ProTeam Management (PTM) ***Policy Manual***	Section:	Information Technology
	Policy #:	IT CWI 11-2024 V1
	Subject:	**CMS Web Interface Bring Your Own Device (BYOD) Policy**

CROSS-REFERENCES:
CWI Electronic Communications Policy CWI IT Security and HIPAA Compliance Policy

PURPOSE & OVERVIEW

Everyone has a mobile phone/smart phone, many have their own laptops and desktops as well.

In some cases, contractors may wish to incorporate their devices to help perform their work.

This is referred to as “Bring Your Own Device” (BYOD)

This policy outlines when it is acceptable to use your own device and under what technical configuration you are responsible to adhere to.

Our CWI focus is on abstracting sensitive Protected Health Information (PHI). As such, **PTM is contractually obligated to safeguard all PHI per HIPAA requirements.**

These policies are designed to support legal obligations and requirements to (but not confined to):

- Prevent unauthorized disclosure of PHI and confidential information,
- Ensure integrity of PHI and confidential data,
- Implement appropriate retention and disposal of PHI and confidential information,
- Provide employees with training about HIPAA and their responsivities.

POLICY GUIDELINES – Permitted User Devices to access PTM systems

Permitted User Devices to access PTM Information Systems

- PTM issued and owned IT devices (laptops, tablets, etc.)
    - All of which are configured per PTM HIPAA security provisions

- User owned IT Devices (laptop, tablets, mobile phones, watches etc.)
  - MUST comply with PTM HIPAA security provisions
- All users must adhere to PTM HIPAA policies regardless of type of device

POLICY GUIDELINES – HIPAA Security Provisions

- Data Storage – Any kind of digital storage of data "at rest" - Hard Drives, USB Drives, Cloud storage, etc.
  - All data drives must be encrypted using at least AES 256-bit encryption[1]
- Device Access – Logging in to your devices
  - To access your device requires authentication such as a user ID and a password or PIN to access the device
  - Multi Factor authentication[2]
  - Password Management - minimum length and complexity of passwords and passwords must be changed on a regular basis
- Login Management
  - Device locks out of PTM information systems which contain PHI after five failed login attempts
- Automatic Logoff
  - After fifteen minutes of inactivity and require the user to log back into the device
- Applications
  - All application downloads should be scanned for virus before download
- Lost or Stolen Devices
  - Ability for PTM IT to remotely access, wipe and disable any mobile device being used to access PTM systems
- Termination Procedures
  - PTM owned equipment - returned to PTM IT
  - User Owned Equipment - Remote wipe
- Network Security – See CWI
  - PTM property – Same as CWI
  - User Proprietary – Same as CWI
- Transmission
  - PHI can only be transmitted using approved encrypted methods.
  - Email transmissions containing electronic PHI are encrypted and decrypted by the PTM email system using at least AES 256-bit encryption.
  - Other transmissions are encrypted and decrypted using at least 256-bit encryption, such as HTTPS. When applicable, a Virtual Private Network is utilized to access PHI. If a client contract requires a different transmission method, that method will be used as long as it is HIPAA compliant.

[1] What is AES 256 bit encryption (AES)? How does it work?

[2] What is: Multifactor Authentication

CWI IT Bring Your Own Device (BYOD) Policy

Process Owner	Chief Information Officer
Department	Information Technology
Effective Date	December 01, 2024
Revision Date(s)	December 01, 2024
Authorities	

APPROVED BY: CHIEF OPERATING AND INFORMATION OFFICER, MANAGER OF CMS WEB INTERFACE PROGRAMS, MANAGER OF IT OPERATIONS, AND IT SYSTEM ADMINISTRATOR	**DECEMBER 01, 2024**