Privacy and Security
Risk Assessment Report

Organization Name

Waverly Family Health Services

Submitted by

Anne Frunk

Submitted to

Tennille Gifford MSN, RN, RN-BC, CPHIMS

Part I: Executive Summary

The Health Insurance Portability and Accountability Act (HIPAA) is a collection of federal statutes regarding portability of health insurance, administrative simplification, privacy and security of health information. It is essential to ensure the protection of electronic health protected information (ePHI) at Waverly Family Health Services. Anne Frunk Consulting Group has been contracted to provide a HIPAA Privacy and Security Risk Assessment and Mitigation Plan for the organization.

Anne Frunk Consulting Group performed security, technical, and physical safeguard assessments. The assessments included a review of business and clinical processes involving ePHI and evaluation of risk and exposure to such processes. An overview of the assessments is provided below.

Part II: Scope

The scope of the Privacy and Security Risk Assessment Report is focused on all activities of Waverly Family Health Services. This includes business, clinical, and remote environments that interact with PHI and any application and supporting IT infrastructure which create, receive, maintain, or transmit ePHI are considered in scope.

Part III: Risk Assessment and User Access

Risk Assessment Methodology

The Privacy and Security Risk Assessment was performed both onsite and as a desk audit. Interviews were also conducted as needed to provide background information.

Security Officer

Mrs. Jones, Clinic Director, Privacy and Security Officer

Inventory

Waverly Family Health Services has electronic databases that contain, receive, and transmit PHI information. These databases are Practice Fusion EHR, Billing software, and a calendar for patient appointments. PHI is stored electronically on a server and in paper-based charts. External vendors are Jones Billing Service, paper shredding company, lab processing company and medical supply company. All ePHI is encrypted and data is back-up to a secure cloud.

Hardware: Each clinic exam room (4) has a workstation consisting of a Dell “all-in-one” desktop with 8GB of ram and Intel i7 processor, 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 of the Medical Assistants

(MAs), front office clerk, biller and directors 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 recycle shredding. There are shredding bins in the front and back office areas as well as lab and offices.

Business Associate Agreements

Waverly Family Health Services has Business Associate (BA) contracts with the following organizations:

1. Jones Billing service: All clinic billing is performed by this group off site; they have access to the billing module in the EHR, computer systems from our server, and paper-based charts.

2. Paper shredding company: Paper shredding company provides services to health care organizations for the HIPAA compliant management and destruction of HIPAA data. They pick up paper-based items from contracted organizations on a scheduled basis.

3. Lab processing company: All lab work is performed at the off-site location, as no blood samples are drawn in the clinic.

4. Medical supply company: Waverly Family Health Services order front and back office supplies through this company, including all medications and biologics (vaccines).

Note: Waverly Family Health Services also has a policy that covers subcontractors of business associate agreements to ensure they meet HIPPA requirements. They have business associate agreements with all entities that access our PHI, regardless of the purpose for accessing the PHI.

PHI Access

Waverly Family Health Services staff have access to all electronic databases and charts based on roles, rights, and authorization. Vendors have business associate agreements in place with PHI access only relevant to services provided.

This space is intentionally left blank

Summary of Access Authorization

Job Title	User Rights/Access to PHI	Miscellaneous
Front Office	Appointment Scheduling, EHR, paper charts	Faxes, Insurance Portals, Patient registration paperwork
Medical Assistants, back office staff	Appointment Scheduling, EHR, paper charts	Faxes, Labs
Clinicians, Medical Director	Appointment Scheduling, EHR, paper charts	Faxes, Labs
Jones Billing Service	Patient Billing, Paper Charts	Paper EOBs, Insurance cards, Insurance portals
Paper Shredding Company	Shred bens	

Part IV: Privacy and Security Audit

In this section, we have summarized a general overview of Administrative Safeguards for Waverly Family Health Services to utilize in part with our findings.

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. Keep in mind that a risk assessment is not a one-time requirement, but rather 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 to determine all of the ways in which 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 introduced

- **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 the event of 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 in order that action can be taken to prevent a breach whenever possible.

Administrative Risk Audit Matrix Summary

Security Privacy Concern	Existing Controls to Mitigate Risk	Impact of Risk (i.e. High, Med, or Low)	Mitigation Plan (brief summary statement)
Categorize Information Systems if unavailable	Partial Existing	Low	EHR is backed up to cloud, however Waverly Family Health Services should strategize and mitigate areas with a moderate or large impact should they become unavailable.
Conduct Risk analysis upon occurrence of significant event or change	Partial Existing	Medium	Waverly conducts an annual risk assessment and sharing the results with all staff to receive their input. They also audit access controls to software, hardware and physical building every 6 months. However, I could not find documentation where risk assessments are conducted

			upon occurrence of a significant event.
Formally Documented Security Plan	No/Unclear	Medium	Waverly has policies and procedures for Privacy and Security, Emergency Plan, Incident Response and Downtime Response. However, I do not see a formal Security Plan but the pieces are there. Create a Security Plan that describes the policies and procedures listed and what is included.
Formal HR Policy to discipline staff	No	Medium	Establish HR policy to prevent system misuse, abuse, and any harmful activities that involve your practice's ePHI
Sanction Policies	No	Medium	Include sanction policies and train staff of penalties. Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
Qualified Contact to assess security protections	No/Unclear	High	Please provide Mrs. Jones's credentials. While the organization does have good practices in the place, having a qualified person will help mitigate these risks.
Security Contact Job Description	No/Unclear	Medium	I do not see "job description" of person mentioned.
Access Level of BAAs	No/Unclear	Medium	While a list is in place of BAAs, you must also assess what access each of them need. For example, billing may need different access and permissions than the lab processing company.
Job Qualifications for roles and job duties	No/Unclear	Medium	There is a list of job duties and roles, but I think this pertains to downtime procedures and system access. No qualification mentioned.
Screening Workforce	No	High	Verify the education level, degrees, professional certifications, and criminal history of workforce members.

Workforce Role Based Training	No	Medium	While cyber and security training is performed, it does not state whether this is specific to roles. Specific knowledge is necessary for the workforce member to understand how to perform the activities they are required to perform based on their role so that the privacy and security of ePHI can be established and maintained. This is frequently referred to as "Role-based Training" activities
Staff Training upgrades, patches	No/Unclear	Medium	Training workforce members to make updates to workstations and devices when requested to do so can help to reduce the risk presented by malware. Training workforce members not to load software to your practice's workstations and devices, without approval from the security official. *No mention if this is included as part of training content*.

Technical Safeguards

The Security Rule defines technical safeguards as the policy and procedures that protect electronic protected health information and control access to it. 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. Thereafter, 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 off 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

Security Privacy Concern	Existing Controls to Mitigate Risk	Impact of Risk (i.e. High, Med, or Low)	Mitigation Plan (brief summary statement)
Backup Information Systems	No	Low	Waverly does not have redundant information systems, with the same operating system environment and real-time data replication, in order to transfer and continue operations during an emergency. However, they do have emergency downtime plans and how to function when the EHR is not accessible.
Effective recovery from emergency downtime	No/Unclear	Medium	Evaluate your practice to determine if it clearly explains when and how to reinstitute normal access controls once an emergency passes. This might be part of your business continuity strategy. Your practice might not be able to reinstitute normal access controls after an emergency if your practice does not clearly explain when and how to recover from an emergency.
Responsible person for	No	Medium	Identify information system components and responsible person in your practice who oversees

automatic log off settings			electronic devices with auto log-off capabilities.
Encryption capabilities of electronic devices	No	Medium	Although Waverly encrypts all data, they know they don't have the ability to determine if someone has intercepted our data while it is in transit. They 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.
Deny access to unauthorized users	No	Medium/High	Waverly should implement encryption controls to reduce the risk for unauthorized access to ePHI and other health information when it is stored/maintained on an electronic device or portable media that is at greater risk of loss or theft (such as laptop, tablet, smartphone, or thumb device). Ensures that encryption standards are consistent with leading practices.
Identify & categorize activities that create, store, and transmit ePHI	No	Medium	Your practice might not implement access controls to protect its ePHI if it does not identify and categorize the activities that create, store, and transmit ePHI and the information systems that support these activities. Recommend identifying and categorizing such activities and systems that support them.
Identify frequency of audits from risk analysis	Partial Existing	Medium	Audits are done every 6 months. 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.
Policies and procedures for protecting ePHI from unauthorized modification or destruction	No	Medium	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
Verification practices that	No	Medium/High	Waverly is looking at contracting with a company to assist with

ePHI has not been altered, modified or destroyed in an unauthorized manner, including when in transit			tracking encrypted data while in transit to help determine if PHI has been accessed, altered, or deleted. Please implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
Authentication Mechanisms	No	Medium/High	Determines the suitability of each authentication method based on its analysis of risks
Protect user passwords	No/Unclear	Medium/High	Protect the confidentiality of the documentation containing access control records (list of authorized users and passwords).

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 that are 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

Security Privacy Concern	Existing Controls to Mitigate Risk	Impact of Risk (i.e. High, Med, or Low)	Mitigation Plan (brief summary statement)
Access Log to Facility (including visitors/vendors)	Partial Existing	Medium	They do have a sign-in sheet at the front office desk where patients write their name upon entering the clinic, but it is not clear if this includes visitors. Please include vendors and any visitors.
Monitoring Equipment	No	Low/Medium	Waverly does have an audit plan as part of this policy to review access by staff and role but unclear if they have monitoring equipment included. Consider the valuable role that monitoring equipment (e.g., a key card reader, video camera, or motion sensor) can provide to help your practice make sure that facility access is controlled according to your practice's policies and procedures**.**
Maintenance and Repair Records	No	Low/Medium	Implement policies and procedures to document facility and information system maintenance (repairs and modifications) and review them on a regular basis.
Workstation Policies and Procedures	Partial Existing	Low/Medium	Waverly does have policies and procedures regarding hardware purchases, placement, and movement but unclear if that means positioning to reduce ePHI exposure. Consider the steps that

			your practice takes to make sure that the work environment is configured in a manner that inhibits non-employees, visitors, and patients from incidentally viewing another person's ePHI on workstations. This includes use outside the facility.
Secure storage and ePHI removal of electronic devices, disposal, and re-use	No	Medium	While Waverly has policies regarding hardware purchases, placement, and movement, please implement policies and procedures that govern the receipt, internal movement, and removal of hardware and electronic media that contain ePHI.
Employee record and backup files of removing electronic devices	No/unclear	Medium/High	It is unclear if "movement" in your policy includes maintaining records of employees removing electronic devices and media from your facility that has or can be used to access ePHI. Recommend updating policy and procedures.

Part V: Risk Mitigation Strategies

Policy for Breach Notification

Waverly Family Health Services has policies and procedures regarding breach notification. The policy outlines procedures and processes. At this time, the clinic hasn't had any known breaches, or unintentional or intentional releases of data.

Disaster Recovery Plan

Waverly Family Health Services has a robust disaster recovery plan. This plan includes disaster management, including definitions for an emergency, staff's roles, backup procedures, and downtime procedures. The policy identifies roles, who is responsible for activating the emergency/disaster plan. The policy also describes the frequency of disaster drills and emergency access to PHI. In addition, data is backed up to a cloud and they can access the cloud within 30 minutes via web access. They have drills every 6 months to determine if they can access all backed up data.

Annual Training

Waverly Family Health Services conducts an initial training for new employees and annual training for all employees on privacy and security. They also update annual clinical competency skills.

Waverly has policies for the following areas:

- Annual training and documentation of training
- Ongoing training and implementing just-in-time training on cyber security awareness

Our ongoing training addresses the following topics:

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

Cyber Insurance

Currently, Waverly Family Health services does not carry cyber insurance. Health centers should have cyber insurance regardless of their size. Cyber insurance generally covers your business' liability for a data breach involving sensitive customer information, such as Social Security numbers, credit card numbers, account numbers, driver's license numbers and health records. A cyber insurance policy, also referred to as “cyber risk insurance” or “cyber liability insurance” coverage, is a financial product that enables businesses and clinical practices to transfer the costs involved with recovery from a cyber-related security breach or similar events. There are various insurance companies that offer ranges of coverage that include:

- Data compromise protection, which insures a commercial entity when there is a data breach, theft, or unauthorized disclosure of personal information

- Identity recovery protection, which helps victims of identity fraud restore their credit history.

- Cyber Protection, which protects your business against damage caused by a virus or computer attack, as well as helping with the cost of restoring and recreating data.

We recommend data compromise protection and cyber protection. With cyber-attacks becoming more frequent, there’s a growing chance that a clinical practice like yours will suffer a data breach or computer attack. That’s why you need protection to help offset the devastating effects it can have on your practice from a financial, patient safety, and reputation standpoint. One company that offers such coverage is Nationwide and we know of other health centers like yours that also use this company.

Summary of Risk Assessment and Mitigation Recommendations

Cybersecurity incidents continue to place immense pressure on healthcare organizations, community partners and their patients, jeopardizing not just patient data but also putting health care organizations at risk. Protecting patient health information is crucial and ensuring health centers are managing those risks well isn't easy. Overall, Waverly Family Health Center does a good job but there is room for improvement. Below are recommendations concluded from our Privacy and Security audit to help mitigate future risk.

Areas of Focus

- ✓ Implement an official security plan and address items found in above sections.
- ✓ Manage personal devices where ePHI is accessed. If you want to allow access to databases with ePHI from personal devices, implemented a BYOD policy and procedure.
- ✓ Ensure ePHI is not accessed, altered, or deleted when sending encrypted data. You are currently researching this and we recommend ongoing regular review.
- ✓ Obtain cyber insurance. Lack of sufficient cyber-insurance funds could lead to major out of pocket expenses during a breach.
- ✓ Implement vulnerability/risk testing not just every 6 months but when changes occur such as system upgrades, patches, and facility physical changes as well.
- ✓ Make sure you have a log of all visitors (not just patients), this includes family members and vendors.

Anne Frunk Consulting Group thanks you for the opportunity to work with your leadership and clinical staff. Please do not hesitate to reach out if you have any questions or need further assistance. We are also happy to conduct another review once recommendations have been implemented or if other concerns should arise.