South Carolina Health Information Exchange
(SCHIEx)
Health IT Privacy and Security Resources and DIRECT Messaging Best Practices

The Office of the National Coordinator (ONC) in collaboration with Office of Civil Rights and other Health and Human Services agencies provides a comprehensive Health IT Privacy and Security information and resources for Health Providers at ***HealthIT.gov***. Below are links to just a few of the available resources and tools.

Health Information Privacy, Security, and Your EHR
http://www.healthit.gov/providers-professionals/ehr-privacy-security

CyberSecurity - Top 10 Tips for CyberSecurity in Health Care
https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

Health IT Privacy and Security Resources
http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources

Frequently Asked Questions
https://www.healthit.gov/topic/privacy-security-and-hipaa/frequently-asked-questions

In addition, a list of key security best practices related to DIRECT secure messaging is available on the following page. These best practices were shared by other ONC State Cooperative Agreement exchanges and adapted for use.

DIRECT Secure Messaging
Security Best Practices

The following provide best practices on user-controlled activities related to the use of the DIRECT secure messaging. These practices do not, in and of themselves, determine whether a user is fully compliant with HIPAA Security and Privacy requirements as defined in "Security Standards for the Protection of Electronic Protected Health Information (EPHI)" (45 CFR Part 164, Subpart C), commonly known as the Security Rule, and in "Privacy of Individually Identifiable Health Information" (45 CFR Part 164, Subpart E), commonly known as the Privacy Rule.

Keep your computer and devices which may contain PHI secure
When sharing information via DIRECT secure messaging, it is important to follow the same security guidelines currently used at your practice for computers containing PHI. Because files containing PHI might need to be stored in your computer before they are attached to a DIRECT message, it is important that the computer is protected (i.e., whole-disk encryption, not left unattended and unlocked, etc.). It is also important to lockdown and encrypt your wireless network. Users should follow internal policies and procedures related to the security requirements for media and devices which contain PHI and move beyond the organization's physical control. Such media and devices include laptops, hard drives, backup media, USB flash drives and any other data storage item which could potentially be removed from the organization's facilities.

Access and download PHI using a secured workstation computer
DIRECT is a secure messaging application; however it should not be accessed from non-secure devices such as public use workstations or home computers where security controls cannot be enforced. Public use workstations and other non-secure devices are those where general public access is allowed, or where technical security and physical security requirements cannot be applied and controlled. You should only download information from your DIRECT account to a secured computer.

Examine risks and implement protections if your organization allows access via Mobile Devices
Accessing DIRECT secure messages from mobile devices (laptops, smartphones, tablets, etc.) or is not prohibited; however, each subscriber organization and individual user should examine the risk associated with potentially having PHI located on these devices through sharing of patient data. The following protection mechanisms should be implemented to protect any PHI that is stored locally on a user device:

- Device password lock activated and used to gain local access to the given device,
- Virus and other malware protection, and
- File encryption and/or encryption of data at rest.

It is also strongly recommended that subscribing organizations include, but not be limited to, the following protection mechanisms for all devices used by their affiliated users:

- Establishing PHI deletion policies and media disposal procedures for mobile devices.
- Maintaining an accurate mobile device tracking and asset management program.
- Developing policies for the proper use or restriction of personal mobile devices for access to any PHI system.

<u>Email Confidentiality Notices</u>
Each subscriber has a responsibility to ensure the protection of patient data that is viewed or discussed via DIRECT messaging is consistent with the HIPAA Privacy Rule, including disclosures to unauthorized individuals. Each DIRECT user must ensure that communications involving patient data are between authorized individuals and that any authorizations or consents required by applicable law are obtained prior to disclosure. It is recommended DIRECT messages routinely contain a confidentiality statement such as: CONFIDENTIALITY NOTICE: This electronic email may contain information that is privileged, confidential, and/or otherwise protected from disclosure to anyone other than its intended recipient(s). Any dissemination or use of this electronic mail or its contents by persons other than the intended recipient(s) is strictly prohibited. If you have received this communication in error, please notify the sender immediately by reply email so that we may correct our internal records. Please then delete the original message.