Frequently Asked Questions about HIPAA Privacy

Please use this page as a quick reference for frequently asked questions about HIPAA privacy. If you have additional questions or need clarification, please reach out to our helpline 813-974-2222 or privacy@usf.edu.

What does the HIPAA Privacy Rule do?

The HIPAA Privacy Rule creates national standards to protect individuals' medical records and other personal health information. The Privacy Rule gives patients more control over their health information; sets boundaries on the use and release of health records; establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information; holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights; and it strikes a balance when public responsibility supports disclosure of some forms of data – for example, to protect public health.

For patients – it means being able to make informed choices when seeking care and reimbursement for care based on how personal health information may be used. It also:

- enables patients to find out how their information may be used, and about certain disclosures of their information that have been made;
- generally limits release of information to the minimum reasonably needed for the purpose of the disclosure;
- generally gives patients the right to examine and obtain a copy of their own health records and request corrections; and
- empowers individuals to control certain uses and disclosures of their health information.

What are Permitted Uses and Disclosures in HIPAA?

The HIPAA Privacy Rule defines when, under federal law, a covered entity such as USF Health may use or disclose an individual's Protected Health Information (PHI). In general, a covered entity may only use or disclose PHI if either:

- the HIPAA Privacy Rule specifically permits or requires it; or
- the individual who is the subject of the information gives authorization in writing. However, please note that other federal or state privacy laws may apply.

For example, the HIPAA Privacy Rule specifically permits a use or disclosure of PHI for the covered entity that collected or created it for its own **treatment, payment, and health care operations** activities. Similarly, HIPAA also permits the covered entity that collected or created the PHI to disclose it to another covered entity for treatment, payment, and in some cases, the health care operations of the recipient covered entity.

If the covered entity wishes to use or disclose the PHI for something other than treatment, payment, or health care operations, it must obtain patient authorization to do so, unless the use or disclosure is permitted by another provision of the HIPAA Privacy Rule.

Who may access protected health information (PHI)?

Only those workforce members who need access for a HIPAA authorized business reasons and who have been authorized to receive it. Providers who are delivering health care treatment to a patient may access the patient's protected health information. All others who are either engaged in health care operations or payment operations may only access the "minimum necessary" amount of PHI in accordance with performing his or her job role.

What is meant by having access to the "minimum necessary" information to perform your job role?

The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires USF Health to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. The minimum necessary standard does not apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an individual's authorization.
- Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
- Uses or disclosures that are required by other law.

The implementation specifications for this provision require USF Health to develop and implement policies and procedures appropriate for its own organization, reflecting the entity's business practices and workforce. While guidance cannot anticipate every question or factual application of the minimum necessary standard to each specific industry context, where it

would be generally helpful, we will seek to provide additional clarification on this issue in the future. In addition, the Department will continue to monitor the workability of the minimum necessary standard and consider proposing revisions, where appropriate, to ensure that the Rule does not hinder timely access to quality health care.

What is the difference between "consent" and "authorization" under the HIPAA Privacy Rule?

The Privacy Rule permits, but does not require, a covered entity voluntarily to obtain patient consent for uses and disclosures of protected health information for treatment, payment, and health care operations. Covered entities that do so have complete discretion to design a process that best suits their needs.

An “authorization” is required by the Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization.

Who is our privacy officer?

USF Health and USF Tampa General Physicians’ Privacy Officer is Barbara J. Wolodzko.

Who is responsible for maintaining a secure environment and patient privacy?
Every workforce member here at USF Health is responsible for protecting our patients’ privacy.

May I discuss patients with my spouse if he/she doesn't work here and promises to keep it secret?
No.

Am I permitted to look up my sick father's medical record?
No. You are not allowed to access a patient’s medical record unless you are doing so in your employment role.

Does the HIPAA Privacy Rule permit a doctor to discuss a patient's health status, treatment, or payment arrangements with the patient's family and friends?
Yes. The HIPAA Privacy Rule specifically permits covered entities to share information that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient’s care or payment for health care. If the patient is present, or is otherwise available prior to the disclosure, and has the capacity to make health care decisions, the covered entity may discuss this information with the family and these other persons if the patient agrees or, when given the opportunity, does not object. The covered entity may also share relevant information with the family and these other persons if it can

reasonably infer, based on professional judgment that the patient does not object. Under these circumstances, for example:

- A doctor may give information about a patient's mobility limitations to a friend driving the patient home from a clinic visit.
- A clinic may discuss a patient's payment options with her adult daughter that is present during the office visit.
- A doctor may instruct a patient's roommate about proper medicine dosage when she comes to the patient's appointment.
- A physician may discuss a patient's treatment with the patient in the presence of a friend when the patient brings the friend to a medical appointment and asks if the friend can come into the treatment room.

If I have Epic access, am I permitted to view my own medical record electronically? If I do so, is that considered a HIPAA violation?

You are only permitted to view your own medical record via Epic if you are a credentialed treating provider and your license permits self-treatment. Such treatment would be documented in Epic as appropriate. Otherwise, you must access your own medical record via either MyChart or by requesting a copy of your medical record by reaching out to Health Information Management.

No. It is NOT a HIPAA violation to view your own medical record via Epic but it is a violation of USF Health policy if you do so without being a credentialed provider whose licensure permits self-treatment that is documented in Epic.

We know that medical records whether paper or electronic are confidential. What about handwritten notes and phone calls?

All forms of patient protected health information written, spoken, or electronic are confidential and must be protected.

How should you dispose of confidential papers?
Put them in the locked shredder bin in your area. Make sure you always leave your workspace free of paper PHI before you leave at the end of your shift.

Who is responsible if I "lend" my password to my co-worker, and she uses it to look up information on a friend she's concerned about?
Both of you have violated USF's policy and may be subject to sanctions. Each workforce member is responsible to keeping his or her login and password protected.