WEBER HUMAN SERVICES	**Policy & Procedure** HIPAA / PRIVACY **MOBILE COMPUTING DEVICE (MCD) SECURITY**	**NUMBER** 21 **APPROVED** 3/1/2018 **REVIEWED** **REVISED** 1/1/2017

POLICY:
Mobile Computing Device (MCD) Security

PURPOSE:
Weber Human Services (WHS) has established this policy for the secure connection and deployment of mobile computing and storage devices within WHS to support both privacy and security of sensitive information and compliance with applicable agency and regulatory requirements (e.g. HIPAA, local, state and federal laws).

SCOPE:
This policy applies to:

- Employees
- Volunteers
- Students
- Temporary Staff
- Agency and Contracted Staff

This policy covers mobile telecommunication and mobile computing devices which can execute programs or store data. This policy defines the requirements that must be followed when connecting either institutionally or personally-owned MCDs to WHS systems or networks. All MCD equipment procured by WHS is institutional property, regardless of the source of funds from which they were purchased.

DEFINITIONS:
Mobile Computing Device (MCD): Includes laptop and tablet computers, smartphones, and external storage devices.

Confidential or Restricted Data: Includes, but is not limited to, organizational-related personally-identifiable information that is not in the public domain and if improperly disclosed could be used to steal and individual's identity, violate an individual's right to privacy or otherwise harm an individual. Organizational information that is not in the public domain and if improperly disclosed might: cause a significant or severe degradation in mission capability; result in significant or major damage to organizational assets; result in significant or major financial loss; or result in significant, severe or catastrophic harm to individuals whose personal information is under the stewardship of WHS.

This data may include, but is not limited to:

- Behavioral Health-related client information (electronic Protected Health Information)
- Financial information about the Health Center (budget, strategic revenue plans, accounts receivable/payable details.) **NOTE:** Credit card numbers are not to be collected, transmitted, or stored on WHS computing devices and networks under any circumstances.
- Employee HR and financial information
- Any information that includes Social Security numbers
- IDs and/or passwords for access to WHS computing resources

POLICY:

Permissible Use

1. WHS *confidential or restricted data, including email,* is not authorized to be accessed through or stored on either a WHS or non-WHS owned MCD unless all the criteria below are met:

    a. The device stores only the minimum data necessary to perform the function necessitating storage on the device.
    b. Information is stored only for the time needed to perform the function.
    c. The device requires a password for access and is encrypted using methods authorized by the WHS IT Department.
    d. The user will maintain the original device operating system and will not "Jail Break" the device (installing software that allows the user to bypass standard built-in security features and controls).
    e. The user/owner will allow the installation of third party software by the WHS Security Officer or designee to protect the safety and security of the device and will not delete the software from the device.
    f. The user/owner will sign the User Acknowledgment and Agreement, indicating their agreement to comply with the terms of this policy. The signed agreement will be forwarded to HR to be stored in the employee's personnel file.

Institutionally-Owned Devices

1. MCDs will be provisioned using software and/or controls which will be defined by WHS IT Security and may include, but are not limited to:

    a. Encryption of the device
    b. Use of personal identification (PIN) security pattern, password or other form of authentication as provided by the device manufacturer consisting of a minimum of four (4) characters or other form of authentication to gain access to the device.

c. Setting of an inactivity timeout of no more than 15 minutes requiring the password or PIN to be entered when the timeout is excluded.
d. Ability to initiate a remote “wipe” or deletion of data if a credible report is received that the device is lost or stolen.
e. Installation of third party software to protect the safety and security of the device.

Personally-Owned Devices

1. Users will be granted the authority to configure their personally-owned MCDs to access WHS electronic information, under the following conditions:

    a. The user understands and agrees that such access is considered a personal convenience for the user and as such, WHS will not reimburse or otherwise compensate the user for any costs associated with such access. Such costs may include, but are not limited to, monthly call and data plans, long distance calling charges, additional data or roaming fees, charges for excess minutes or usage, equipment, surcharges and any applicable fees or taxes.

2. Users agree to secure their wireless devices using software and/or controls which will be defined by WHS IT Security. These controls may include, but are not limited to, the following:

    a. If the device accesses WHS systems/data of any type:

        i. Use of a personal identification number (PIN) security pattern, password or other form of authentication as provided by the device manufacturer consisting of a minimum of four (4) characters or other form of authentication to gain access to the device.
        ii. Setting an inactivity timeout of no more than 15 minutes requiring the password or PIN to be entered when the timeout is exceeded.
        iii. External storage devices are excluded from i) and ii) above.
        iv. The user/owner will allow the installation of third party software by the WHS Security Officer or designee to protect the safety and security of the device and will not delete the software from the device. IT Security will ensure that the approved security controls, including encryption, are installed on the device.

3. The user understands that he/she may be held liable for any criminal and/or civil penalties that may result from loss, theft or misuse of the confidential information accessed and/or stored on the personal device.

4. Upon termination of affiliation with WHS, users agree:

        a. To immediately delete all institutional data, including email, stored on the device.

b. To remove the WHS email account and WiFi settings from the device.
c. Failure to complete the above may result in the device being auto-wiped by IT Security.

5. The user acknowledges that WHS does not provide support for personally-owned devices and has no liability for such devices. Configuration of any personally-owned device is the user's responsibility.

6. The user acknowledges that access to WHS systems/data through a personally owned MCD can be terminated at any time for any reason.

7. The user agrees that the device will not be shared with other individuals or family members, due to the business use of the device (potential access to email, etc.).

Additional MCD User Responsibilities

1. Users may not bypass or disable WHS-required security mechanisms under any circumstances.
2. Users are expected to take the appropriate precautions to safeguard their MCD against loss or theft.
3. Unauthorized physical access, tampering, loss or theft of an MCD, including a personally owned device that has been granted access to WHS systems/data, must immediately be reported to the WHS Security Officer and the employee's immediate supervisor in order to initiate effective and timely response and remediation of any possible breach of WHS data. The user acknowledges that remediation may include remotely wiping the MCD.
4. Users must abide by the laws governing the use of mobile devices while driving.

Expectation of Privacy: WHS will respect the privacy of personally owned devices and will only request access to the device to implement security controls, as outlined in this policy, or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings (applicable only if user downloads WHS email/attachments/documents to their personal device.) This differs from policy for WHS owned devices where WHS employees do not have the right, nor should they have the expectation, of privacy while using WHS equipment or services. While access to the personal device itself is restricted, WHS policy regarding the use/access of WHS email and other WHS systems/services remains in effect.

Enforcement

1. Failure to adhere to this security policy and associated procedures may result in sanctions as per applicable WHS policy.

User Acknowledgement and Agreement

It is WHS' right to restrict or rescind computing privileges, or take other administrative or legal action due to failure to comply with the WHS Mobile Device Security Policy. Violation of this policy may be grounds for disciplinary action up to and including termination.

I acknowledge, understand and will comply with the WHS Mobile Device Security Policy, as applicable to my usage of WHS systems/data.

Should I later decide to discontinue my use of WHS systems/data through my personally owned MCD, I will allow WHS to remove and disable any WHS provided third-party software and services from my personal device.

Employee Name: _____

Employee ID: _____

MCD(s) given access to WHS systems/data: _____

_____

WHS services to be used: _____

Employee Signature: _____ Date: _____

For IT Use Only:

Encryption Verified: ☐

Third Party Security Software Installed: ☐

IT Employee Signature: _____ Date: _____