# HIPAA HIGHLIGHTS

*May 2025*

## *The Key to Strong Security Begins with Your Password*

Passwords are the first line of defense against cybercriminals. One of the simplest ways to protect yourself and the University is to use secure passwords for your accounts. Think of your password as the lock on the front door of your home. You want a robust and secure deadbolt to keep out any intruders. Strong passwords are essential to prevent unauthorized access to our personal and business data.

### Creating Strong Passwords

| | |
|---|---|
| **Length:** Aim for at least 12-15 characters. Longer passwords are harder to guess or brute force crack. | **Complexity:** Include a mix of uppercase and lowercase letters, numbers, and symbols. Use passphrases rather than a single password. |
| **Avoid Common Mistakes:** Don't use easily guessable passwords like "password123" or birthdays, which are common targets for hackers. | **Avoid Personal Information:** Don't use easily identifiable details like names, pets, or the street you grew up on. |
| **Use Unique Passwords for Every Account:** Using the same password across multiple platforms is akin to using the same key for every door. Protect your data by creating unique, one-of-a-kind passwords for each of your online accounts to ensure that cybercriminals cannot access your other accounts. | |

### UR's Password Keeper

Keeper is a secure password management tool that employs end-to-end encryption to ensure your logins and files are always secure. The University offers Keeper Password Manager for free to all faculty, staff, and students. Once you've signed up, you can also share this service with up to 5 family members. Check it out @ https://tech.rochester.edu/services/keeper/ (annual registration is required to maintain your free account).

### Safe Password Practices

| | |
|---|---|
| **Enable Two-Factor Authentication (2FA):** Two-factor authentication adds an extra layer of security by requiring a second form of verification, such as an app on your phone used to verify your login. It's important to enable 2FA on financial accounts like bank accounts or credit cards to prohibit cybercriminals from gaining access to your account. | **Use a Password Manager:** Managing numerous complex passwords can be overwhelming. A password manager securely stores your credentials, generating strong passwords and auto-filling login information. |
| **Don't Share Your Passwords:** Unless through a password manager. | **Regularly review passwords:** Review and update your passwords to stay ahead of evolving threats. |

Your personal data is just that, yours. You should always have the peace of mind knowing that your personal information is safe and accessible! By following these guidelines and utilizing the resources provided by the University, you can ensure that your passwords are strong and your data is secure.

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.