Date: June 24, 2018
To: Duke Health Workforce Members and Affiliates
From: Duke Health Information Security Office (ISO)
Subject: Secure System Usage Memo

Attn: The links in this document are compatible with Internet Explorer and Safari. If you experience difficulties with a link, try using one of these browser or copying the hyperlink directly into your browser of choice.

Every member of the Duke Health workforce has a role to play in protecting the confidentiality, integrity, and availability of the valuable clinical and research data that Duke collects, produces, and maintains. The purpose of this memo is to provide you with an overview of the information security policies, standards, and procedures that apply to all Duke Health faculty, staff, students, and affiliates. Your commitment to following the steps outlined in this memo can help protect the personal information of our patients, their loved ones, and each other.

Sensitive Electronic Information

- Duke has established a three-tier Data Classification Standard to identify the security requirements for how data should be handled. The three tiers are Sensitive, Restricted, and Public.
- Sensitive Electronic Information, or SEI, refers to data that Duke must protect by law, or that Duke protects to reduce institutional risk. Some important examples of SEI include:
  - Protected Health Information, or PHI. Refer to the Uses and Disclosures of Protected Health Information Policy for more information on identifying and managing PHI.
  - Social Security Numbers, or SSNs, and other Personally Identifiable Information, or PII, as defined in North Carolina General Statute 14-113.20(b). Duke's Policy on SSN Usage defines our organization's requirements for limiting the use of and access to SSNs.
  - Student grades, evaluation forms and other records that must be protected according to the Federal Educational Rights and Privacy Act (FERPA).
  - Credit/debit card numbers, contracts, and other financial account information.
  - Unpublished research, manuscripts, and other intellectual property that should not be publicly disclosed.

Passwords

- Everyone using Duke Health IT resources must create and use passwords that comply with the Duke Health Password Standard.
- **Use Duke's Multi-Factor Authentication (MFA) to improve the security of your passwords**. Also known as two-step verification, MFA requires a user to log in using both a password and a randomly generated code. The codes can be generated by a special device or token or can be sent by text message or smartphone application. Find out more on the Multi-Factor Authentication web site.
- Passwords must be changed at a minimum of every 180 days.
- Your Duke passwords are never to be shared with another individual, including Service Desk staff and administrative assistants. Doing so is a breach of policy and can result in disciplinary action.
- Never use your Duke password on a non-Duke system (e.g. for personal email, banking, or social media site).
- Avoid writing your passwords on paper (e.g. sticky / Post-it notes) or other non-encrypted media. If you need assistance remembering and managing your passwords, Duke has licensed the LastPass utility, which can be used to generate strong passwords and store them in a secure fashion. For more information, see the LastPass FAQ.

Security Issues Related to Email and Web Browsing

- Phishing refers to the act of a malicious individual attempting to gain access to sensitive information, such as usernames and passwords, by impersonating a trustworthy party. Duke users frequently are targeted by phishing emails and phone calls. It is critical for everyone to be on the lookout for suspicious communications. For tips on

identifying potential phishing messages, visit https://security.duke.edu/phishing.

- **Think before you click on links and attachments in emails**. Inspect email addresses and web site URLs for contents that point to unfamiliar sites, and be suspicious of any that ask for your Duke NetID or password.
- Email attachments and downloaded files, particularly Office documents (Word, Excel, PDF, etc.), archive files (e.g. .zip, .rar, etc.), and executable files (e.g. .bin, .exe, .run, etc.) should be accessed with extreme caution.
- Never open an email attachment if you do not trust the source, or if you were not expecting the file.
- **Never** provide your password to anyone. If you receive a request to supply your password via email or phone, it should be considered fraudulent.

Protecting Workstations and Laptops

- Never uninstall or alter the configuration or operation of any systems management agent or anti-virus software that is installed on your Duke workstation or laptop.
- Discontinue use of any system that shows signs of being infected by a computer virus (also referred to as malware). See the "Recognizing and Reporting Security Incidents" section below for more information.
- Arrange computer monitors so that, as much as possible, they are facing only the individual using them. If available to you, consider the use of screen filters to limit visibility to those directly in front of the screen. You are responsible for ensuring that unauthorized individuals are not able to view your screen.
- Log off or lock your workstation or laptop if leaving the system unattended.
- Per Duke Health policy, all laptops must be fully encrypted using an ISO-approved solution, unless the Chief Information Security Officer (CISO) has granted an exception. Currently, Microsoft Bitlocker, Symantec PGP and Apple's FileVault 2 are the approved solutions. Contact your IT support group for assistance with encrypting a laptop.
- Ensure that laptops are stored in secure locations when unattended. If possible, **do not** leave them in a car, and if you must, place them in a locked hidden location, like a trunk.
- Provisions for installing hardware or software on workstations and laptops:
  - **If your workstation or laptop is used to conduct work under a Federal contract or Medicare Shared Savings Program (MSSP) which requires FISMA compliance**, you may not install software, hardware, or otherwise change the configuration of your workstation or laptop without explicit approval from your IT support group. **Failure to do so may place Duke out of compliance with federal contract requirements.**
  - For all other workstations and laptops, extreme caution should be used when installing any new hardware or software. It is recommended that you contact your local IT support group for assistance in making any hardware or software changes to your system.

Protecting Mobile Devices (Smartphones, Tablets, etc.)

- All devices, including those that are personally-owned, must be enrolled in the Duke Health Mobile Device Manager (MDM) program in order to access Duke Health services such as email, corporate WiFi network, and clinical applications such as Haiku/Canto. The Mobile Device Manager enforces a basic set of security controls that include the following:
  - Requiring the use of a lock, and passcode to unlock, the device when it is idle for more than three minutes. Numeric passcodes are the minimum requirement; alphanumeric are recommended.
  - Automatically wiping the device after ten successive failed attempts to use a passcode to unlock the device.
  - Encryption is enabled on the device and for any external storage cards (e.g. SD Cards) on Android devices.
- You are responsible for applying software updates to your device and any installed applications as soon as practical after being made available by the vendor.
- **Do not "jail break" or "root" your device.** Doing so disables basic security controls, and increases the chance of the device being compromised. Jailbroken/rooted devices will not be allowed to connect to Duke Health resources.

- Only install apps from legitimate sources, such as the Apple App Store or Google Play.
- If your device has been lost or stolen, please note that Duke Health reserves the right to remotely wipe all Duke data and applications from the device to prevent the loss of PHI. This should not affect personal data.
- For more information on the Duke Health Mobile Device Manager, including how to enroll a device, please see https://mobile.dhts.duke.edu/.

Protecting Data Storage, Transmission, and Backups

- With the exception of explicitly approved uses such as receiving Duke Health email on personal smartphone or tablet, do not store SEI on non-Duke systems or devices, such as flash drives or personal computers at home.
- PHI and other SEI that has been approved for storage on mobile devices or removable media (e.g. portable hard drives, memory sticks, flash drives, CD/DVDs, etc.) must be encrypted in accordance with the DM Mobile Computing and Storage Device Standard. Always ensure that mobile devices and removable media are stored in a secure (e.g. out of plain sight and locked) area when not in use.
- Duke's Box cloud-based file sharing service may be used to securely store and share files, including those containing PHI. Microsoft's OneDrive service, which is part of Duke's Office365 service, may be used to synchronize files between your mobile devices, but cannot be used to share files. Other cloud-based file storage and sharing services, including but not limited to Dropbox, Google Drive, and SugarSync, is strongly discouraged, **and must never be used to store PHI or other SEI.** A listing of Duke Services with Allowable Storage is available based on data classification.
- Clinical data may not be shared with vendors or other third parties who perform services on behalf of Duke unless there is a Business Associate Agreement (BAA) and Data Security Agreement (DSA) in place with the organization that would be receiving or accessing the data. If there are any questions about whether there is a BAA or DSA in place, you may contact Duke Procurement Services. BAAs and DSAs must be reviewed and approved through Procurement's processes, and may only be signed by Procurement. Duke Procurement Services and their assigns are the only parties authorized to sign contracts on behalf of Duke Health.
- Research data collected from Duke Health clinical activities under an IRB-approved protocol must be stored on Duke Health managed servers, not Duke University, VA or any other third party servers, unless (a) it has been fully de-identified or anonymized, (b) outlined in an informed consent, (c) under a Waiver of Consent and Authorization, (d) as a Limited Data Set with Data Use Agreement and/or (e) a Data Transfer Agreement has been put in place to allow the third party to receive that data. The Duke Health Institutional Review Board (IRB) and the Office of Research Contracts may consult on requirements.
- The Duke Protected Analytics Computing Environment (PACE) is a FISMA compliant, highly protected, virtual network space where users can analyze, store and work with consented, non-consented, QI, research, limited and identifiable protected health information. PACE is strongly preferred for research collaboration rather than sending clinical or research data to outside parties. If clinical data, research data, or other SEI is sent outside of the Duke Health network, SSL-encrypted protocols such as HTTPS or FTPS must always be used.
- User devices, including workstations, laptops, and other mobile devices, are generally not backed up. Any data stored on a user device may be permanently lost in case of a system failure or the loss of the device. Instead, store data on Duke Health servers or OneDrive through network shared drives.
- Dispose of all old storage media, including but not limited to hard drives and backup tapes in accordance with the Electronic Media Control Standard.
- External data recovery services (e.g. to recover data from failed hard drives) may not be used unless there is a BAA and DSA in place with the vendor.
- If you have any questions about how to securely store, manage, or transfer data, please contact the Duke Health ISO for assistance.

Securing Electronic Communications

- There is a strong preference for using Duke's Box (see above) cloud-based file sharing solution over email when possible. Email containing SEI that is sent outside of Duke Health must be sent using the Secure Email feature in

the Duke E-mail system by placing the text "(secure)" at the beginning of the Subject line of your email.

- Only use a Duke Health approved email system for Duke Health communications. Currently approved email systems include the Duke Health Exchange server and Duke's Microsoft Office 365 email solution. **Personal email accounts through services such Gmail, Yahoo, and Hotmail, or external sites that aggregate email accounts, may not be used to conduct Duke Health business.**
- Duke Health email containing PHI or SEI may not be forwarded to a non-Duke Health email account.
- The Duke Health Electronic Communications Policy provides further requirements for securing electronic communications, including faxing and text paging.
- The Duke Health Social Media Policy provides the policies and guidelines for the appropriate and secure use of social media sites such as Facebook, Twitter, and others. **PHI must never be posted on social media sites**, including online forums provided by Duke unless they have been specifically approved for PHI. Social media posts should always be presumed to be public.
- Extreme caution must be used with photography and videography inside of clinical facilities to prevent inadvertent disclosures of PHI. Please refer to the Photographing/Videotaping/Audiotaping of Patients policy.

Prohibited Software

- Peer-to-peer file sharing and installation of P2P programs, such as but not limited to BitTorrent, are prohibited.
- Use of software that permits a Duke computer to be remotely controlled, such as LogMeIn, TeamViewer, and BackToMyMac, must be approved by the Duke Health Information Security Office.
- The use of hacking tools, such as network sniffers, password crackers, and vulnerability scanners is prohibited unless the Duke Health Chief Information Security Officer has approved the usage for specific, legitimate purposes.

Physical Security

- Retrieve printed sensitive information immediately upon printing. When disposing of hardcopy, use bins that have been marked for the disposal of confidential documents. If those are not available, use a crosscut shredder.
- Report unauthorized or unknown people that appear in non-public areas to a manager or facilities security officer.
- In areas that require badge access, do not allow others to follow you through a door without badging in.

Recognizing and Reporting Security Incidents

- A security incident is an event that may result in the confidentiality, integrity, or availability of Duke Health information systems or data being compromised. Indications of a security incident may include the following:
  - The intentional or unintentional misuse of (a) patient information, (b) information pertaining to Duke Health faculty, faculty, or students, (c) Duke Health computer systems, or (d) other information that is classified as sensitive or restricted by Duke's Data Classification Standard.
  - Theft or loss of a computer or mobile device (e.g. smartphone or tablet) that is either owned by Duke or possibly stored or had access to Duke Health patient information or other sensitive data.
  - Unplanned disruption or denial of service.
  - Observing odd behavior or other signs that a computer may have been infected with malware or otherwise compromised by an intruder.
  - Clicking on a link or opening an attachment in a suspicious email.
  - Finding evidence that a Duke Health system, application, or data set may have been modified or accessed without authorization.
  - Storing patient information or other sensitive data in an insecure manner on a workstation, computer media (e.g. flash drive or CD/DVD), or unauthorized web site (e.g. file sharing sites such as DropBox).
  - Leaving printed output containing patient information or other sensitive data in a location where unauthorized individuals may view it.

- If you suspect someone knows your password, your last date and time noted on the login screen is not correct, or your account has been locked out.
- Faxing, mailing, or emailing patient information or other sensitive data to an incorrect phone number or address.

- If you believe that you have observed an information security incident, please take the following steps:
  - **Report the incident immediately** to the Duke Health Service Desk by calling 919-684-2243 or online at https://security.duke.edu/get-help.
  - **If the incident involves your computer:** Discontinue using it until the Duke Health Information Security Office has evaluated the situation.
  - **If the incident involves the loss or theft of a computer or mobile device:** In addition to reporting the incident to the Duke Health Service Desk, file a report with the Duke University Police Department, which can be reached at 919-684-2444.

For More Information

The Duke Health and Duke University Security Office website provides additional information and advice on our security policies, standards, guidelines, and alerts.

If you have any additional information security questions or concerns that you would like to discuss, you can contact the ISO via email at infosec@dm.duke.edu.

Contact Information:

- Duke Health Information Security Office (DHTS): Email - infosec@dm.duke.edu
- Duke University IT Security Office (OIT): Email - security@duke.edu
- Duke Health Service Desk: Phone - 919-684-2243; Web - https://duke.service-now.com
- Duke University Police Department: Phone - 919-684-2444