What information and Data should you Safeguard?

More and more, personal data is stored online. And, of course, anything online can be hacked, stolen, and leveraged to the rightful owner's detriment. Unfortunately, that doesn't just apply to your credit card information, but to your personal health data, financial information, and any data collected on you as you wander the internet, as well.

What is HIPAA (Privacy Rule)?

The Privacy Rule standards address the use and disclosure of individuals' health information (known as *protected health information* or *PHI*) by entities subject to the Privacy Rule. These individuals and organizations are called "covered entities."

HIPAA designated healthcare entities must safeguard PHI during storage, use and disclosure. These safeguards apply to the Privacy and Security of the data and must include:

- Administrative Safeguards (e.g. policies, procedures, training, contractual agreements)
- Physical Safeguards (e.g. doors, privacy curtains, locking cabinets)
- Technical Safeguards (e.g. password protected computers, encryption)

For more information on HIPAA and the regulations that covered entities have to follow, please visit https://compliance.uccs.edu/news/health-insurance-portability-and-accountability-act-1996-hipaa

What is FERPA?

FERPA is a federal act designed to protect the privacy of college students by limiting access to their student records. Once a student enrolls in college (please note that FERPA does not apply until a student begins taking classes), he or she can determine what types of information parents and other caregivers can access.

This information falls into three basic categories:

- Financial records (i.e. bills and financial aid information)
- Educational records (i.e. grades and class schedules)
- Student life records (i.e. disciplinary actions).

For more detailed information on FERPA and the regulations please visit https://registrar.uccs.edu/ferpa-the-family-educational-rights-and-privacy-act

What is PCI?

PCI DSS is a cybersecurity standard backed by all the major credit card and payment processing companies that aims to keep credit and debit card numbers safe. PCI data is anything related to your Credit Card information or Card Holder Data. The 16 digit account on the front of the card, CVV number on the back, magnetic strip data, and chip data. All of these need to be protected by any business taking Credit Card information as a form of payment.

Credit Card information is very sought after by malicious actors. For this reason, it is paramount to keep this data safe. While businesses do this because it is mandated to do so. It is important that we as users also do our part to keep this information safe.

How to keep CC information safe?

- Do use Apple Wallet and Google Wallet
- Do use your banks monitoring and alerting on Credit Card usage
- Do be wary of websites that are selling items/services too good to be true
- Don't give out CC information to unknown persons
- Don't enter CC information into a website over a Public WiFi Network

For more information on Credit Card security please reach out to Security@uccs.edu

#BeCyberSmart #CybersecurityAwarenessMonth #security@uccs.edu