Protecting Patient Information: Telework Quick Reference Guide to Complying with HIPAA

Telework Quick Reference Guide

This Telework Quick Reference Guide is a supplement to the MFA's current guide to complying with HIPAA. Please make sure you have reviewed that document, which can be found on The Connector. Click here to view the full guide to complying with HIPAA.

If you have any questions about patient privacy, the content of either guide, or any issues involving HIPAA, please reach out to privacyofficer@mfa.gwu.edu.

Connectivity: VDI (VMware) is Best

VMware is the preferred tool to connect and work remotely. It allows full access to the MFA's servers and applications, including Email, Allscripts, IDX, Office 365, WebEx and Jabber.

- **ISTConnect.org** is MFA's landing site for accessing links on how to connect and work remotely.
- Working through VMWare allows you to save documents on the shared network drives so they are secure, backed up, and available to the rest of your team and encrypted in accordance with our HIPAA Privacy and Security requirements.

Phone

Jabber is strongly recommended and preferred, especially if you need to contact patients. However, if this is not possible then your cell or home phone is acceptable to use.

- **WHEN LEAVING MESSAGES:** Remember to only state the minimal amount of information necessary for the patient to return your call (you are calling from the MFA, your name and number where you can be reached).

Printers, Copiers and Scanners, Oh My!

All of these replication devices typically have hard drives and are rarely encrypted – something that HIPAA requires.

- Do NOT use your personal replication devices for any task that involves PHI.

Paper is Evil

Paper with patient information should typically never leave the MFA premises. If there is a business need where this cannot be avoided then:

- It needs to be logged out, and back in (review with your manager what this process will be for your department).

- Transportation of paper, if necessary, should be in closed containers, ideally locked, and never left in cars.

Work on documents electronically and keep them in that state. Paper should not typically ever be created outside the MFA.

- If it is, you should store it securely and bring it back to MFA to be shredded.

Managers and staff should think through each specific workflow for ways to eliminate, minimize or group tasks that require interacting with paper. If you need to send out letters periodically to patients, there are a couple of options:

- Draft them as part of the normal workflow, but save printing them until you have a bunch ready and come into the office to do so.
- Convert them into PDFs and email them securely using "**FSecure"** (Force Secure).

E-mailing

Generally, we do not email with patients. Given the need for social distancing, it may be desired to do so. If so, we need remember the following guidelines and **ALWAYS ENCRYPT.**

- Always use your MFA email account – do NOT under any circumstances use a personal email account for MFA business.
- Never include any sensitive information in the subject line of an email regardless of encryption method used – it is never encrypted.

There are two options for email encryption:

1. ZSecure – Easy Secure

- Base level TLS Encryption. Shows up in the recipient's mailbox as long as their mail service is configured with the TLS protocol (most, including Gmail, are).
- Should be used for benign messages with limited sensitivity and individualized content.
- No way to track or recall.

2. FSecure – Force Secure

- Higher level of encryption requiring the recipient to sign into a secure portal to retrieve the message.
- Should be used for attaching documents and emails with any sensitive communication.
- Messages expire after 14 days.