(7)(ii)(A) (HIPAA Security Rule, Contingency Plan, and Data Backup Plan). The procedures will assure that complete, accurate, retrievable, and tested back-ups are available for all ePHI on all information systems used by the department with the following exceptions:

- **Additional copies of ePHI created for convenience do not need to be backed up provided that the original document is adequately backed up and available as required by the HIPAA Security Rule**
- **Data sets containing ePHI which were generated from other data sets do not need to be backed up provided that the original data sets containing ePHI are appropriately backed up and available as required by the HIPAA Security Rule, and it is possible to recreate enough of the generated data set promptly so that ePHI in the generated data set is available as required by the HIPAA Security Rule**

The department creates a retrievable exact backup copy of ePHI before movement of equipment as required by 45 CFR § 164.310(d)(2)(iv) (HIPAA Security Rule,

Device and Media Controls, Data Backup and Storage). The same exceptions listed above apply.

The department maintains a record of movements of hardware and electronic media containing ePHI and any person responsible, therefore as required by 45 CFR § 164.310(d)(2)(iii) (HIPAA Security Rule, Device and Media Controls, Accountability). The department creates and stores backup copies per the Continuity of Operations Plan described in ICHOR Health and Wellness Center's HIPAA Security Risk Management Policy.

The department creates backup copies at a sufficient frequency and retains them in safe locations for an adequate length of time to accomplish all of the following:

- **Data backups that enable the restoration of ePHI that is lost or corrupted**
- **Data backups that support the department's Disaster Recovery Plan (or the equivalent) as required by 45 CFR § 164.308(a)(7)(ii)(B) (HIPAA Security Rule, Contingency Plan, Disaster Recovery Plan) and as described in HIPAA Security Contingency Planning, Institutional Policy**
- **Data backups that support the department's Data Emergency Action Plan (or the equivalent) as required by 45 CFR § 164.308(a)(7)(ii)(C) (HIPAA Security Rule – Contingency Plan – Emergency Mode Operations Plan)**
- **Data backups that support the department's mechanisms to authenticate ePHI, as required by 45 CFR § 164.312(c)(2) (HIPAA Security Rule, Integrity, Mechanism to Authenticate Electronic Protected Health Information) and as described in HIPAA Security Auditing, Institutional Policy.**

The following is typical of backup arrangements and can be used as a template for variation:

- **A typical arrangement includes a daily backup of data that has changed on all systems that create, receive, maintain or transmit ePHI**
- **Data backup systems may be manual or automated. Automated systems electronically capture backup locations, date, time, and other similar criteria. If the process is manual, documentation of the backup should include**
    - **Site/location name**
    - **Name of the system**
    - **Type of data**
    - **Date & time of backup**
    - **Where backup is stored (or to whom it was provided)**
    - **Signature of individual that completed the backup**

Stored backups must be sufficiently accessible and retrievable to meet the department's Data Emergency Action Plan specifications.

All media used for backing up ePHI must be stored in a physically secure environment, such as a safe, off-site storage facility or, if backup media remains on-site, in a physically secure location, different from the computer systems' site backed up. Suppose an off-site storage facility or backup service is used. In that case, a Business Associate Agreement (BAA) must be used to ensure that the business associate will appropriately safeguard the ePHI. A BAA might not be needed for off-site storage or backup services at certain PCC facilities. This will need to be evaluated case-by-case basis by ICHOR Health and Wellness Center's HIPAA Privacy Officer and HIPAA Security Officer. Data backups should be tested and data restored to assure accuracy. Documentation of backup testing or restore logs should be maintained and capture the date and time the data was restored. Operational procedures for backup, recovery, and testing should be documented and periodically reviewed. Proper management of data backup and recovery situations, such as emergencies or other occurrences, should be addressed in the COOP as described in HIPAA Security Contingency Planning, Institutional Policy.

Failure to back up a system in the absence of a system failure violates this Policy. Violation of this Policy and procedures by others, including providers, providers' offices, business associates, and partners, may result in termination of the relationship and associated privileges.

Business Associate Agreements

Indicate the Business Associate agreements that exist or need to be established for organizations or companies that access PHI through the health care organization. Refer to the following website for information regarding BA requirements. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html?language=es

Below is a general description of a Business Associate:

- performs or assists in executing a company function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

Some examples of Business Associates are as follows:

- A third-party administrator assists the company with billing and claims processing.
- A CPA firm whose accounting services to a health care provider involves access to protected health information.
- An attorney whose legal services involve access to protected health information.
- A consultant that performs utilization reviews for the company.

- An independent medical transcriptionist that provides transcription services for the company.

The term "Business Associate" refers to a person or entity not affiliated with ICHOR Health and Wellness Center that performs or assists in achieving for or on behalf of any unit in the ICHOR Health and Wellness Center component, business support functions/services that involve the use of PHI. NOTE: A health care provider that assists in providing treatment to patients is not considered a business associate.

The term "Business Associate Agreement" refers to a contract entered into between ICHOR Health and Wellness Center and an external party that contains specific terms and conditions, as required by the HIPAA Privacy Rule, governing the use and disclosure of protected health information by business associates. For purposes of this policy, a business associate agreement refers to both a stand-alone contract with the required HIPAA language or a broader contract that incorporates the required HIPAA language with other provisions.

Under ICHOR Health and Wellness Center risk management program, a risk assessment and risk analysis will be performed as the prelude to, during, or as a follow-up activity for the following:

• Breach Notification: As required by HIPAA's breach notification requirement, a breach risk assessment will be performed upon the discovery of a security incident by ICHOR Health and Wellness Center or its business associates involving protected health information. The purpose of the breach risk assessment will be to determine if the incident is a reportable breach

• Business Associates: Risk assessments performed on business associates will be conducted before signing any contracts and annually after that. If risk analysis is needed, then it will be completed per ICHOR Health and Wellness Center Third-Party Assurance procedure

PHI Access

In this section, indicate who can access ePHI in the organization. Provide a summary in the text box below. You will provide more detail by specific role and user access to PHI in the table below.

Following the standards set forth under federal and state statutory requirements (hereafter referred to as regulatory requirements), ICHOR Health and Wellness Center is committed to ensuring all protected health information's confidentiality, integrity, and availability (PHI/ePHI), confidential. Sensitive data (hereafter referred to as covered information) creates, receives, maintains, and transmits at a reasonable and appropriate level with the associated classification level, regardless of format (i.e., electronic, paper, voice, etc.).

The purpose of this procedure is to define ICHOR Health and Wellness Center's information security risk management program. This policy outlines the scope, responsibilities, and processes associated with risk identification, assessment/analysis, mitigation, acceptance, continuous monitoring, and revalidation.

Each department performs periodic technical and non-technical assessments of compliance with the HIPAA Security Rule requirements with additional reviews in response to environmental or operational changes affecting the security of ePHI to:

- **Ensure the confidentiality, integrity, and availability of all ePHI the department creates, receives, maintains, and transmits**
- **Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI**
- **Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required**
- **Ensure compliance by workforce**

Summary of Access Authorization

Using the table below, indicate each job or role in the organization and its associated user rights or access. An example is provided in the first row of the table.

**HIPAA requires that when PHI is used or disclosed, the amount disclosed must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.*

Job Title	User Rights/Access to PHI	Miscellaneous
(e.g., front office staff)	(e.g., access EHR -access to patient billing -access to appointment scheduling -patient emails)	(e.g., occasional interns may receive access to specific data systems containing PHI)
Chief Compliance Officer	**-Develop a HIPAA-compliant privacy program** **-Enforce privacy policies** **-Monitor changes to HIPAA rules** **-Create training programs and teach employees about the organization's privacy program**	

	-Conduct risk assessments on HIPAA compliance **-Provide patients with explanations of their rights under HIPAA**	
Senior Director for IT	**-Implementing HIPAA-compliant privacy programs** **-Conduct employee training on HIPAA policies** **-Conduct risk assessments on HIPAA violations** **-Investigate breaches and report them to the necessary authorities** **-Keep apprised of the recent laws regarding patient privacy**	
HIPAA Privacy Officer(s)	**-Oversee all ongoing activities related to the organizations' s privacy policies per applicable and federal and state laws to include HIPAA, HITECH, and Omnibus** **-Ensures privacy forms, policies, standards, and procedures are up-to-date** **-Works with senior organization management, security, and corporate compliance officer to establish governance for the privacy program** **-Works with the information security officer, an ongoing process to track, investigate and report inappropriate access and disclosure of protected health information. Monitor patterns of improper entry and disclosure of protected health information**	

	-Performs required breach risk assessment, documentation, and mitigation. Works with Human Resources to ensure consistent application of sanctions for privacy violations **-Cooperates with the U.S. Department of Health and Human Service's Office for Civil Rights, State regulators, and other legal entities in any compliance reviews or investigations** **-Collaborate with the information security officer to ensure alignment between security and privacy compliance programs, including policies, practices, investigations, and acts as a liaison to the information systems department**	
HIPAA Security Officer or designee	**-Implementing the technology to keep PHI protected** **-Developing a company-wide disaster recovery plan** **-Preventing unauthorized access to PHI** **-Implementing procedures for transmitting electronic PHI (ePHI)** **-Determining how to store ePHI properly** **-Because the duties of the privacy officer and**	
Information Security Officer	**-Incorporate IT security and HIPAA compliance with business**	

	strategies and requirements of the organization **-Employee training in conjunction with the HIPAA Privacy Officer** **-Perform risk analyses and audits on Business Associates** **-Look into data breaches and enforcement actions to prevent future occurrences**	

Part IV: Privacy and Security Audit

In this section, utilize the information you obtained from your desk audits in Modules 2, 3, and 4. Follow the directions to complete each table. You will use the information in the tables to create your report summary.

Administrative Safeguards
The Administrative Safeguards are the policies and procedures that bring the Privacy Rule and the Security Rule together. They are the pivotal elements of a HIPAA compliance checklist that govern the conduct of the workplace and require that a Security Officer and a Privacy Officer (which may be the same person) be assigned to put measures in place to protect ePHI. Remember that a risk assessment is not a one-time requirement but a regular task necessary to ensure continued compliance.

Overview
The following is an overview of administrative safeguards. The audit tool contains specific requirements.

- **Conducting risk assessments**– Among the Security Officer´s main tasks is the compilation of a risk assessment to identify every area in which ePHI is being used and determine how breaches of ePHI could occur.
- **Introducing a risk management policy**– The risk assessment must be repeated at regular intervals with measures introduced to reduce the risks to an appropriate level. A sanctions policy for employees who fail to comply with HIPAA regulations must also be submitted.
- **Training employees to be secure**– Training schedules must be introduced to raise awareness of the policies and procedures governing access to ePHI and how to identify malicious software attacks and malware. All training must be documented.

- **Developing a contingency plan**– In the event of an emergency, a contingency plan must be ready to enable the continuation of critical business processes while protecting the integrity of ePHI while an organization operates in emergency mode.
- **Testing of contingency plan**– The contingency plan must be tested periodically to assess the relative criticality of specific applications. There must also be accessible backups of ePHI and procedures to restore lost data in an emergency.
- **Restricting third-party access**– It is the role of the Security Officer to ensure that ePHI is not accessed by unauthorized parent organizations and subcontractors and that Business Associate Agreements are signed with all business partners who will have access to ePHI.
- **Reporting security incidents**– The reporting of security incidents is different from the Breach Notification Rule, as incidents can be contained and data retrieved before the incident develops into a breach. Organizations should stress the need for all employees to be aware of how and when to report an incident so that action can be taken to prevent a breach whenever possible.

Administrative Risk Audit Matrix Summary

Instructions:

1. Using the table below, fill in the "Security Privacy Concern" column with the privacy or security issue(s) you identified in your audit.
2. For each security privacy concern, indicate the following:
    a) Identify the existing mitigations/controls
        - Indicate if there are any existing controls or if there are no controls
    b) Indicate the impact (high/med/low) of each security privacy concern on the organization. This could be high, which might mean risk of breach, or low with no risk of violation.
    c) Indicate steps you are proposing to mitigate the risk.
3. Add any additional information you have identified or have concerns about.

Security Privacy Concern	Existing Controls to Mitigate Risk	Impact of Risk (i.e., High, Med, or Low)	Mitigation Plan (summary statement)
-Unauthorized disclosure, loss, or theft of ePHI can lead to medical identity theft. -Accurate ePHI may not be available when needed, which	-Training staff on our software that screens access automatically when they access any systems in the clinic -Staff are trained that systems that are accessed by	Overall security risk is low	-Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a). [45 CFR §164.308(a)(1)(ii)(B)] -Document, review, and disseminate risk assessment results to members of the workforce who are responsible for mitigating the threats and vulnerabilities

can adversely impact your healthcare professionals' ability to diagnose and treat their patients	them through the use of their log on will log them out if there is no activity (EHR, clinical databases, etc.) in 5 minutes of non-activity		to ePHI identified as a result of a risk assessment. [NIST SP 800-53 RA-3]
-Your practice may not be able to hold workforce members accountable (and take appropriate disciplinary action) if it does not have documented policies, procedures, and processes for disciplining those who violated the security policies and procedures put into place to safeguard your practice's ePHI	-Consider whether your practice consulted legal counsel in the drafting of its workforce sanctions policy. -Consider whether your practice's sanction policies focus on workforce members who fail to comply with the security policies and procedures.	Overall security risk is medium	- Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate. [45 CFR §164.308(a)(1)(ii)(C)]
- Your practice's policies and procedures for access authorization must address when and how to grant access privileges to business associates who need access to perform	N/A	Overall security risk is medium	-Implement procedures for the authorization and supervision of workforce members who work with electronically protected health information or in locations where it might be accessed. [45 CFR §164.308(a)(3)(ii)(A)] Develop processes to establish and maintain a list of authorized maintenance organizations or personnel that identify their access level to facilities, information systems, and ePHI. [NIST SP 800-53 MA-5]

permitted business activities.			-Develop processes to establish and monitor the security roles and responsibilities of 3rd party providers who access the practice facilities, information systems, and ePHI. [NIST SP 800-53 PS-7]

Technical Safeguards

The Security Rule defines technical safeguards as the policy and procedures that protect electronically protected health information and control its access. The only stipulation is that ePHI – whether at rest or in transit – be encrypted once it travels beyond an organization's internal firewalled servers. This is so that any breach of confidential patient data renders the data unreadable, undecipherable and unusable. After that, organizations are free to select whichever mechanisms are most appropriate. The following is an overview of technical safeguards the audit tool provides specific items.

Overview

The following is an overview of technical safeguards and requirements. The audit tool contains specific requirements.

- **Implement a means of access control**– This not only means assigning a centrally controlled unique username and PIN code for each user but also establishing procedures to govern the release or disclosure of ePHI during an emergency.
- **Introduce a mechanism to authenticate ePHI**– This mechanism is essential to comply with HIPAA regulations, as it confirms whether ePHI has been altered or destroyed in an unauthorized manner.
- **Implement tools for encryption and decryption**– This guideline relates to the devices used by authorized users, which must have the functionality to encrypt messages when they are sent beyond an internal firewalled server and decrypt those messages when they are received.
- **Introduce activity audit controls**– The audit controls required under the technical safeguards are there to register attempted access to ePHI and record what is done with that data once it has been accessed.
- **Facilitate automatic logoff**– This function – although only addressable – logs authorized personnel of the device they are using to access or communicate ePHI after a pre-defined period. This prevents unauthorized access of ePHI should the device be left unattended.

Technical Risk Audit Matrix Summary

Instructions:

1. Using the table below, fill in the "Security Privacy Concerns" area with the privacy or security issues you identified in your audit.

2. For each security concern, indicate the following:
    a) Identify the existing mitigations/controls
        - Indicate if there are any existing controls or no controls
    b) Indicate the Impact on the organization (high/med/low) for each concern. This could be high, which might mean risk of breach, or low with no chance of a breach.
    c) Indicate steps you are proposing to mitigate the risk.
3. Add any additional information you have identified or have concerns about.

Security Privacy Concern	**Existing Controls to Mitigate Risk**	**Impact of Risk (i.e., High, Med, or Low)**	**Mitigation Plan (summary statement)**
Some potential impacts include: • Human threats, such as an unauthorized user, can vandalize or compromise the confidentiality, availability, and integrity of ePHI • Unauthorized disclosure (including disclosure through theft or loss) of ePHI can lead to identity theft • Accurate ePHI might not be available, which can adversely impact a practitioner's ability to diagnose and treat the patient	Additionally, we have a policy regarding who has access to our systems and electronic and hard copy data. We have policies that assign roles for incident response and detail how staff are to function during downtimes, emergencies, and incident responses. We have a policy and annual training that governs downtime activity.	Overall security risk is medium	-Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

-If your practice does not have policies regarding mechanisms (hardware and software) that can record and examine information system activity, then inappropriate use of information systems and access to ePHI can go undetected.	We audit all user access every 3 months, and we can see which systems, databases, or EHR are accessed at any time by anyone. Copies of our audits are maintained for 7 years. We have policies that reflect our audit activity. We audit external organizations seeking access to our data, including business associates or other health care organizations such as lab, imaging, or health care organizations. All of our audits are reviewed by leadership and shared with staff to understand threats and vulnerabilities. We audit access controls to software, hardware, and physical buildings every 6 months	Overall security risk is low	Develop, document, and disseminate to workforce members an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. [NIST SP 800-53 AU-1]
-Your practice might not be able to identify which	We perform a risk analysis every year,	Overall security risk is high	-Implement hardware, software, and procedural mechanisms that record and examine activity in information systems containing or using ePHI.

business activities are at highest risk and subsequently determine the appropriate frequency and scope of its audits if it does not use the results of its previous risk analyses	including all hardware, software, databases, physical access, and HIPAA contracts. Although we encrypt all data, we know we can't determine if someone intercepted our data while in transit. So, we are looking at contracting with a company to assist with tracking encrypted data while in transit to help determine if PHI has been accessed, altered, or deleted		[45 CFR §164.312(b)] -Document and disseminate an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, compliance, procedures, and the coordination necessary among key stakeholders to implement the audit. [NIST SP 800-53 AU-1] -Use the risk-based categorization of key audit events (e.g., activities that create, store, and transmit ePHI) to determine the scope and frequency of audits. [NIST SP 800-53 AU-2]

Physical Safeguards

The Security Rule defines physical safeguards as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion." The standards are another line of defense (adding to the Security Rule's administrative and technical safeguards) for protecting an organization's EHR.

The Physical Safeguards focus on physical access to ePHI irrespective of its location. ePHI could be stored in a remote data center, in the cloud, or on servers located within the premises of the HIPAA-covered entity. They also stipulate how workstations and mobile devices should be secured against unauthorized access.

Overview

The following is an overview of physical safeguards and requirements. The audit tool contains specific requirements.

- **Facility access controls must be implemented (addressable)** – Procedures must be introduced to record any person who has physical access to the location where ePHI is stored. This includes software engineers, cleaners and even a handyman coming to change a light bulb. The procedures must also include safeguards to prevent unauthorized physical access, tampering, and theft.
- **Policies relating to workstation use (required)** – Policies must be devised and implemented to restrict the use of workstations that have access to ePHI, to specify the protective surrounding of a workstation (so that the screen of a workstation cannot be overlooked from an unrestricted area) and govern how functions are to be performed on the workstations.
- **Policies and procedures for mobile devices**– If mobile devices are to be allowed access to ePHI, policies must be devised and implemented to govern how ePHI is removed from the device before it is re-used.
- **Inventory of hardware** – An inventory of all hardware must be maintained, together with a record of the movements of each item. A retrievable exact copy of ePHI must be made before any equipment is moved.

Physical Risk Audit Matrix Summary

Instructions:

1. Using the table below, fill in the "Security Privacy Concerns" area with the privacy or security issues you identified in your audit.
2. For each security concern, indicate the following:
    a) Identify the existing mitigations/controls
        - Indicate if there are any existing controls or if there are no controls
    b) Indicate the Impact on the organization (high/med/low) for each concern. This could be high, which might mean risk of breach, or low with no risk of breach.
    c) Indicate steps you are proposing to mitigate the risk.
3. Add any additional information you have identified or have concerns about.

Security Privacy Concern	Existing Controls to Mitigate Risk	Impact of Risk (i.e., High, Med, or Low)	Mitigation Plan (summary statement)
Some potential impacts include: • Natural threats, such as hurricanes, tornadoes, and earthquakes, can cause damage or loss of ePHI. • Human threats,	Each clinic exam room (4) has a workstation consisting of a Dell "all-in-one" desktop with 8GB of ram and Intel i7 processor	Overall security risk is high	Establish physical access control procedures to: • Limit entrance to and exit of the facility using one or more physical access methods. • Control access to areas within the facility that are designated as publicly accessible. • Secure keys, combinations, and

such as an unauthorized user who can vandalize or compromise the integrity of ePHI. Unauthorized disclosure and loss or theft of ePHI can lead to identity theft.	and a 23-inch screen. The units are wall-mounted, and the monitor is on an articulated arm allowing the patient to see the screen when the clinician wants to share information. Each Medical Assistants (MA), front office clerk, biller, and director have similar workstations. The workstation configurations meet the minimum standards for utilizing the web-based EHR. Each exam room has a printer for printing out discharge instructions. They contain a blue bin for recycling shredding. There are shredding bins in the front and back-office areas, as well		other physical access devices. [NIST SP 800-53 PE-3]

	as labs and offices.		
Some potential impacts include: • Environmental threats, such as power failure and temperature extremes, which can cause damage to your information systems	Devices monitor all access points within the clinic and generate reports reviewed by leadership to ensure only authorized staff has physical access and access to controls. -Public access to workstations. We have a courtesy workstation in our lobby for patients and visitors. We monitor all activity on this computer, and it does not have the capability of accessing any of our clinical databases, EHR, or HIPAA-sensitive databases. -Workstation access, including data access by	Overall security risk is low	Have a plan designed to control physical access to information systems that have ePHI, including the facilities and rooms within them where your information systems are located. [45 CFR §164.310(a)(1)]

	role. We can also audit all activities for appropriate usage. -Hardware purchases, placement, and movement. This policy designates one person as being responsible for tracking and granting access. No staff can add software, download software or peripheral devices, and conduct an audit every 6 months for this activity.		
Some potential impacts include: • Natural and environmental threats, such as fire, water, loss of power, and temperature extremes, which can compromise the function and integrity of your practice's information systems.	- Emergency incident responses and annual testing of the plan. That plan aligns with our backup plan and emergency contingency plan	Overall security risk is high	Establish an alternate processing site to continue operations by: • Having appropriate agreements to permit the transfer and resumption of information services. • Ensuring required equipment and supplies are on site. • Ensuring applicable security safeguards are in place. [NIST SP 800-53 CP-7] When necessary, establish an Alternate Work Site to continue operations that include: • Security controls. • Continuous monitoring of control

			effectiveness. • Incident reporting and response. [NIST SP 800-53 PE-17]

Part V: Risk Mitigation Strategies

Policy for Breach Notification

Provide a summary of the organization's breach notification policy. The policy should indicate who the organization's privacy and security officer is and what the organization's reporting protocol is when a breach is identified.

This policy defines a breach according to the HIPAA Privacy Rule. It guides the steps team members and ICHOR Health and Wellness Center affiliates should take if they become aware of a breach. Further, the policy stipulates the steps to determine the extent and nature of the protected health information (PHI) that was breached and the procedures to notify affected parties. This policy applies to all ICHOR Health and Wellness Center team members, including board members, vendors, independent contractors, students, trainees, medical professionals and specialists, volunteers, business partners, and workforce members. Workforce members include all of the above-listed team members (and any other persons) whose conduct, in the performance of work for ICHOR Health and Wellness Center, is under ICHOR Health and Wellness Center's direct control, whether or not ICHOR Health and Wellness Center pay them.

It is the policy of ICHOR Health and Wellness Center's to maintain PHI confidentiality and safeguard against the unauthorized use or disclosure of PHI. ICHOR Health and Wellness Center team members will report any suspected breach as soon as possible to the ICHOR Health and Wellness Center Chief Privacy Officer. In the event ICHOR, Health and Wellness Center discovers a breach of any unsecured PHI, then ICHOR Health and Wellness Center will take action as required by law to notify the necessary parties, mitigate against the potential harm of the breach, and take appropriate action to safeguard against the violation from recurring

Disaster Recovery Plan

Indicate the organization's disaster recovery plan and downtime plan when access to ePHI is not available.

The scope of ICHOR Health and Wellness Center's contingency plan program is to ensure business operations continue with minimal or no disruption during a localized or catastrophic disaster. Contingency management is combined planning efforts for the business continuity plan (BCP) and disaster recovery plan (DRP). Goals are as follows:

- **Assign responsibilities for the management and maintenance of the contingency planning program**
- **Plan to ensure the safety of the workforce, clients, and customers**
- **Base plans on identifying events (or sequence of events) that can cause interruptions to critical business processes (e.g., equipment failure, human errors, theft, fire, natural disasters, and acts of terrorism)**
- **Minimize the loss of patient/client/customer and public confidence**

- **Expeditious recovery of data with no loss or degradation to integrity**
- **Facilitate the prompt resumption of services**
- **Maintain security of covered information**

The contingency plan strategy represents a critical aspect of contingency planning and is derived from the information collected during the business impact analysis (BIA) process. The following components must be considered when defining the contingency plan strategy and developing the related plans:

- **Personnel and who needs to be involved**
- **Communication (internal and external)**
- **Conditions to activate the business continuity plan as well as escalation plans**
- **Networking equipment and network services**
- **Technology issues (i.e., disaster recovery plan)**
- **Facilities (e.g., security, relocation, safety, emergency power, and communications)**
- **Critical business processes and systems**
- **Manual operations (i.e., what if technology resources are not available?)**
- **Resumption procedures which describe the actions to be taken to return to normal business operations**
- **Succession planning for each role in the event someone is not available to fulfill their responsibilities during a crisis**

When developing the contingency plan strategy, consideration will be given to short-term and long-term goals and objectives. Short-term goals and objectives include, but are not limited to:

- **Critical personnel, facilities, computer systems, operations, and equipment•**
- **Priorities for processing, recovery, and mitigation**
- **Maximum downtime before recovery of operations**
- **Minimum resources required for recovery**

Long-term goals and objectives include, but are not limited to

- **Management's enterprise-wide strategic plan• Coordination of personnel and activities**
- **Budgetary considerations**
- **Supervision of third-party resources confidence**
- **Expeditious recovery of data with no loss or degradation to integrity**
- **Facilitate the prompt resumption of services**
- **Maintain security of covered information**

Annual Training

Indicate the organization's annual staff privacy and security training program or processes.

At ICHOR Health and Wellness Center, we conduct initial training for new employees and annual training for all employees on privacy and security. We also update annual clinical competency skills.

We have policies for the following areas:

- **Annual training and documentation of training**
- **Ongoing training and implementing just-in-time training on cybersecurity awareness**

Our ongoing training addresses the following topics:

- **Malware access**
- **Preventing cyber threats**
- **Changing passwords**
- **Log in reminders**

We maintain policies and procedures regarding cybersecurity for the following:

- **Training and awareness of cyber threats**
- **Segregating access to systems based upon job title or role**
- **Maintaining training logs on annual and just-in-time training as needed**
- **Reviewing all activities and assuring that all staff have received training**
- **Training staff annually on downtime procedures when we don't have access to the HER**
- **Training staff on cyber threats and how to avoid them, such as avoiding phishing emails, spam, and non-secure website access**
- **Updating staff on all policies related to HIPPA and HIPPA violations**
- **Conducting an annual risk assessment and sharing the results with all staff to receive their input**
- **Delineating who can access PHI and the consequences for accessing PHI when one is not authorized to do so**
- **Training staff on our software that screens access automatically when they access any systems in the clinic**
- **Staff are trained that systems that are accessed by them through the use of their log on will log them out if there is no activity (EHR, clinical databases, etc.) in 5 minutes of non-activity**

Cyber Insurance

Indicate if the audit organization has a cyber insurance plan. If the organization lacks a covered procedure, tell what cyber insurance plan you would recommend in this section. This will require you to research information on the web to find an appropriate cyber plan. Provide a summary of the cyber insurance you would recommend for the organization (if indicated) and why you selected that particular cyber insurance company.

Cyber liability insurance is recommended. It helps cover financial losses due to cyberattacks or other tech-related risks, as well as private investigations or lawsuits following an attack. For example, if a hacker locks your computers, starts deleting files, and demands a ransom, this insurance can help you respond to the attack and help your business recover lost files and income. If your business is the victim of a cyberattack, cyber liability insurance can help cover:

- **Legal services to help you meet state and federal regulations**
- **Notification expenses to alert affected customers that their personal information was compromised**
- **Extortion paid to recover locked files in a ransomware attack**
- **Lost income from a network outage**
- **Lawsuits related to customer or employee privacy and security**
- **Regulatory fines from state and federal agencies**

It's essential to know these insurance policies don't cover every type of claim, and you may need other types of business insurance to create a comprehensive protection plan, such as:

- **General liability insurance to help cover claims your business caused property damage or bodily injury**
- **Commercial property insurance, which helps protect your business' owned or rented physical location and equipment**
- **Employment practices liability insurance to help cover employee claims of harassment, discrimination, or wrongful termination**
- **Professional liability insurance, which can help cover claims of mistakes or omissions in your professional business services.**

Summary of Risk Assessment and Mitigation Recommendations

In this section, write a three- to four-paragraph summary of your Privacy and Security audit. Include your recommendations for mitigating security privacy concerns or threats you identified.

We may revise this Privacy Statement from time to time as we add new features or change laws that may affect our services. If we make material changes to our Privacy Statement, we'll post a notice on our website. Any revised Privacy Statement will apply to information we already have about you at the time of the change and any personal information created or received after the change takes effect. Each new version of the Privacy Statement is dated. We encourage you to periodically reread this Privacy Statement to see if any changes to our policies may affect you.

This procedure applies to all ICHOR Health and Wellness Center information systems and the systems' users. The goals for auditing and monitoring systems and users are as follows:

- **Compliance with federal regulatory requirements**
- **Identify, respond, and mitigate:**

- **Insider threat deterrence**
- **Fraudulent activity**
- **External intrusions**
- **Security risks**
- **System performance problems and flaws**

- **Capture evidence for taking disciplinary action, forensic analysis, and potential civil and criminal litigation**

The CISO is responsible for, but not limited to, the following activities:

- **Ensuring all users are subject to audit and monitoring, including system/application administrators, privileged users, etc**
- **Ensuring all systems that store, process, or transmit covered information is subject to audit and monitoring**
- **Ensuring that all audit systems used can provide filtering capabilities (able to find specific logging events based on selectable criteria) and reporting functionality**
- **Ensuring the ability to manipulate, disable, and delete audit logs is restricted or monitored to detect these activities and positively identify anyone who executes these functions. • Ensuring the access to audit logs is restricted to the least number of people (e.g., administrators) as possible**
- **Ensuring that the workforce members responsible for the management and review of the audit logging and monitoring systems are qualified to perform the duties. For any systems that require a certification, ensure the applicable workforce members obtain these**

System/application administrators are responsible for, but not limited to, the following activities:

- **Ensuring all users, including administrators and privileged users, are being monitored and their activities are captured in the system audit logs**
- **Restricting all users, to include administrators and privileged users, the ability to manipulate, disable, and delete audit logs, and monitoring to detect these activities and positively identify anyone who executes these functions**
- **Configuring audit log capability to capture all activity required by this procedure**
- **Reviewing audit logs daily for unusual or suspicious activity and taking appropriate action, including informing the CISO**
- **Review any unauthorized remote access connections to the organization's network and information systems upon alert receipt and take appropriate action when unauthorized links are discovered. In addition, review with management quarterly**
- **Periodically checking to make sure the audit logging and monitoring systems are functioning and collecting data as expected, and fixing any issues that are discovered**

Operations/business owners are responsible for, but not limited to, the following activities

- **Restricting user access to audit logs to the minimum necessary based on job responsibilities**
- **Ensuring all user activity is being monitored and reviewed, to include system/application administrator and privileged user activity**
- **Ensuring the ability to manipulate, disable, and delete audit logs is restricted or monitored to detect these activities and positively identify anyone who executes these functions**

All systems have one audit log. Described below are several types of audit activity that are captured in logs:

- **User-level audit trails generally monitor and log all commands directly initiated by the user, all identification and authentication attempts, and files and resources accessed**
- **Application/database level audit trails generally monitor and log user activities, including data files opened and closed, specific actions defined in this procedure, and printing reports**
- **System-level audit trails generally monitor and log user activities, applications accessed, and other system-defined specific actions**
- **Network-level audit trails generally monitor what is operating, unauthorized access attempts, and vulnerabilities**

The following general attributes are mandatory audit requirements:

- **Audit log entries must include:**
    - **The user ID or service name that initiated an event**
    - **The unique data subject ID or function that was performed**
    - **Date and time the event was completed (timestamp)**
- **Any privileged operations (root, admin, security, supervisory, etc.) performed by the endpoint**
- **System startup, reboot, or shutdown**

At a minimum, the following security-related events will be captured in audit logs:

- **Successful and unsuccessful access attempts to access the system**
- **User accounts that have been inactive for longer than 30 days**
- **Changes to access rights and privileges**
- **Unsuccessful attempts to use or access privileged operations**
- **Inbound and outbound communications from external entities**
- **File integrity monitoring**
- **System configuration and security policy changes**
- **Date and time password changes are made**

- **Access to and changes to covered information, critical resources, and processes involved**
- **Attempts to reactivate or access disabled accounts**

All employees, volunteers, trainees, consultants, contractors, and other persons (i.e., workforce) whose conduct, in the performance of work for ICHOR Health and Wellness System, is under the direct control of ICHOR Health and Wellness Center, whether or not they are compensated by ICHOR Health and Wellness Center.

Workforce members are required to comply with all information security policies/procedures as a condition of employment/contract with ICHOR Health and Wellness Center. Workforce members who fail to abide by requirements outlined in information security policies/procedures are subject to disciplinary action up to and including termination of employment/contract.

