Data Security for the MFT-PRN: Policies and Procedures

Purpose and Structure of the MFT-PRN Project:

Purpose: The mission of the MFT-PRN is to improve patient outcomes by*:*

1. Facilitating routine outcome monitoring. The MFT-PRN allows therapists to easily track patient progress in therapy through routine administration of questionnaires that assess individual and relational health. Graphical display of patient progress, including clinical cutoffs, provides therapists with information that they can use to assess patient functioning, create treatment plans, and modify those plans based on patient response to treatment.
2. Facilitating clinical research in marriage and family therapy. The MFT-PRN provides de-identified data from patients that have consented at participating clinics across the network, to researchers who are seeking to understand and improve the practice of couple and family therapy.

Users/Developers of the MFT-PRN Project: The MFT-PRN project is accomplished through six main groups:

1. The MFT-PRN Project Team Located at BYU: This team is responsible for the overall project, recruitment of new sites, providing the website development team with what we want the program to do, and to set up new sites. The team is also responsible for providing de-identified data to researchers interested in using combined data from clinics within the MFT-PRN. The team consists of the following individuals.
    a. Executive Team
    b. Project Manager
    c. Data Security Officer
    d. Grad assistants.
2. Software Technology Group, Inc.: This team is responsible for developing the website (MFT-PRN Portal) and ensuring it has the necessary technological safeguards to maintain confidentiality of patient data.
3. Microsoft Azure Server: Microsoft is responsible for securely housing the data and for data monitoring.
4. Individual Clinic Sites: Each site is responsible for the use of the Portal in their clinic. The site signs a data transfer agreement that governs the protection and use of patient data from their site. They are responsible for ensuring that use of the MFT-PRN Portal meets all local and national laws in their country, and for developing clinic policies and procedures to ensure protection of PHI of their patients. Users at the site become part of the MFT-PRN and are able to access the data for research purposes
    a. Clinic director
    b. Site administrative staff
    c. Therapists

5. Patients: Patients complete questionnaires about individual and relational health via the MFT-PRN Portal throughout their treatment. This information is used for their clinical treatment and, with their consent, for research purposes.
6. Researchers: Members of the MFT-PRN are able to access data from their own clinic whenever they would like. They are also able to access de-identified data from the entire MFT-PRN through a formal submission process

Description of the MFT-PRN Portal: https://mft-prn.byu.edu/

- Description of structure of MFT-PRN Portal: STG can provide this information.
- Developer-facing:
  - Developers have access to the databases as a necessary requirement to perform the work on the project. The developer has signed a non-disclosure agreement, Business Associate Agreement (BAA), and data privacy and security addendum that bind them to confidentiality and provides BYU legal remedy in the case they do not follow the provisions of these agreements.
- Microsoft Azure Server:
  - ePHI is created, received, transmitted, and maintained from a Microsoft Azure Server. Microsoft has provided a Business Associate Agreement that outlines their responsibilities for maintaining data security and protection, including technological and physical safeguards, as well as requirements for reporting data breaches. Developers at Software Technology Group, Inc., principal investigators, and project manager have access to ePHI stored in Microsoft Azure Server.
- System-wide-user-facing:
  - Allows us to create new clinics, program assessments, and schedules for what assessments are given when.
  - We can access site users' information to assist in restoring accounts, resetting passwords
  - Two-factor authentication protects login credentials
  - No ePHI is created, transmitted, received, or maintained at this level of the MFT-PRN.
- Site-facing
  - Scheduler Version: includes calendar to schedule rooms and clients in rooms
  - Non-Scheduler Version: therapists enter appointment when client arrives
  - For both versions, the clinic director for the site is responsible for the administration and use of the site at their clinic. This includes creating policies and procedures for data protection at that site, providing training, enforcing
  - ePHI is created, transmitted, and received at this level of the MFT-PRN.
  - Site can create and access client ePHI for their own site but not for any other site in the MFT-PRN.
  - Site can receive client ePHI with names linked to data for all clients at their site.
- Patient-facing

- Can only access online questionnaires that patient completes either at home using an emailed link to the questionnaires or on a tablet at the clinic.
- Patients create and transmit ePHI at the patient-facing level of the MFT-PRN.

Policies and Procedures to Protect Patient Health Information.

The following policies and procedures address the administrative, physical, and technical safeguards used in the MFT-PRN Project. They will focus primarily on those safeguards for which the MFT-PRN Project Team are responsible. Agreements with Software Technology Group, Inc., Microsoft, and individual clinical sites are provided as appendices to this document. Each of those entities is responsible for having policies and procedures for protecting patient data in place to fulfill their roles in the project.

Administrative Safeguards

- **Security Management Process:**
  - Risk Analysis: *Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the covered entity*.
    - Risk analysis policy and procedures. Once per year using the security risk assessment tool (SRA) from HealthIT.gov. Security risk assessment is performed by project manager and data security officer each April. Results of the SRA are shared via email with Data security officer and PIs of the project. Brigham Young University's data security specialist over the FHSS School will be called upon as needed to assess risk. Data security officer then drafts policy to address any new security issues and executive committee reviews them for adoption. Will include review of any changes to HIPAA and other data protection laws in countries where the MFT-PRN is present.
  - Risk Management: *Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.*
    - Security measures that are identified in yearly risk analysis will be implemented to reduce risks and vulnerabilities. The project manager is responsible for updating this document with updated policies and procedures approved by the executive team.
  - Sanction Policy: *Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.*
    - MFT-PRN project manager and data security officer provide data security training to workforce members on security policies and procedures. Members who violate policies and procedures after initial training will receive a warning and additional training. Secondary or severe violations will lead to termination from the MFT-PRN workforce.

        - Information System Activity Review: *Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.*
            - Our contract with Microsoft Azure provides for system activity review and data monitoring to report data activity or breaches to MFT-PRN principal investigators and project manager. Software Technology Group, Inc. has also contracted to notify the MFT-PRN personnel of data breaches or security incidents.
    - **Security Personnel**:
        - The data security official (DSO) oversees data protection in the project in consultation with the Executive Committee of the MFT-PRN project. The DSO conducts the risk analysis, proposes updates to policies and procedures to address new risks and vulnerabilities, and interfaces with legal counsel regarding data security laws in newly added countries. The DSO also receives reports of irregularities or breaches from Microsoft and Software Technology Group, Inc.
        - Roy Bean, Ph.D., is the DSO for the MFT-PRN.
    - **Information Access Management**: (R)*Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of subpart E of this part.*
        - Isolating Health Care Clearinghouse Function (R) *If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization*.
            - Server is housed on an off-site location. Server access is only available to white-listed addresses.
            - Access to server, data, and MFT-PRN site are restricted only to those at BYU who are part of the MFT-PRN project.
            - Each site is responsible for access management at their site. The MFT-PRN system has been designed to facilitate this using role-based access. Sites can choose which individuals are given access to information based on defined roles.
        - Access Authorization (A): *Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanisms.*
            - The MFT-PRN Portal requires access authorization. This occurs through creating unique identifiable user accounts who can only access the site with a secure password, and who are granted access only to the ePHI that the clinic director deems necessary to accomplish their designated duties in the clinic.
            - The MFT-PRN Project Team has access to the System-Wide User-Facing Portal. The team is not able to access patient ePHI however we are able to see information about users of the system (therapists, clinic administration). The following describes the various roles of team members and access members have to the MFT-PRN Portal
                - PI's:

        - Full system-wide user-facing portal access
        - Two PI's so if one leaves the other is responsible for terminating rights of the other
        - They are also responsible for terminating access rights of project manager when the project manager leaves
    - Executive Team
        - MFT-PRN Executive Committee does not have access to the system-wide user-facing portal processes.
    - Project Manager
        - Full system-wide user-facing portal access
        - Responsible for managing access for all other project personnel other than PIs
        - Responsible for terminating access of project personnel immediately when those students leave the project (graduation or other assignment)
        - Monitors all active accounts, training, and remediation for violations of security procedures and ensures that project personnel have the most restrictive access necessary to perform duties assigned.
    - Other Project Personnel
        - Project personnel are given the most restrictive access necessary to perform duties assigned by the project manager.
- Access Establishment and Modification (A) *Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.*
    - The Project Manager (PM) is responsible for establishing user accounts for members of the MFT-PRN Project Team. User accounts are only created for individuals who require access to the portal to accomplish the tasks required for their position in the project. Users are given the most restrictive permissions that still allow them to complete their assignments.
    - The PM documents the active users and the rights assigned to these users and dates for training, access granting, violations, remediation, and removal of access.
    - The PM reviews this document regularly and modifies access rights that are no longer needed to perform the user's job responsibilities.
    - The PM terminates access rights for users who are no longer part of the project at the time the user leaves the project.

- **Workforce Security**: *Implement policies and procedures to ensure that all members of its workforce have appropriate access to ePHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4)of this section from obtaining access to ePHI.*

- Authorization and/or Supervision (A) *Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed*.
  - The Project Manager (PM) authorizes, supervises, and provides training for members of the team that require access to the MFT-PRN Portal to accomplish the tasks required of their position.
- Workforce Clearance Procedure (A) *Implement procedures to determine that the access of a workforce member to ePHI.*
  - Prior to accessing the MFT-PRN Portal, the PM ensures users have been trained in data security policies and have signed non-disclosure agreements.
- Termination Procedures (A) *Implement procedures for terminating access to ePHI when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.*
  - The PM terminates the user account associated with any member of the team immediately following their departure from the project and documents when access was removed.
- The MFT-PRN team provides initial training regarding operation of the Portal including the security measures when setting up a new site. Each site is responsible for determining who is authorized to use the MFT-PRN Portal, supervising workforce members, ensuring all workforce members are trained, as well as developing and enforcing appropriate sanctions when members of the workforce violate the site's policies and procedures.

- **Security Awareness and Training** (R)*Implement a security awareness and training program for all members of its workforce (including management).*
  - Security Reminders (A): Implement policies and procedures for periodic security updates
    - Following each annual security review, the MFT-PRN security officer or project manager will send a summary of MFT-PRN data security procedures to all personnel with access to system-wide user-facing processes.
  - Protection from Malicious Software(A): *Implement procedures for guarding against, detecting, and reporting malicious software.*
    - Any users who have access to full administrator access to the system-wide user-facing portal will have an active anti-virus software on computers used to access the MFT-PRN. If malicious software is detected, it will be reported to the project manager and data security officer. If such activity occurs, FHSS computer support will be consulted to determine whether the device is secure before accessing the MFT-PRN through that device.
  - Log-in Monitoring (A): *Implement procedures for monitoring log-in attempts and reporting discrepancies*
    - System locks out users after three incorrect password attempts. Locked accounts are reported to system administrators, who will only unlock the locked account after confirming with user. In the even that the

locked account was not due to the user's error, a password change will be required.

- Password Management (A): *Implement procedures for creating, changing, and safeguarding passwords.*
    - All user accounts with system-wide user-facing access are required to be protected by password and two-factor authentication, as documented by the project manager.
    - Passwords must be 16 characters long.
    - Passwords must be kept secure and should not be written, or saved electronically unless as part of a password management app.
    - Passwords can be changed by clicking on the "Reset Password" link, which will generate a password reset email to the email on file for the user.
    - If a password is on a compromised list of pre-existing passwords, the password will be rejected by the system.
    - All user accounts with system-wide user-facing access passwords must be changed if the user's account is locked not due to user error.

- **Security Incident Procedures (R):** *Implement policies and procedures to address security incidents*
    - Response and Reporting (R): *Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.*
        - Data is monitored for security incidents by Microsoft. Software Technology Group, Inc. has also contracted to report security incidents to MFT-PRN administrators.
        - Security incidents will be reported to the Data Security officer and Software Technology Group, Inc. developers
        - Site will be taken offline until risk is mitigated
        - DSO will inform Project Manager of the security incident who will report the incident to the Clinic Director at impacted sites.
        - Sites are responsible for reporting incident to impacted patients.
- **Contingency Plan (R):** *Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrences (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.*
    - Data Backup Plan (R): *Establish and implement procedures to create and maintain retrievable exact copies of ePHI.*
        - A complete backup of data is maintained by Azure.
        - Clinics are told that they are ultimately responsible for their own data and should backup routinely
    - Data Recovery Plan(R): *Establish (and implement as needed) procedures to restore any loss of data.*
        - Microsoft Azure has agreed to provide for data restoration as part of Business Associate Agreement.
        - Clinics are told that they are ultimately responsible for their own data and should backup routinely.

        - Emergency Mode Operation Plan (R): *Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode*.
            - The MFT-PRN is not central to the operation of partnered sites; clinic can operate appropriately without accessing MFT-PRN poral. There are no critical business processes that are contingent in the event of a critical failure of the MFT-PRN. Hard copies of MFT-PRN assessments may be provided upon request.
        - Testing and Revision Procedure (A): *Implement procedures for periodic testing and revision of contingency plans*.
            - Since the MFT-PRN is not central to the operation of partnered sites, testing and revision of contingency plans is not implemented.
        - Applications and Data Criticality Analysis (A): *Implement policies and procedures to assess the relative criticality of specific applications and data in support of other contingency plan components.*
            - Our current assessment is that MFT-PRN processes are not central to operation of partnered sites. This assessment will be revisited and evaluated with each annual security review.
    - **Evaluation**: *Implement policies and procedures to perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of ePHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.*
        - As part of the Security Management Process, we periodically assess how well the security policies developed for MFT-PRN meet HIPAA and other regulatory standards.
- **Physical Safeguards (Need to fill this out some more with info from Microsoft)**
    - System-wide user-facing users do not have access to ePHI. System administrators can access de-identified data through MFT-PRN portal and are able to access ePHI on the server. While the MFT-PRN administrators moderate user accounts and have access to ePHI through the Microsoft Azure server, they will not log in, download, or view any ePHI through the Microsoft user interface. Due to limited risk, physical safeguards are maintained primarily by Microsoft Azure.
    - **Facility Access and Control**: *Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.*
        - Contingency Operations (A): *Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.*
        - Facility Security Plan (A): *Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.*
        - Access Control and Validation Procedures (A): *Implement procedures to control and validate a person's access to facilities based on their role or*

function, including visitor control, and control of access to software programs for testing and revision.

- Maintenance Records (A): *Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks).*
- The MFT-PRN pays for space on Microsoft Azure Servers that are HIPAA compliant. As part of our BAA with Microsoft Azure, physical safeguards are implemented for data security. In addition, we pay for data monitoring. Microsoft has developed policies and procedures to address the physical safeguard requirements. As part of the yearly risk analysis, we ascertain that Microsoft has these policies and procedures in place.

- **Workstation Security**: *Implement policies and procedures to ensure that all members of the workforce have appropriate access to ePHI and to prevent workforce members who do not have access from obtaining access to ePHI. Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.*
  - Microsoft Azure Server: These controls are included as part of Microsoft's policies and procedures
  - BYU: All workstations are restricted to authorized users. Access to the MFT-PRN Portal is further restricted to authorized users with specific role-based access.
- **Workstation Use (R):** *Implement policies and procedures to ensure that workstations and other computer systems that may be used to send, receive, store or access ePHI are only used in a secure and legitimate manner. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.*
  - Microsoft Azure Server: These controls are included as part of Microsoft's policies and procedures
  - BYU: The MFT-PRN Portal can be accessed from any internet-enabled device. As part of training, users are informed not to access the portal in a public location.
- **Device and Media Controls (R)**
  Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.
  - Disposal (R): *Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.*
    - In the event of termination of the Microsoft Azure Server contract. A full encryptyed copy of the data will be provided to the MFT-PRN executive team.
    - Microsoft Azure Server: These controls are included as part of Microsoft's policies and procedures

        - Media Re-Use (R): *Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.*
            - Microsoft Azure Server: These controls are included as part of Microsoft's policies and procedures
        - Accountability (A): *Implement procedures to maintain a record of the movements of hardware and electronic media and any person responsible therefore*
            - Microsoft Azure Server: These controls are included as part of Microsoft's policies and procedures
        - Data Backup and Storage (A): *Implement policies and procedures to create a retrievable, exact copy of ePHI, when needed, before movement of equipment.*
            - Microsoft Azure Server: These controls are included as part of Microsoft's policies and procedures
        - MFT-PRN data with identifying information or information that could be reconstructed to identify individuals will not be screenshotted or converted into any form of electronic media.
- **Technical Safeguards**
    - **Access Control.** A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).[24]
        - Unique User Identification (R): *Implement procedures to assign a unique name and/or number for identifying and tracking user identity.*
            - Each user creates a unique username that is used to identify and track user identity.
            - Use of the site, including what data is visible to the user, is highly restricted/filtered based on that user's configured role permissions
                - Each clinic determines what users are granted what roles
                - The site clearly lists what access rights each user has
        - Emergency Access Procedure (R): *Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.*
            - MFT-PRN personnel at BYU do not access ePHI.
        - Automatic Logoff (A): *Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.*
            - Automatic logoff occurs after 30 minutes of inactivity
        - Encryption and Decryption (A): *Implement procedures to describe a mechanism to encrypt and decrypt ePHI.*
            - At rest: Data on the Microsoft Azure Server is encrypted according to the business associate agreement with Microsoft.
            - In transit: Data is encrypted using HTTPS as it is transferred between the browser and server.
    - **Person or Entity Authentication:** (R) *Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.*
        - Users choose a unique password that must meet the following requirements:

        - Minimum of 16 characters
        - Password cannot be on a list of commonly-used or compromised passwords.
      - After 5 failed login attempts, the user is locked out and their account must be unlocked by a system admin.
      - BYU users are required to enable two-factor authentication.
  - **Audit Controls.** A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.[25]
    - BYU users do not access ePHI.
    - Audit controls are in place for Microsoft Azure according to business associate agreement.
    - Access to ePHI by Software Technology Group, Inc. is governed by business associate agreement and non-disclosure agreement.
    - Anytime anyone for any reason views a page or makes changes to any data that surfaces or affects Patient Health Info, it is logged separately as to who, when, what they saw, and what they changed (if any)
  - **Integrity Controls.** A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.[26]
    - MFT-PRN system administrators will not alter or destroy data.
  - **Transmission Security.** A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.[27]
    - MFT PRN Portal requires HTTPS encrypt data in transit between client and server
    - HSTS is enabled to ensure that browser always points to HTTPS rather than HTTP

Policies and Procedures and Documentation Requirements

- A covered entity must adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities or assessments.[30]

- **Updates.** A covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of electronic protected health information (e-PHI).[31]