HIPAA HIGHLIGHTS

March 2022

Prompt Reporting of Possible Breaches of PHI – Policy Review

Policy 0P31 Breach of Unsecured Protected Health Information (PHI)
All workforce members of URMC and Affiliates are required to promptly report possible breaches of protected health information (PHI) as soon as they are discovered, including any suspected breach by a business associate of URMC and Affiliates.

Who needs to follow this policy?
Any staff, faculty, volunteer or student who becomes aware of a possible breach.

What is unsecured PHI?
All PHI is "unsecured" unless it has been made unreadable or not understandable in any form such as through encryption of electronic PHI or proper disposal or destruction of PHI when it is no longer needed.

What is a breach?
A breach occurs when unsecured PHI is inappropriately acquired, accessed, used, or disclosed.

What should I do if I see or learn of a breach?

- If you become aware of a possible breach of PHI, you should immediately notify your supervisor. You or your supervisor must call the URMC Integrity Hotline at 585-756-8888 or contact a Privacy Officer. Calls to the Hotline may be made anonymously.
- It is very important that you contact the Hotline or a Privacy Officer right away since there are strict deadlines to follow for breach investigations.

What happens after I report a breach?

A Privacy Officer will review the information and coordinate an investigation to determine how to reduce possible harm caused by the breach and whether the breach is reportable. When a breach is reportable, we must notify each individual whose PHI was breached and the Office for Civil Rights within the required time frame. In addition, we are now required to notify the NYS Attorney General's Office and may be required to other organizations. The Privacy Office will also coordinate any 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.
- Looking at PHI without a legitimate, business-related reason for doing so; for example, accessing patient medical records for personal reasons.
- Postings to social networking sites, blogs, 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.
- Evidence of "hacking" into computer files or Web sites.
- Misdirected mail, e-mail, or faxes; e.g. emailing PHI intended for a co-worker via "reply to all" when some recipients are external.
- Improper disposal of unsecured PHI (computer files, paper, flash drives, medication containers, photos, etc.).

More information can be found at the URMC and Affiliates HIPAA Privacy Training Module for this policy.

Your Privacy Officer and HIPAA Security Official are available to answer questions about HIPAA, or you may refer to URMC's HIPAA Intranet site.