THE UNIVERSITY OF CHICAGO | Biological Sciences Information Security Office

October 2022

Cyber Security Awareness Newsletter

Protecting yourself and information from cyber security threats

We are in October with Cybersecurity Awareness Month events well on the way! We hope you enjoy and learn from the lineup of tech talk events listed here: https://security.uchicago.edu/tech-talk-series-registration-page/
If at any point you have any questions on any of the content, please e-mail us at security@bsd.uchicago.edu.

Highlight for this month:
For faculty, staff, students, and trainees who work with Research Health Information (RHI), a new change has been made to RHI and new guidelines surrounding RHI use with software have been created.

What is RHI?
Research Health Information (RHI) - RHI is UChicago Medicine (UCM) patient data that is approved to be used for research by the BSD IRB.

The change?
RHI is does not fall under HIPAA protections. While RHI does not fall under HIPAA protections, it is still subject to state Privacy Laws. RHI is still the personal information of our patients and should be treated with the same level of security as we would treat PHI.

This following step must be followed prior to using software with RHI:

Steps	Guideline	Description
1	IRB Approval	Approved IRB Protocol must include reference to the software and the purpose of its use.
2	Data Sharing	If the software is used to share data outside of University of Chicago, there must be an appropriate Data Use Agreement (DUA) or Data Transfer/Collaborator Agreement in place.
3	Information Security and Privacy Review	The software and its use must have BSD Information Security (BSD ISO) System Assessment and Authorization (SAA) prior to use. IRB number as well any relevant Data Use or Sharing Agreements and contract will need to be provided for the review. BSD ISO will engage the UChicago Privacy Office as needed during the SAA process. SAA information can be found at https://security.bsd.uchicago.edu/bsdsaa/.

More information can be found here: Guidelines for Use of Systems with RHI.

This month's newsletter is short as we recap topics leading into Cybersecurity Awareness Month – See Yourself In Cyber. Our highlighted actions for this month:

- **Think Before You Click: Recognize and Report Phishing:** If a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.
    - Quick tip for spotting a phishing email:
        - Contains an offer that's too good to be true
        - Language that's urgent, alarming, or threatening
        - Poorly crafted writing with misspellings and bad grammar
        - Greetings that are ambiguous or very generic
        - Requests to send personal information
        - Urgency to click on unfamiliar hyperlinks or attachments
        - Strange or abrupt business requests
        - Sending e-mail address doesn't match the company it's coming from
    - Report suspicious emails to security@bsd.uchicago.edu
- **Update Your Software:** Don't delay -- If you see a software update notification, act promptly. Better yet, turn on automatic updates. Always

implement in test before you apply in production. When downloading a software update for any application, only get it from the company that created it. Hacked, pirated or unlicensed software versions often contain malware and cause more problems than they solve.

- **Use Strong Passwords:** Use passwords that are long, unique, and randomly generated. Password managers can generate and remember different, complex passwords for each of your accounts. A passwords manager will encrypt passwords, securing them for you! Lastpass, Onepassword and Bitwarden are our currently recommended password managers. On the horizon, the University is looking into a password manager for the institution.
- **Enable Multi-Factor Authentication:** You need more than a password to protect your online accounts, and **enabling MFA makes you significantly less likely to get hacked.** In case your password becomes compromised, the second factor, like a text, email, or passcode verification, will keep your account—and in turn your data—safe from malicious actors.