Great Ways to Observe Data Privacy Month in 2018

1. Change your IU passphrase regularly and keep it confidential!
   Having a unique IU passphrase that is not used for any other service or website helps protect IU. In addition, never store your passphrase in memory. For more information, please see How do I change my IU Network ID passphrase?

2. Review your employee FERPA responsibilities here:
   https://ferpa.iu.edu/responsibilities/index.html. Remember casual access of student data for personal reasons or just out of curiosity is a violation. There is auditing of "high profile" records and accessing records without legitimate educational interest can result in termination of access or employment.

3. Dispose of restricted and critical data securely, and keep data only if it is a requirement. Records Retention Schedule:
   https://vpgc.iu.edu/about/guidelines/records-retention.html
   Clean up your email: Save only those emails you really need and unsubscribe to email you no longer need/want to receive.
   File upkeep: Delete or archive older files such as numerous drafts of the same document and outdated financial statements.
   Dispose of electronics securely: Wiping data isn't enough. When you dispose of old electronics, look for facilities that shred hard drives, disks and memory cards…
   Empty your trash or recycle bin on all devices: Make sure to permanently delete old files. Check out https://staysafeonline.org/stay-safe-online/ for more information.

4. Stay on alert for phishing scams. Always verify the sender before opening attachments or links embedded in an email. For more information:
   https://protect.iu.edu/online-safety/personal-preparedness/email-phishing.html

5. Stay secure online. Personal Identifiable Information (PII) must be protected.
   - **Passcode Protect Devices accessing IU data:** All mobile devices must be passcode protected and meet the standards outlined in IT- 12.1.
   - **Delete apps when done:** Some applications are installed on mobile devices for specific purposes like conferences or tours that collect personal information. It's good practice to delete all apps when no longer in use and be careful what information you agree to provide.
   - **Disable Wifi and Bluetooth** on mobile devices when not in use to avoid tracking by stores and other services.
   - **Use a VPN:** Public wireless networks and hotspots are not secure. For more information see: VPN at IU
   - **Use slashtmp for critical data to share sensitive information.** Do not send large datasets with student information through email (>100 students).