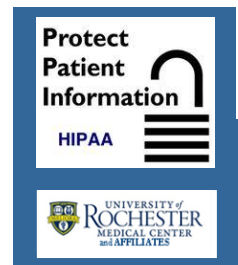


HIPAA HIGHLIGHTS

February 2024



Keeping Data Safe: A Look at Data Security in Healthcare

The healthcare industry juggles a precious commodity: data. We interact with it daily, whether incidentally or as part of our jobs. And data breaches in healthcare are on the rise, exposing sensitive information and posing a significant threat to patient privacy and safety. Understanding the [University's Data Security Classification Policy](#) helps each of us with understanding when data can be shared, with whom and helps each of us prevent data breaches.

Why is data security so crucial?

- **Patient privacy:** Breaches can expose personal details, diagnoses, and treatment histories, leading to identity theft, discrimination, and emotional distress.
- **Financial implications:** Healthcare organizations face hefty fines and lawsuits for non-compliance with data protection regulations.
- **Operational disruption:** Breaches can cripple IT systems, delaying care and impacting patient outcomes.
- **Erosion of trust:** Data breaches can damage the trust patients have in healthcare systems.

Beyond the basics:

[Data Security Classifications - At a Glance](#), introduces examples of high, moderate and low risk data and some appropriate handling measures.

Protecting the House:

Safeguarding against data threats requires a multi-layered approach:

- **Using strong, secure passwords & passphrases and keeping them safe:** Ensuring that bad actors can't access our data.
- **Securing devices when not in use:** Ensuring data is not lost or access inappropriately.
- **Recognizing the latest scams & cyberattack techniques:** By reading the weekly @Rochester security tips, participating in Ask Security Anything and other information sessions
- **Staff training:** Educating employees on cybersecurity best practices and phishing awareness.
- **Backing up data in approved storage areas:** Using URMC Box, SharePoint or OneDrive.

The future of data security in healthcare:

As technology advances, so too must data security measures. Watch the @Rochester security tips for upcoming information on sharing data with AI assistants like Copilot or ChatGPT.

And Remember: Data security is not a one-time fix, but an ongoing commitment. By prioritizing patient privacy and implementing robust security measures, we build a safer, more trustworthy environment for everyone.

For additional information on any HIPAA-related topics, please refer to the URMS intranet site at <http://sites.mc.rochester.edu/departments/hipaa/>. For any questions regarding HIPAA, please contact your [Privacy Officer](#) or [HIPAA Security Official](#).