New Employee Orientation
Technology Reference Guide

I. Introduction
    A. Purpose of the Guide
    B. Importance of Technology in Behavioral Healthcare
II. Company Technology Overview
    A. Hardware
        1. Computers/Laptops
        2. Mobile Devices
        3. Printers/Scanners
    B. Software
        1. Electronic Health Record (EHR) System
        2. Telehealth Platforms
        3. Communication Tools, Incident Reporting and Policies
    C. Network Infrastructure
        1. Internet Connectivity
        2. Intranet and VPN Access
III. Access and Security
    A. User Accounts and Permissions
    B. Password Management
    C. Data Security and HIPAA Compliance
IV. Best Practices for Technology Use
    A. Data Privacy and Confidentiality
    B. Proper Use of Communication Tools
    C. Remote Work Guidelines
    D. Backup and Recovery Procedures
V. Training and Support
    A. Orientation and Onboarding Sessions
    B. Online Training Modules and User Guides
    C. IT Support Services

I. Introduction

A. Purpose of this Guide

As a new member of our team, technology will play a critical role in your daily responsibilities and interactions with clients. This Technology Reference Guide is designed to be your comprehensive resource for understanding the hardware, software, and IT infrastructure that are essential to our operations.

Our company is committed to leveraging the latest advancements in healthcare technology to provide exceptional patient care and support. From the electronic health record (EHR) system that manages client records, to the telehealth platforms that facilitate remote consultations, the tools and technologies covered in this guide are fundamental to how we work.

By familiarizing yourself with the information in this reference, you will be equipped to navigate our technology ecosystem efficiently and securely. This will allow you to focus on delivering the highest quality of behavioral healthcare services to our clients. Please use this guide as a go-to resource during your onboarding and beyond. If you have any questions or need further assistance, our IT support team is here to help.

B. Importance of Technology in Behavioral Healthcare

In the rapidly evolving field of behavioral healthcare, technology has become an indispensable tool for driving better outcomes for clients. The integration of digital solutions throughout our industry has transformed the ways in which clinicians, therapists, and support staff are able to deliver care. From improving the efficiency and accuracy of electronic health record (EHR) documentation, to facilitating secure telehealth sessions that expand access to services, technology permeates nearly every aspect of modern behavioral healthcare.

Beyond enhancing core clinical workflows, technological innovations also play a crucial role in supporting the overarching goals of our industry. For example, data analytics capabilities allow us to identify trends, monitor treatment progress, and make more informed decisions. Furthermore, advancements in communication tools enable seamless collaboration between interdisciplinary teams, as well as stronger connections between providers and the communities they serve. As we continue to navigate an evolving healthcare landscape, it is imperative that all members of our organization develop a strong familiarity and comfort with the technologies that power our business. By embracing these digital solutions, we can elevate the standard of care, improve clinical outcomes, and foster a more connected, patient-centric model of behavioral healthcare delivery.

II. Company Technology Overview

A. Hardware

1. Computers/Laptops

- Standard desktop computers and laptops provided to all employees depending on their job requirements and any accommodations that can be made to improve productivity of an employee
- Minimum specifications:
  - Intel Core i5 processor or equivalent
  - 8GB RAM
  - 256GB SSD encrypted storage
  - Equipped with Windows 10/11 Pro operating system and Microsoft Office suite (optional)
- Regular hardware refreshes every 4 years to ensure optimal performance

2. Mobile Devices

- Company-issued smartphones and tablets available for staff based on position and program designation.
- Models: iPhone 12+, Android standard tablet
- Enabled with secure access to email, calendar, and other core applications
- Mobile device management (MDM) policies enforced for data protection

3. Multifunction print and scan devices/Cloud faxing

- Multifunction devices are strategically placed throughout our facilities
- They support printing, scanning and copying
- Network-connected to allow access from any workstation and print to any printer with your work badge or login credentials using FollowMe technology
- Maintained under a managed print services contract for supplies and repairs
- Scan to OneDrive from any multifunction device
  - Scan to OneDrive Instructions (MyMeridian ->Resources->IT Documents)
- Cloud fax available upon request, send/receive faxes from your email
  - Cloud Fax Instructions (MyMeridian ->Resources->IT Documents)

B. Software

1. SmartCare - Electronic Health Record (EHR) System

- Primary platform for managing client medical records
- Fully integrated with billing, scheduling, and reporting functionalities

- Secure data storage and role-based access controls
- Comprehensive training provided during onboarding
    - Training site: SmartCare - Training
    - Production site: SmartCare - Production

2. Mend and MS Teams Telehealth Platforms

- Video virtual care solution for conducting remote therapy sessions
- HIPAA-compliant video conferencing with end-to-end encryption
- Accessible through desktop, mobile, and tablet devices

3. Communication Tools, Incident Reporting and Policies

- Microsoft 365 suite, including Outlook for email, Teams for chat/video, and SharePoint and OneDrive for file sharing
- Incident reporting, report important work-related events: Incident Reporting
- PolicyTech, Meridian's go to source for internal policies: PolicyTech
- Facility work orders, Facilities Work Order
- IT support tickets, Support : MyMeridian Support Portal
- Datis, HR/timeclock, https://epunch.datis.com/

C. Network Infrastructure

1. Internet Connectivity

Internet is provided in 3 forms at Meridian: ethernet, wireless and wireless hotspots. Where possible, Meridian recommends plugging into an assigned Ethernet port. Wireless from our WIFI6 routers is accessible at most of our locations using the MeridianWifi SSID. Meridian Guest SSID is used for any non-staff Internet access. Meridian's Internet is filtered by an advanced UTM (Unified Threat Management) system. Internet is for business purposes only and all actions are logged and regularly reviewed. When in the field or during times of outage, Meridian issued hotspots are available for business Internet use.

2. Intranet and VPN Access

Meridian's intranet, MyMeridian, is accessible only from a Meridian campus location. https://mymeridian.mbhci.org. Our intranet contains important corporate events, staff information, contests, department resources and more. Check it out!

Currently, VPN access to Meridian's network is on an approved basis only. VPN access is generally reserved for emergency vendor access and is not part of the daily routine of a Meridian staff.

III. Access and Security

A. User Accounts and Permissions

1. User Accounts

User accounts are uniquely assigned to each employee and follow the format firstname_lastname@mbhci.org. Hyphens are not to be used and can either be replaced with an underscore or removed from the username.

2. Permissions

Permissions are assigned based on role. Special permissions for applications can be requested by your supervisor.

B. Password Management, Multifactor Authentication (MFA) and Single Sign-On (SS0)

Passwords should remain private and not shared. Meridian's password policy requires passwords to be at least 14 characters, with numbers, upper and lower case characters and a symbol. You may reset your password 1x every 24 hours by pressing CTRL+ALT+DEL and selecting reset password. Passwords should be kept private and not shared with others. If you feel your password has been compromised, you should reset your password immediately or contact IT for assistance.

Multi-factor authentication (MFA) and single sign-on (SSO) are two critical components of our company's cybersecurity infrastructure, designed to ensure the security of our digital assets and systems. MFA adds an extra layer of protection beyond just a password by requiring additional verification steps, such as a fingerprint scan, a code sent to a mobile device, or a security token. This significantly reduces the risk of unauthorized access, even if passwords are compromised. On the other hand, SSO simplifies the user experience by allowing employees to access multiple applications and services with just one set of login credentials. By centralizing authentication, SSO enhances productivity while maintaining security standards. Together, MFA and SSO play integral roles in safeguarding our company's data and systems from cyber threats.

C. Data Security and HIPAA Compliance

When it comes to handling sensitive information in healthcare settings, your role in ensuring data security and HIPAA compliance is pivotal. You are the frontline defenders of patient privacy and confidentiality. It's essential to understand that every action you take, from accessing patient records to transmitting information, impacts the security of sensitive data. By following strict protocols and guidelines, such as securely storing passwords and employing encryption methods for data transmission, you can significantly mitigate the risk of unauthorized access or breaches. Regular training and education on HIPAA

regulations are key to empowering you with the knowledge and tools needed to navigate the complexities of data security effectively. Your commitment to upholding these standards not only protects patient information but also strengthens trust between healthcare providers and patients. Together, let's prioritize data security and HIPAA compliance to ensure the integrity and confidentiality of patient data remains intact. Meridian also requires HIPAA information training thru our internal training platform, Relias, Relias - Meridian Behavioral Healthcare.

IV. Best Practices for Technology Use

A. Data Privacy and Confidentiality

Data privacy and confidentiality are paramount in today's digital age. As an end user, it's crucial to understand and uphold these principles to protect sensitive information. Data privacy refers to the protection of personal data from unauthorized access, use, or disclosure, ensuring that individuals have control over their own information. Confidentiality, on the other hand, extends this concept to encompass all types of sensitive data, not just personal information, and emphasizes the importance of keeping it secure and undisclosed. By respecting data privacy and confidentiality measures, end users play a vital role in maintaining trust and integrity in digital interactions, safeguarding both personal privacy and sensitive business information. This involves being mindful of the permissions granted to apps and services, using strong passwords, being cautious with sharing information online, and staying informed about privacy policies and regulations. Ultimately, prioritizing data privacy and confidentiality not only protects individuals and organizations from potential harm but also fosters a safer and more trustworthy digital environment for everyone.

Our company is committed to fortifying data privacy and confidentiality training through quarterly internal phishing campaigns. These initiatives are designed to empower employees with the skills to swiftly identify and thwart various threats to our data security.

B. Proper Use of Communication Tools

1. **Email**:
    - Use for formal or detailed communication that requires documentation.
    - Keep the subject line clear and concise.
    - Use a professional tone and grammar.
    - Be mindful of reply-all and consider whether all recipients need to be included.
    - Respect privacy and confidentiality when sharing sensitive information.
    - Encryption is required for any client PHI or PII emails

2. **Instant Messaging (IM) / Chat**:
    - Ideal for quick exchanges and informal communication within teams.
    - Use appropriate language and tone, considering the recipient and the context.
    - Avoid discussing sensitive or confidential information unless the platform is secure.
    - Use emojis or emoticons judiciously to convey tone or emotion.
3. **Video Conferencing**:
    - Use for meetings that require visual communication or collaboration.
    - Ensure a quiet and well-lit environment.
    - Test equipment and connections beforehand to avoid technical issues.
    - Be mindful of background noise and interruptions.
    - Encourage participation and engagement from all attendees.
4. **Phone Calls**:
    - Use for urgent matters, complex discussions, or when tone is crucial.
    - Introduce yourself clearly at the beginning of the call.
    - Speak clearly and at an appropriate volume.
    - Be mindful of time zones when scheduling calls.
    - Take notes during the call to ensure follow-up actions are captured.
5. **Collaboration Platforms (e.g., Slack, Microsoft Teams)**:
    - Use for ongoing team communication, project collaboration, and file sharing.
    - Organize conversations into relevant channels or threads to keep discussions focused.
    - Utilize features like mentions and notifications effectively to ensure important messages are seen.
    - Respect designated communication norms and guidelines within your organization.
6. **Social Media**:
    - Use for public communication, brand promotion, or networking.
    - Tailor messages to suit the platform and audience.
    - Be mindful of tone, as social media posts can have a significant impact on reputation.
    - Engage with followers and respond to comments or messages in a timely manner.
    - Avoid controversial topics or engaging in arguments that could damage your personal or professional image.
7. **Project Management Tools (e.g., Trello, Asana)**:

- Use for organizing tasks, setting deadlines, and tracking progress.
- Ensure tasks are clearly defined and assigned to the appropriate team members.
- Regularly update task statuses to keep everyone informed of progress.
- Use comments or chat features within the tool for discussions related to specific tasks.

Regardless of the communication tool used, always prioritize clarity, professionalism, and respect for others' time and privacy. Adapt your communication style to suit the platform and the preferences of your audience to ensure effective and productive communication.

C. Remote Work Guidelines

Currently, remote work is only approved as needed. Meridian employees are expected to complete their work on Meridian campus or out in the field with clients. If working remote, it is best practice to follow these guidelines to ensure HIPAA compliance and IT security rules are being followed:

1. **Secure Workspace:**
    a. Find a quiet and secure location in your home to set up your remote workspace.
    b. Ensure that your workspace is free from distractions and interruptions to maintain focus on your work tasks.
2. **Screen Privacy:**
    a. Position your computer screen in a way that it's not visible to others who might be in the vicinity.
    b. Consider using a privacy screen or adjusting the screen brightness to minimize the risk of unauthorized viewing of patient information.
3. **Password Protection:**
    a. Keep your work devices password protected and avoid sharing your login credentials with others.
    b. Use strong and unique passwords for accessing work-related systems and applications and consider using a password manager to securely store and manage your passwords.
4. **Secure Communication:**
    a. Use encrypted communication tools provided by your organization for all work-related discussions.
    b. Avoid discussing patient information in public or over unsecured channels such as public Wi-Fi networks or non-encrypted messaging apps.
5. **Data Handling:**

a. Handle patient data with care and ensure that it's not left unattended or exposed to unauthorized individuals.
b. Store any physical documents containing patient information in a locked drawer or cabinet when not in use.

6. **Device Security:**
    a. Keep your work devices updated with the latest security patches and antivirus software to protect against malware and other cyber threats.
    b. Enable automatic locking or screen timeout on your devices to prevent unauthorized access when you're away from your workspace.
7. **Confidentiality:**
    a. Avoid discussing patient information or work-related matters in public settings or where others can overhear.
    b. Be mindful of your surroundings during virtual meetings and ensure that no confidential information is visible or audible to unauthorized individuals.
8. **Physical Security:**
    a. Secure your work devices and any physical documents containing patient information when not in use.
    b. If working in a shared space, consider using a lockable storage container or laptop lock to prevent theft or unauthorized access.
9. **HIPAA Training:**
    a. Participate in HIPAA training provided by your organization to understand your responsibilities regarding patient privacy and data security.
    b. Stay informed about any updates or changes to HIPAA regulations and guidelines to ensure ongoing compliance.
10. **Incident Reporting:**
    a. Report any security incidents, breaches, or potential privacy violations to your organization's IT or security team immediately.
    b. Follow your organization's incident response procedures and cooperate with any investigations or remediation efforts.

D. Backup and Recovery Procedures

Our company employs a robust suite of tools for backing up and recovering your data, ensuring the safety and accessibility of your files. Leveraging the power of OneDrive and your department’s dedicated SharePoint site, we securely back up and store your files in Microsoft’s cloud infrastructure. Additionally, as a secondary safeguard, our company utilizes Barracuda Cloud to Cloud backup, covering your email, OneDrive, and departmental SharePoint files.

In the event that you require assistance with file recovery, our dedicated IT support team is readily available. Simply submit an IT ticket at Support : MyMeridian Support Portal.

V. Training and Support

A. Orientation and Onboarding Sessions

At our company, we understand the importance of getting started on the right foot. That's why we hold New Employee Orientation (NEO) every Monday, a mandatory program designed to ensure all new team members are equipped with the knowledge and tools they need to excel. Depending on your role, NEO typically spans 2-3 days, during which you'll dive into critical company policies, procedures, and programs to familiarize yourself with our operations.

As part of NEO, you'll also undergo training through our Relias program. This comprehensive training covers essential skills such as leadership, job responsibilities, and cybersecurity, tailored specifically to our behavioral healthcare environment.

Following NEO, our IT team will personally onboard you, ensuring a seamless transition into your new role. During this session, you'll receive any necessary hardware required for your job's success. If you have any special needs or requests, simply inform your supervisor, and we'll work diligently to accommodate them.

B. Online Training Modules and User Guides

Our company uses Relias for internal training - Relias - Meridian Behavioral Healthcare. There you will find training modules on generic healthcare information, teamwork, cyber security, leadership, behavioral healthcare and more. These courses are required throughout the year, and you will receive notices as due dates approach for you to complete your courses.

User guides can be found on our local intranet site, My Meridian - https://mymeridian.mbhci.org. Department specific guides, including templates for marketing supplies, ordering forms, scan to OneDrive, eFax, and more can be found under Resources=>Documents on MyMeridian.

C. IT Support Services

Our company has an internal IT Department dedicated to addressing technical concerns promptly. To streamline the process, we encourage utilizing our preferred method of contact by creating an IT ticket online via Support : MyMeridian Support Portal. Alternatively, assistance is also available by dialing

extension 8346 from any Meridian phone. Each ticket and call is assessed and handled with priority, adhering to Meridian's standard operating procedures for the helpdesk. Technical issues are prioritized according to the following criteria:

1. Cybersecurity incidents
2. On-site client work stoppages
3. Work stoppages related to reporting or project deadlines
4. Work stoppages with no immediate impact
5. Non-work stoppage technical issues
6. Equipment requests

Rest assured, our team is committed to resolving your concerns efficiently and effectively.