Prepared for:

The Haven

Security Risk Assessment

Feb 2024

Prepared by:

JNR Networks
Do IT Different

Table of Contents

Overviews

Corporate Overview

- The Haven provides effective, affordable substance use recovery for women in a family-inclusive environment.
- Services are provided both inpatient and outpatient across 3 locations.

Protected Data Overview

- Core HIPAA Data Locations:
  - Kipu EHR
  - O365 environment (SharePoint, OneDrive, e-mail)
  - Submission sites with third parties
  - Paper
  - Fax via Copier/Printer and Online Fax (eFax – Unknown if HIPAA version)
- Other Protected Responsibilities:
  - Social Responsibility to funders, payers, clients and community
  - Employee data (O365 and Paycom)
  - Legal – Regulations, laws, guidelines, contract deliverables
  - Corporate Data (O365, QuickBooks)
  - Non-HIPAA Client Data (Client Stories, pictues, etc.)

IT Overview

- 3 Site networks interconnected by VPN tunnels
- On-site servers house Active Directry domain, printing funcations, QuickBooks and historical NextGen data.
- Primary data storage is in O365 and Kipu.
- Website hosted by AnchorWave with data hooks into eTapestry for donations.
- MFA is present on O365 and Kipu environments.
- On-site and O365 data is backed up daily by JNR Networks with a 30 day retention period.
- Backups of Kipu, website, Kipu and eTapestry are performed by the respective providers.

Observations and Opinions

We (JNR) are in a unique position as we have been working with The Haven for a number of years now. This provides us with some historical context in which to understand what we see in a site survey that might be otherwise missed.

The Haven has grown from a smaller organization into one that has a significant and growing staff count that are dispursed across multiple sites. This growth necessitates some cultural, paradigm and leadership growth that is happening but also has some gaps.

One unique benefit at The Haven is that staff come from a wide variety of walks. Some have extensive formal education while others have extensive street education. Some have been through their own recovery journeys. This variety provides a diverse perspective within the organization that has its benefits but can also lead to issues when trying to build mature, optimized processes, with everyone on the same page.

It appears, and is corroborated in interviews, that there is a general perception that people want to do the “right thing”. There do not seem to be many staff with an overall negative or intentionally careless attitude towards the work of The Haven and its responsibilities. In the areas where there are gaps and weaknesses, these seem to boil down to a few reasons:

1. People are busy getting work done and run out of time to do things perfect so they cut a corner here or there to make sure the work gets done. (ie. Cabinets and doors left open.)
2. Lack of skill, either in ways to do something better technically or in thought processes that would lead towards a more optimized approach.
3. There is a lack of systems, either soft or technical, to effectively or efficiently do the job so people adapt a non-optimized system to get the job done.

With evolving threats, especially on the IT front, we should seriously consider an increased security stance. Without this increased stance, even with increased user training and process improvement, it is likely that the question of a future breach is less a matter of if but when and to what extent. While no solutions can guarantee zero risk, an increased security stance should provide better capabilities to know if/when an issue arises so it can be shut down quicker, with better awareness of what a hacker was able to actually accomplish.

Opportunities and Recommendations

1. Process Optimization
    - Culture, processes and systems needed
2. User Education
    - Culture shift around attitudes towards protecting sensitive information
    - Training on what is protected and how to protect it
    - Training on general IT functions to increase awareness of actions in the system and potential ramifications
    - Training on when, where and how to share data externally.
    - Need one-time, at point of onboarding, and ongoing
3. Defined Policies, Procedures, Roles, Responsibilities and Authority Clarifications
    - Role Overlaps
        - IT and Maintenance roles can sometimes overlap
        - Software Evaluation (ie. eTapestry, Campbell Camera Installation)
    - Development
        - Emilia has her own process for handling pictures and getting releases but this is not clearly documented.
        - Unsure if staff are aware of how to properly review photos prior to posting anywhere.
        - Lack of clear delineation of when data is authorized for public release and who is authorized to make this decision.
4. Increased IT Security Stance
    - Conditional Access to O365, enforcing BYOD-type policies
    - Network access restrictions, blocking unauthorized access
    - Increased endpoint and network protections via tighter configurations, enforcement tools and enhanced monitoring

Interviews

Aimee Graves, Chief Executive Officer

- What do you have that needs to be protected?
  - Social Capital – Funders, payers, etc. Takes a while to build social capital and an instant to lose it.
  - Best practices, regulations, laws, guidelines, deliverables on contracts.
  - Employees and clients' health, safety and reputation.
  - Clients, reputation – we can damage their reputation if we aren't appropriately secure with their information.
- How are you doing at protecting data?
  - Have had a rough few months but, overall, probably pretty decent.
  - Starting to get trust in the leadership team to not run from things that are not perfect.
  - Do people recognize when things are a high priority? Are they able to properly communicate the priorities and urgencies with adequate words, are they safe to do so, etc.?
- Culture
  - Hard working people that care but have had to deal with lesser things and sometimes don't call things out as well as they need to.
  - Opportunity to improve the culture.
  - Many roles are a bit confused as to the scope and authority of them.
- Succession Planning
  - There are places where there is no solid succession plan.
- Opportunities
  - Culture Improvement
  - Leadership improvement. Succession plans, redundancy, improve competency.
  - Shift to optimization focus beyond the basics and core survival.

Cynthia Duncan, Senior Vice President of Finance & Administrative Services

- Role Confusion
  - Maintenance sometimes does IT stuff without communication. Goes back to the lack of clarity and definition between roles.
- What needs to be protected?
  - Financial data – Payroll, patient records, staff data
  - Corporate records
  - Patient data

    - Dual sided – Both that the data is present and accessible but also that the wrong people aren't able to access data they shouldn't have access to.
- Risks
    - User competency
        - Users can get dangerous with data.
        - E-mailing documents vs links to files.
            - Sometimes, users are sharing links but people don't know where the root document is.
                - Are users sending the hyperlink to a file or sharing the file uniquely?
        - Data Integrity
            - Inadvertent deletion of data.
            - Lack of clarity of where the master is sometimes…copies of copies of copies of copies.
        - Organization
            - It looks like there may be confusion or too few root SharePoint locations where too many people have access to places that are too generic for their function.
                - Ie. Finance, HR, Leadership
- CARF Test
    - They want TH to do a BDR test of some sort.
    - Is there a way for JNR to more clearly indicate validation and restoration tests.

Suzi Armenta, Information Technology Manager

- What do you have that needs to be protected?
    - Client Information – Kipu (primary), e-mail, SharePoint, OneDrive
    - Financial Information – 365, QuickBooks
    - HR Data – 365, Paycom
    - Everything we do.
- Shared Documents
    - Internal
        - Sometimes sharing from OneDrive, sometimes from SharePoint
        - SharePoint Sharing – Sometimes doing a share event, sometimes just copying the link.

Erisha Green, Vice President of Quality, Compliance & Risk Management

- What do you have that needs to be protected?

    - HIPAA information, specifically part 2 information about substance abuse, etc.
        - SSNs, Diagnosis, medial information
- How and where is protected data handled?
    - Kipu EHR system
    - Paper, sometimes
    - E-mail
    - O365 documents
    - WhatsApp – Shut down
    - Other than Kipu and Paper, if the product isn't MS approved and TH hasn't paid for it, users should not be sharing information on it.
    - Text messaging, sometimes, but information should be stripped of PII
    - Faxes – via Copier/Printer or via Online Fax (eFax)
- How is compliance going?
    - Was going really good, then Aimee's e-mail got hacked and realized that people were not using the system the way they were supposed to.
    - Post Aimee's hack:
        - The process of e-mailing the census was immediately stopped.
        - Trying to get people to access and more consistently use SharePoint documents via hyperlinks vs e-mailing attachments via e-mail.
- What other things do you see that are concerning?
    - Nothing
    - Post Aimee's hack, lawyers and such indicated they were pretty happy with what TH already had in place. The main suggestion was to not directly put PHI/PII in e-mail but to use the hyperlink sharing method.
- Are there any other risks to the organization that you can see?
    - Recently found that people are using USB drives. Need to have an Executive level discussion around USB policy prior to a decision and policy being developed.
        - Assumption is that Cynthia will discuss with JNR and bring that insight to bear in the Leadership Team meeting.
    - Definable process and policy – Discoveries, like the USB drive discovery and decision making around it aren't driven by policy but more common knowledge.
- How does someone know that data is PII/PHI
    - Federal government online tool. Employees are trained on the use of this tool on an annual basis.
    - Clients Sharing Information:
        - Have clients sign a waiver document allowing release and sharing.
        - Usually have the client write up a document vs talking live.

Emilia Honkasaari, Vice President of Communications & Development

- What do you have that needs to be protected?
  - Client data, health records
  - Client stories, client pictures, etc.
  - Internal board and administrative documents, including financials
- How do you know something can be shared?
  - Have a release from the client. Whether it's a media release, release of information, etc. form.
  - While not formally required, Emilia personally asks clients if they are comfortable and okay with her sharing their story. Even though she has a legal release, she focuses on making sure the client is personally comfortable with the release.
  - Internal Conversations – ie. Annual report has distilled outcome and financial data that gets released publicly.
- Protected Information
  - Have access to EHR but rarely goes there. May go there to confirm that a media release is on file.
  - Data Emilia handles has usually been released or stripped of PHI/PII.
  - Releasees are stored in Kipu.
  - Statistics – Typically gets from Allie…isn't usually looking at the actual data.
- Process
  - Emilia might take pictures then post them on SharePoint and ask appropriate people if TH has releases for all of the people in the photos before she uses the photos for anything.
- Risks
  - Photos
    - If they aren't appropriately reviewed prior to release.
    - Do staff know how to properly review a photos prior to any posting anywhere?
    - Possibly don't have media release forms for staff.
  - E-mails – Compromise
  - Social Media – Multiple people use the same login to social media.
    - Using a "fake" Margaret Higgins profile to manage social media. If that was marked as fake, would be an issue.
    - Emilia and Suzi have a lot of the credentials but they are not necessarily stored in an appropriate central location.
    - Not using separate user accounts for social media access and administration.
  - Software Evaluation

        - Not a clearly defined process that requires all parties, including IT. Relies on common sense. Finance will have to be involved due to budgeting but some others might not be included.
        - Example: eTapestry for Donor database. Who all was involved in the evaluation and decision of using the system?
            - Included input from a consultant they were working with.
            - Emilia talked with Cynthia and Aimee prior to making a decision.
            - Not sure what kind of evaluation Cynthia and Aimee did other than responding to Emilia's Pro/Con list.
    - Website
        - Linked to eTapestry for donation form and for direct client services that are being paid for.
        - Hosted and managed by AnchorWave

Amanda Veigel, Residential Technician Supervisor

- What is your role?
    - Res Tech Supervisor
        - Supervises alongside with Brianna, handles scheduling, time cards, coverage for shifts, and other such supervisory duties.
    - Schedules Urine Samples (UDS's):
        - The schedule is printed in 2 copies, one for Amanda and one for the Res Techs
- What Sensitive Data (PHI) do you handle, and how is it accessed and managed?
    - PHI is often scanned and put into OneDrive and for Federal Pre-trial there is a web portal that she logs into for uploading the data.
        - Once scanned, it is put into a file cabinet that is kept locked (mostly, sometimes locking it is inconvenient)
    - PHI is in emails internally, usually just names of individuals are spelled out in the body of the subject.
    - Teams is used for instant messaging and sometimes PHI such as confirming information.
- What training is made available to staff around securing member information?
    - Every RT that starts here goes through initial onboarding training. Then they also go through the policy and Relias training.
        - There are training checklists that they work through including how to handle UDS, Federal Probably information, etc.
        - Then they take a test, and then they can start on those items.
    - The policy behind breaches is to notify the member that there was a breach of their information. For any staff that were responsible for the breach, there would be disciplinary action.

- What else am I not asking about?
    - The most dangerous things that RTs do is make a physical list of who needs to do a UDS and that is kept in pockets and sometimes those notes fall out of pocket.
    - Sometimes they (RT's) need to go pick up medication, they take a paper with written member name and birthday. They are supposed to shred these papers when they are done.

Ashley Elizabeth, Residential Technician II

- What is your role?
    - Residential Technician
- What Sensitive Data (PHI) do you handle, and how is it accessed and managed?
    - Most everything is kept in KIPU
    - Millenium is a separate system from KIPU that is used for sending UDS's out to the lab.
    - The UDS's are kept onsite and Millenium would come and pick up the samples.
    - With the UDS's, if it's for federal cases, there is a paper copy that gets saved and is kept in the RT office under lock and is picked up by a supervisor the next morning.
- What training is made available around securing member information?
    - Relias training and motivational interviewing. Training was partially useful.
    - In the event of a potential breach, would likely notify somebody, but doesn't know what that process would look like.

Anne Thomas, Residential Technician I

- What is your role?
    - Lead Staff First Shift (RT1)
        - Supervises that everyone is doing what they need to do and that the shift is running well, and reports issues to Amanda as needed.
- What Sensitive Data (PHI) do you handle, and how is it accessed and managed?
    - All medical records are kept in KIPU. Only time anything gets printed out from KIPU is to give information needed to the member.
    - When information about members is sent via email, the information is obfuscated by only including initials.
    - RT's all handle medication for members, once appropriate training is given.
        - Keys are locked in the cabinet for the nurses office for when medications need to be given out.
- What training is made available around securing member information?
    - Res Techs go through a medication training before being allowed to give out medications.

- Relias tests are given annually. Training is effective, something new is added every year.
- Do you ever have a need to send PHI externally?
  - RT's do not have any need or use for sending any information to outside providers.

Savannah Robbins, Nurse Manager

- What is your role?
  - Nurse manager, direct patient care and coordination with outside agencies and handling escalation of care.
  - Basic triage is done, and then management of the patients.
- What Sensitive Data (PHI) do you handle, and how is it accessed and managed?
  - Physical PHI includes clinical assessments that are printed when they do the nursing assessment and then write up a narrative once they leave. Kept in a locked room or directly in-hand. Once the notes on the assessment are typed into KIPU, the notes go into the shred bin.
  - Clinic door that is connected to the conference room is often left unlocked (not by nursing staff). Savannah thinks it is not managed well.
  - Keys for Savannah's office is limited to 3 staff: Melissa, the Case Aide, and herself. Tom does not have a key to Savannah's office.
  - Residential Technicians have a set of keys to the clinic. Another spare set is locked in Savannah's office for when one of the Residential Technicians bring their set of keys home (usually on accident).
    - No access log for who uses the Residential Technicians keys and when. The spare set of keys is on a lanyard stored in the residential technician office, inside the large cabinet with the large sets of other keys.
  - A number of files are kept on Savannah's desktop in a "Savannah" file. She doesn't trust that SharePoint is doing its job in keeping information confidential.
- Do you ever have a need to send PHI externally?
  - PHI (Referrals) is sent via email both internally and externally (Narcan list as well).
    - There's a lot of PHI in Savannah's email, kept for the purpose of record of conversations.
    - Example given: when the nurses try to get appointments scheduled with external providers, they need to include information such as the member name and birthdate. These emails are sent plain text. Savannah keeps these emails as she needs a record kept of the conversation since the medical providers often do not fulfill their obligations, and the paper trail is good to have during the case of a quality of care audit.

Melissa Wilt, Registered Nurse

- What is your role?
  - Nurse: completes new admits, assessments, medications and follow ups.
- What Sensitive Data (PHI) do you handle, and how is it accessed and managed?
  - Majority of PHI handled is during coordination of care and communicating via phone calls the medication needs of members.
  - Nurses office manages the medication physically in their office.
  - Notes are taken directly in KIPU, for the most part.
  - Medication is labeled with patient name and is kept behind a lock, narcotics are specifically behind two locks.
  - Assessment notes are sometimes taken in the office on a piece of paper, then immediately put in the shred bin once the notes are transferred into KIPU.
- What training is made available around securing member information?
  - There's initial policy training and an annual HIPAA training done through Relias. Training is fairly effective on teaching the release of information and maintaining the confidentiality of patient data.

Judi Romero, Recovery Coach

- What is your role?
  - Recovery Coach – coordinates services with outsie agencies, federal and local, incurance, pre-trials, etc. This done both over email and over the phone.
  - Meets with members at least one hour, per member, per week.
- What Sensitive Data (PHI) do you handle, and how is it accessed and managed?
  - Most information considered PHI goes through Erisha since she started in August.
    - What is now sent out: Discharge summaries and concurrent reviews.
    - Emails are encrypted before they are sent
    - Information going to United is faxed
    - There is a set standard that all PHI getting sent out is either checked with Erisha, or there are particular sets of data that they are allowed to send out.
    - Physical paper used to fax is put directly in the shred bin in the copy room.
  - Sometimes notes are taken on physical paper, but names are not included and then the notes are taken to the shred.
  - Whatsapp and texting are not used anymore. Teams is used instead for instant messaging.
- What training is made available around securing member information?

- Relias training is enforced and HIPAA is usually once a year. 80% minimum required to pass. Training seems like a checkbox and a bit of wall paper. Some people might learn from it, but since she's been here so long, it seems like it's lost its value.