WEISMAN CHILDREN'S REHABILITATION HOSPITAL (WCRH)

Administrative Manual

SUBJECT: Portable Device Guidelines **NO: AM 3.29**

EFFECTIVE DATE: September, 2010 **PAGE 1 of 4**
REVIEWED/REVISED: 5/11; 5/12; 1/13; 1/14; 1/15; 11/16; 10/17; 1/18; 1/21; 1/24; 3/25; 3/26

PURPOSE:

This policy establishes employees' responsibilities when utilizing laptop computers and other portable devices. Because of the high risk that laptop computers and other portable devices create for a potential privacy breach, it is paramount that guidelines be established to outline employees' responsibilities when utilizing laptop computers and other portable devices.

POLICY:

Off-site use and access to private health information shall be permitted only when deemed necessary by the supervisor. Authorization for remote access shall be granted by the Administrator based solely on the role within WCRH and the need to access data. Staff members must adhere to the guidelines set forth by WCRH and immediately follow prescribed procedures if a device is lost or stolen or if information is in any way compromised. Staff members must notify their supervisor and the organization's privacy/security officer of any incident. Upon notification to the privacy officer, the Information Technology Department will be contacted to disable the device remotely. Secondly, staff members must contact law enforcement officials and file a police report.

If an employee must access PHI from a personal computing device due to their corporate-managed or issued device being unavailable, they agree to follow the guidelines outlined in the EMR Remote Access Usage Policy.

While random searches will not be conducted, employees may be required to provide access to personal devices used to access PHI in the event of legal proceedings or audits to facilitate the collection of unique data (data that cannot be obtained through other company sources).

Additionally, if they have any concerns regarding the integrity or security of the PHI data on their BYOD (bring your own device), they should report the incident to their department head and/or the IT department immediately. This includes, but is not limited to the loss or theft of personal devices used to access PHI.

Definition: Portable Devices include, but are not limited to, memory storage in laptops, mobile phones, tablets, wearable technology (such as smart glasses, smart watches, and other body-worn devices capable of recording, storing, transmitting, or displaying data), and any removable or transportable digital storage media, including external hard drives, USB flash drives, SD cards, CDs, DVDs, and other electronic storage devices.

Note:

The use of voice communication systems, fax machines, telephones, and paper documents is not considered the use of a portable device for the purposes of this policy.

PROCEDURE:

If a portable device has been provided for use when conducting WCRH business, the staff member is required to adhere to the procedures as outlined below. If a question arises, the staff member may contact the IT Department or the Privacy Officer.

1. Employee communication is not private. Wide varieties of laws govern privacy, confidentiality and data security. Many of these laws apply to those staff members who have access to portable devices. In addition, WCRH has defined further guidelines that govern the use of hospital and personal equipment that may be used for hospital activities. These include (but are not limited to):

    a. WCRH treats all correspondence, paper or electronic, as WCRH property. Access to the information systems may be monitored and there should be no expectation of privacy.
    b. Deletion or destruction of electronic mail messages and accompanying logs must be postponed if a subpoena, discovery motion or other legal notice has been received or is imminent.
    c. WCRH e-mail system may not be used to solicit for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations.
    d. Staff is prohibited from making any online statement about WCRH, its position on any issue, or a competitor.
    e. No one may create and/or transmit an electronic message or information to another employee, which could be viewed as offensive or disruptive in nature.
    f. Passwords are an important part of our information security program. If you choose a password that is easy to guess or is written where anyone can see it, you have weakened our security system.

2. Portable devices can provide access to WCRH Information.
    a. Make a written note of the make, model and serial number of your portable device and keep the information in a safe, easily accessible place, e.g. wallet. If the device is stolen, an accurate description will be able to be given to the police.
    b. If the laptop computer requires a user ID/password combination for access, do not affix this information to any part of the computer and do not share this information with others.
    c. Do not leave the portable device unattended or unsecured. Examples of places that a portable device should not be left attended include: a vehicle, restroom, taxi, train, internet café, hotel room, conference room or a lounge.
    d. Regularly back up your files to WCRH's network. This will aid in identifying what was lost and will allow one to continue working with as little disruption as possible.
    e. Lock it or lose it. A portable device that is visible or unattended becomes a target of opportunity to a thief. Use common sense; safeguard portable devices when you transport them.
    f. DO NOT download and install unauthorized programs not approved by the IT department onto your laptop computer.

3. Once approval has been obtained to grant remote access to an employee, the supervisor of the employee will contact the Information Technology Department to obtain the requested equipment.
    a. When the equipment has been received, it will be given to the requesting supervisor.
    b. The supervisor and the employee will complete each respective section of the form “Distribution of Portable Device” (see attached, 3 29.1).
    c. Upon completion of the form, the equipment may be issued by the supervisor. The Distribution of Portable Device Form (“FORM”) will be placed in the employee’s personnel file. Upon employee termination, the FORM will be completed and signed by the supervisor and returned to the employee personnel file.
    d. The employee will then be responsible for any equipment that has been issued to him/her. Upon termination, the employee will be held responsible for return or for the replacement cost of the device. Note: the replacement cost may be taken from the employee’s final paycheck.
    e. For remote access to Electronic Medical Records (EMR) through the CPSI/Thrive web portal, approved employees will review and sign the EMR Remote Access Usage Policy form (see attached, 3 29.2). This form will be placed in the employee’s personnel file.

4. This policy will be enforced when non-compliance is discovered through a report or observation. If the portable device is lost or stolen due to any act or omission, disciplinary action, termination of employment, and/or prosecution depending on the severity of the incident may occur. To report a theft or loss contact the local police department, your supervisor and the Privacy Officer with the following information:

    a. Serial number, make and model of the portable device
    b. Date and location of the incident
    c. Police officer’s name, badge number and the report number
    d. The name and contact information of any witness to the incident.

_____

Administrator

Employee EMR Remote Access Usage Attestation Agreement

Ensuring the security and confidentiality of patient information is a top priority. When accessing Electronic Medical Records (EMR) remotely through the CPSI/Thrive web portal, it is essential to follow healthcare industry best practices to protect sensitive data and comply with HIPAA regulations. Please adhere to the following guidelines:

1. Avoid Using Public Computers – Public or shared computers in libraries, cafes, or other open areas are not secure and should never be used to access EMR systems.

2. Always Log Out – After accessing patient data, always log out completely from the EMR system. Simply closing the browser window does not guarantee a secure logout.

3. Never Leave Your Computer Unattended – If you must step away, ensure that your computer is locked or logged out to prevent unauthorized access.

4. Do Not Use Public Wi-Fi When Possible – Public Wi-Fi networks are often unsecured, making them a high risk for cyber threats. Use a secure, private network when accessing patient records remotely.

5. Utilize Multi-Factor Authentication (MFA) – Whenever remote, ensure you are being prompted for an MFA access code for an additional layer of security to protect access to patient records.

6. Be Wary of Phishing Attempts – Do not click on suspicious links or provide login credentials in response to unsolicited emails or messages.

7. Avoid Using Non-Corporate Managed Devices – When possible, do not access EMR data on a personal or non-corporate managed device. If you must use such a device, do not perform any other functions or have any other applications open, such as checking personal email or browsing unrelated websites when accessing patient data. Keep your computer and mobile devices updated with the latest security patches and antivirus software to minimize vulnerabilities.
8. Stored User Name and Passwords – Saving User Name and Password on any personal device is strictly prohibited.

By following these best practices, we can maintain the integrity and confidentiality of patient data while enabling secure remote access. If you have any questions or need further guidance, please contact the IT Department.

Acknowledgment and Agreement

☐ I acknowledge that I have read and understand the EMR Remote Access Usage Policy. I agree to comply with these policies and understand that failure to do so may result in loss of remote access privileges.

Signature:_____
Print Name:_____ Date:_____