HIPAA HIGHLIGHTS

December 2023

Reporting a Possible Breach Of PHI

What is a breach?
A breach occurs when PHI is inappropriately acquired, accessed, used, or disclosed. PHI stands for Protected Health information.

What should I do if I think a potential breach has occurred?
IMMEDIATELY notify your supervisor. You or your supervisor must contact a HIPAA Privacy Officer or the URMC Integrity Helpline at 585-756-8888. Calls to the Helpline may be made anonymously. All staff, faculty, volunteers and trainees / students should refer to 0P31 URMC and Affiliates HIPAA Privacy Training Module.

What happens after I report a breach?
A Privacy Officer will conduct an investigation to determine if the breach is reportable, and how to reduce possible harm caused by the breach. When a breach is reportable, we must notify each individual whose PHI was breached and the Office for Civil Rights. We are also required to notify the NYS Attorney General's Office and may be required to notify other organizations. **There are strict regulatory timelines required for these notifications so it is important to promptly inform the Privacy Office of any suspected breach.** The Privacy Office will coordinate all required notifications.

What are examples of possible breaches of PHI?
Possible breaches of PHI may include, but are not limited to:

- A patient concern alleging a breach of HIPAA.
- Prescriptions, after visit summaries, or other documents provided to the incorrect patient.
- Looking at PHI without a legitimate, business-related reason for doing so, snooping; for example, accessing patient medical records for personal reasons including family members, friends, neighbors.
- Postings to social networking sites or text messages that contain information which may make it possible to identify a patient.
- Loss or theft of computers, flash drives, paper files, etc., that may contain PHI regardless of whether the device or media is owned personally or by URMC & Affiliates.
- Improper disposal of PHI (computer files, paper, flash drives, medication containers, photos, etc.).
- Misdirected mail, e-mail, or faxes; e.g. emailing PHI intended for a co-worker via "reply to all" when some recipients are external. If an email is sent in error, immediately recall the email and notify a Privacy Officer.

All staff, faculty, volunteers and trainees / students need to follow the 0P31 HIPAA Privacy Policy, 0P31 Policy Breach of Unsecured Protected Health Information.

For information on this or other HIPAA-related topics, please refer to URMC's HIPAA Intranet site or contact your Privacy Officer or HIPAA Security Official.