MOBILE DEVICES

Examples of mobile devices include:

- smartphones
- laptops
- USB drives
- tablets

All mobile devices that were issued by MU or are the personal property of the employee must be password protected and have encryption activated.

All MU issued laptops or tablets must have encryption turned on and have remote wipe software installed.

PHI should **NEVER** be texted.

PHOTOGRAPHS OF PATIENTS SHOULD NEVER BE TAKEN WITH PERSONAL DEVICES SUCH AS SMARTPHONES OR CAMERAS.

DISPOSING OF PHI

University of Missouri Health is not allowed to abandon PHI or dispose of it in dumpsters or other containers that are accessible by the public or unauthorized persons.

Documents containing PHI should NEVER be placed in blue recycling bins. Always place documents that have PHI on them in locked shredding bins.

Prescription bottles, IV bags and other medical supplies labeled with PHI must have the labels made unreadable prior to disposal in the proper receptacle.

PHI on electronic media must be overwritten or cleared of sensitive information, purged (exposing the media to a magnet) or shredded.

Question:
CAN PHI BE DISCARDED IN BLUE RECYCLING BINS?

Answer:
NO. Protected Health Information must be discarded in appropriate locked shredding bins.

For more information, please contact:

Tina Adams-Salter

System Privacy Officer

Phone: 573-882-3293

Email: adamstin@health.missouri.edu

HIPAA/HITECH Privacy *and* Data Security Program

Health
University of Missouri

HIPAA

HIPAA is the acronym for the Health Insurance Portability and Accountability Act that was passed by Congress in 1996. HIPAA consists of a Privacy Rule and a Security Rule.

HIPAA provides federal protections for individually identifiable health information and gives patients an array of rights with respect to that information.

HITECH

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law in February 2009.

It significantly expanded the reach of the HIPAA Privacy Rule and Security Rule, along with the corresponding penalties.

Question:

WHAT DOES HIPAA AND HITECH PROTECT?

Answer:

PROTECTED HEALTH INFORMATION OR PHI. PHI is **ANY** and **ALL** information obtained during a health care encounter.

DISCLOSURES FOR TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS

Protected Health Information may be used or disclosed for treatment, payment, or health care operations, or required by law without a patient authorization.

MINIMUM NECESSARY STANDARD

When accessing, using or disclosing PHI, or requesting PHI from others, HIPAA requires that you use the minimum amount of information necessary to accomplish the intended purpose.

ACCESS AND USE

You may only access, use, and t disclose PHI in order to do your job. You **CANNOT** access or look at **YOUR OWN** medical record, a family member's, a friend or a co-workers.

Never leave PHI out for people to see. When PHI is not in use, file it away or turn it face down. L

EMAIL

MU Health Care emails ending in either health.missouri.edu or missouri.edu are on our network and are considered secure.

Emails going out of MU Health Care are considered non-secure email and must have the word secure in square brackets ([secure]) in the subject line of the email.

Do not use patient specific information in the subject line of the email.

SOCIAL MEDIA

All employees are personally responsible for their own comments online.

When away from work, employees are subject to the same HIPAA and HITECH regulations that they are subject to at their job.

Postings on social media platforms should not discredit MU Health, Co-workers, visitors and patients or contain PHI..

Communicating protected health information online is a HIPAA/HITECH violation that will lead to disciplinary action.

NEVER POST PICTURES OF PATIENTS ON SOCIAL MEDIA PLATFORMS.

BREACH

A data breach is the intentional or unintentional release of PHI to a person or location that is not authorized to access the information.

REPORT ALL SUSPECTED BREACHES TO THE SYSTEM PRIVACY OFFICER.

COMPUTER ACCESS SAFEGUARDS

Passwords must always be kept private. **NEVER** share your passwords with anyone. Always be aware of persons within view of your computer screen. ALWAYS log off/lock your computer when leaving it unattended.

Confirmation of Receipt of HIPAA Brochure

This is to Certify that I have received a copy of the HIPAA/HITECH Privacy and Data Security Program Brochure.

_____

Name Date