Bring Your Own Device (BYOD) Policy

Introduction

A mental health clinic providing clients with a range of mental health services, including individual, couples, and family therapy, as well as community-based services and medication management. The clinic staff includes administrators, administrative support, therapists, and IT professionals, totaling around 20 team members. The clinic's most critical data includes clients' personal information and mental health records. Administrative staff and therapists are required to enter client data into the clinic's Electronic Health Record (EHR) system. Therapists sometimes meet clients off-site (e.g., at a client's home or school) or participate in community services, requiring them to access and submit records using personal devices and external internet connections. Although small in scale, the clinic is well-operated and is committed to valuing client privacy and rights.

Goal

DO NOT COPY

Ensure that employees use their personal devices both on-site and off-site without violating the employer's security and privacy policies.

Objective

- Identify and describe the security procedures required upon onboarding.
- Recognize and respond appropriately to risk control procedures in the workplace.
- Demonstrate correct use of identification and access control protocols in the workplace.
- Employ best practices for protecting data in workplace settings.
- Implement application control measures when using work-related applications.
- Explain and adhere to relevant security and privacy laws and principles.
- Maintain personal security and privacy by applying company guidelines effectively.

Policy

On-boarding

- User Account Registration

Copyright © 2024 Pei-Shan Hsieh

Employees must provide their name, employee ID, job position/role, and department to create an account and register their devices.

- Device Registration
- Employees must provide their device information as brand, serial number, IMEI number (phone or pad only), and MAC address.
- End-user/Service Agreement

Identification & Access Control

- Password
  - At least 12 characters long
  - Avoid using employees' name, birthday, pet's name, or repeating and sequential characters
  - Passwords must contain both upper and lower case characters and have at least one number one special character such as !, @, #, $, %
  - Password should be changed on every 90 days
- Authentication

  Employees must use DUO as Two Factor Authentication when logging in to clinic's information system.

DO NOT COPY

- Authorization

  Employees must map confidential information resource to their device within the context of authentication.
- Accounting

  IT has rights to tracks and monitor the usage when employees' devices link to or log on clinic's system.

Data Protection

- Encryption

  Employees must use AES to protect email and text messages, contacts list, calendar, and other credential information situated in your device built in memory as well as removal/flash memory cards.
- Virtual Private Network (VPN)

  Employees must set and use VPN when trying to link to clinic's information system and database via their devices. Please contact the IT for setting detail.
- Data Wiping

Copyright © 2024 Pei-Shan Hsieh

IT is able to selectively wipe clinic's information resources on employees' devices that are infected or highly vulnerable to malware /viruses, or if employees violate control measures.

- Data Backup
  - Employees must submit all their clients' data to EHR within 48 hours.
  - Employees must back up the data by following the IT's recommended methods.
- Device Lockdown

  IT is able to use applications to remotely lock or shut down your compromised devices.

Application Control

- Licensed and curated application stores

  Employees should download and install applications either from organizational application stores, or from licensed application stores.
- Trusted and Verified Apps
  - Employees should report all applications installed on employees' devices every half year.
  - IT reserves the right to check the apps on employees' devices which are published by suspicious developers or uncertificated by trusted third party.
- Blacklisting and whitelisting applications

  Remove all malicious and untrusted applications identified by IT from your devices.
- Containerization
- Virtualization

Risk Control

- Malware Prevention
  - Employees must install well-known and verified anti-virus and anti-malware programs on their devices. Please contact the IT to require for recommended programs.
  - Employees must maintain regular updates of the anti-virus and antimalware programs on their devices with the most recent signatures.
  - Employees must make sure that the firewall on their devices is open and is able to blocking network traffic from suspected malicious source, and is able to filter and restrict their device access based on network connection, applications type, and other packet attributes such as IP address.

DO NOT COPY

Copyright © 2024 Pei-Shan Hsieh

- Intrusion Detection Prevention
- Auditing

  All employees' devices must be audited annually to check that control measures are operational and the employees are complying with policies.
- Awareness and Training Program

  All employees must annually engaged in face-to-face training programs to increase their focus on security and privacy issues in working environment.

Compliance

- Security/Privacy Principles and Laws

  IT must develop, modify or update clinic's security and privacy policies according to HIPAA (The Health Insurance Portability & Accountability Act).
- Employee Privacy Considerations
  - All employees' personal data access and collection by the clinic must only be carried out when there is a satisfactory warrant in accordance with the authority of law.
  - All employees' personal data shouldn't be disclosed or used for other purposes.
  - All employees are allow to challenge any data collected related to them, to either be erased or amended.

DO NOT COPY

Maintenance

- Internal and External Systems/Devices Update

  The clinic's EHR Information System as well as all employees' device operating systems must be regularly updated.
- Policy Review and Update

  The BYOD policies should be reviewed and updated regularly to ensure adequate control measures that are in compliance with regional laws are in place, and can cope with the continuous demands of BYOD.

Copyright © 2024 Pei-Shan Hsieh