South Carolina

Privacy, Security and Practical Tips for those who are working remotely:

- Prevent inadvertent viewing and sharing of confidential information (such as protected health information (PHI), student or employee information, financial information, etc.); whether it's through the sharing of a personal computer/device or leaving confidential information out in plain view.
- Do not allow friends and family to use devices or applications that contain PHI or other confidential information.
- Keep your physical workspace secure; if possible, designate an area in your home as your workspace.
- Do not forward work e-mails to your personal e-mail. Likewise, do not send work-related emails from your personal email account.
- If you need to discuss PHI or confidential information over the phone, ensure that sensitive conversations cannot be overheard, or work observed by unauthorized persons.
- Take extra time to verify the identities of collaborators and students, particularly as you may be receiving calls from unfamiliar numbers. Verify and double-check identities, email addresses, or phone numbers prior to disclosing confidential or restricted information to anyone.
- Sign out of your computer and applications when you are not actively using them.
- Employees should avoid using or generating PHI or other confidential information in hard copy (paper) form in their home. If you have an unavoidable need to use or generate PHI or other confidential information in hard copy form in your home, then you need to have a lockable file cabinet to store the information when not in use.
- Any confidential information in hard copy form should be shredded when no longer in use. If you have an unavoidable need to use or generate PHI or other confidential information in hard copy form at home, then you need to have a shredder.
- Do not use email to convey highly sensitive confidential information. To discuss highly sensitive information, make sure it is de-identified and/or discuss it over the phone. If there is a need to include confidential information in any email being sent inside of UofSC, be sure to encrypt the email before sending by typing “encrypt” in the subject line.
- Do not save files or data locally on personal computers (such as laptops or desktops).

- Encrypt and secure your electronic devices (computers, laptops, portable drives, etc.).
- Laptops and flash drives that are not in use should be secured/locked away.
- Use of text messaging between mobile devices to discuss any PHI or confidential information is not permitted unless through a secure text platform.
- Opportunistic cyber attackers can take advantage of a crisis with phishing campaigns that target individuals. Do not lower your guard! Be vigilant with COVID-19-themed phishing lures, particularly with emails that contain attachments or links. Many actors are gaining the trust of victims by using branding associated with the CDC, the WHO, or companies, such as FedEx.
- If a laptop, device, or item that contains confidential information is lost or stolen, immediately contact your supervisor as well as the Office of General Counsel and Information Security Offices.