



HIPAA COMPLIANCE

PROTECTING PATIENT PRIVACY: EVERYONE’S RESPONSIBILITY

**What is HIPAA?** The Health Insurance Portability & Accountability Act of 1996 and the regulations which were enacted by the US Department of Health and Human services to implement the Act, provide new rules for how hospitals and other health-care providers, such as UPMC, are permitted to use and disclose or release patient information.

**Who is affected?** All healthcare organizations and providers, such as UPMC, our medical staff and any member of UPMC’s “workforce.”

**Are there penalties?** HIPAA calls for severe civil and criminal penalties for noncompliance, including fines up to \$25,000 for multiple violations of the same standard in a calendar year; fines up to \$250,000; and/or imprisonment up to 10 years for knowing misuse of identifiable patient information.

**Privacy and Confidentiality:** In general, privacy refers to a patient’s right to access his/her health information. The rule covers all individually identifiable health information that health care organizations and providers, such as UPMC, possess.

**The Privacy standards:**

- limit the use and release of private health information without patient/parent consent;
- give patients new rights to access their medical records and to know who else has accessed them;
- restrict most disclosure of health information to the minimum needed for the intended purpose;
- establish new criminal and civil sanctions for improper use or disclosure; and
- establish new requirements for access to records by researchers and others.

**Implementing HIPAA :** It is the policy of UPMC to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule pertaining to the use and disclosure of Protected Health Information (PHI). A number of policies have been developed to assist in our compliance efforts. A student’s access to a patient’s medical record shall only be with the written authorization of his/her UPMC Sponsor.

**Questions?** If you have any questions about how patient information should be used or shared with others outside of the UPMC Health System, you should contact the Corporate Compliance and Privacy Officer at (412) 692-7842.

**Non-Compliance:** Your failure to abide by the HIPAA regulations and UPMC policies concerning patient information may result in your immediate dismissal from the Shadow Program, as well as all other penalties described above.

---

Program Participant (sign)

---

Date