Date: March 6, 2014
To: Duke Medicine Workforce Members and Affiliates
From: Duke Medicine Information Security Office (ISO)
Subject: Secure System Usage Memo

Every member of the Duke Medicine 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 Medicine 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 and the HIPAA FAQs for more information on identifying and managing PHI.
  - Social Security Numbers, or SSNs. Duke's Policy on SSN Usage defines our organization's requirements for limiting the use of and access to SSNs.
  - Credit/debit card numbers and other financial account information.
  - Student information, as defined by the Federal Educational Rights and Privacy Act (FERPA).
  - Other Personally Identifiable Information, or PII, as defined in North Carolina General Statute 14-113.20(b).

Passwords

- Strong passwords must be used to secure access to critical systems and data. A single compromised password can lead to a significant data breach. Duke Medicine relies upon you to protect your passwords at all times.
- Everyone using Duke Medicine IT resources must create and use passwords that comply with the Duke Medicine Password Standard.
- Passwords must be changed at a minimum of every 180 days. You should receive automated reminders several days prior to your password's expiration.
- 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). 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 http://security.duke.edu/internet-safety/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. Contact the Duke Medicine Service Desk at 919-684-2243 to report any suspicious behavior.
- **Never** provide your password to anyone. If you receive a request to supply your password via email or phone, it should be considered fraudulent and reported to the Duke Medicine Service Desk at 919-684-2243.

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. Screen locks should be configured to automatically lock a screen after a maximum of 15 minutes, and requiring that your password be entered to unlock the screen.
- Per Duke Medicine policy, all laptops must be fully encrypted using an ISO-approved solution, unless the Chief Information Security Officer (CISO) has granted an exception. Currently, Symantec PGP and Apple's FileVault 2 are the two 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, never 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.)

- When connecting your mobile device to Duke Medicine's email system, a basic set of security controls will be enforced on your device. These include the following:
  - Requiring the use of a passcode to lock the device when it is idle for more than three minutes. Numeric passcodes are the minimum requirement; alphanumeric are recommended. A password history is maintained to prevent the successive re-use of passcodes.
  - 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 on the device, and increases the chance of a malware infection.
- 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 Medicine reserves the right to remotely wipe the device to prevent the loss of PHI.

Protecting Data Storage, Transmission, and Backups

- Except for explicitly approved uses such as receiving Duke Medicine email on personal smartphone or tablet, do not store Duke SEI on non-Duke owned systems or devices, such as 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.
- Use of file sharing or cloud-based services for data containing SEI (e.g. Dropbox, SkyDrive, Google Drive, etc.) is not allowed without prior approval from the Duke Medicine ISO. Duke is working to provide an alternative solution for this type of service, and it will be announced when available.
- 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 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.
- Research data collected from Duke Medicine clinical activities under an IRB-approved protocol must be stored on Duke Medicine 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, or (c) a Data Transfer Agreement has been put in place to allow the third party to receive that data.
- When sending clinical data, research data, or other SEI outside of the Duke Medicine network, SSL-encrypted protocols such as HTTPS, SFTP, or SCP 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 Medicine servers through network shared drives.
- Dispose of all old storage media, including but not limited to hard drives and backup tapes in accordance with the DM 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 in place with the vendor.
- If you have any questions about how to securely store, manage, or transfer data, please contact your IT support group or the Duke Medicine ISO for assistance.

Securing Electronic Communications

- Email containing SEI that is sent outside of Duke Medicine must be sent using the Secure Email feature in the Duke E-mail system. This may be done using the "Sensitive Electronic Information" button in Outlook, or if that is not available in your email client, by placing the text "(secure)" at the beginning of the Subject line of your email. For more information on using Secure Email, see the Secure Outgoing Messages FAQ.
- Only use a Duke Medicine approved email system for Duke Medicine communications. Currently approved email systems include the Duke Medicine 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 Medicine business.**
- Duke Medicine email containing PHI or SEI may not be forwarded to a non-Duke Medicine email account.
- The Duke Medicine Electronic Communications Policy provides further requirements for securing electronic communications, including faxing and text paging.
- The Duke Medicine 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.
- 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.

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 Medicine 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 Medicine faculty, faculty, or students, (c) Duke Medicine 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 Medicine patient information or other sensitive data.
  - 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 Medicine 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 Medicine Service Desk by calling 919-684-2243 or online at https://duke.service-now.com.
  - **If the incident involves your computer:** Discontinue using it until the Duke Medicine 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 Medicine Service Desk, file a report with the Duke University Police Department, which can be reached at 919-684-2444. For further information, refer to the Lost or Stolen Device Procedure.

For More Information

The Duke Medicine ISO intranet site provides additional information and advice on our security policies, standards, guidelines, and alerts. You can find the ISO site at Duke Health Information Security Office Intranet Site

A complete list of our information security policies can be found at Duke Health Information Security Policies

A complete list of our information security standards can found at Duke Health Information Security Standards

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.

Reference Links

1. Data Transfer Agreements
2. Duke Data Classification Standard
3. Duke Health Electronic Communications Policy
4. Duke Health Information Security Office Intranet Site
5. Duke Health Information Security Policies
6. Duke Health Information Security Standards
7. Duke Health Lost or Stolen Device Procedure
8. Duke Health Media Control Standard
9. Duke Health Mobile Computing and Device Storage Standard
10. Duke Health Photographing/Videotaping/Audiotaping Policy
11. Duke Health Social Media Policy
12. Duke Health Password Standard
13. Duke Social Security Number Usage Policy
14. Duke Health Uses and Disclosures of Protected Health Information Policy
15. Duke Medicine Secure Email
16. The Family Educational Rights and Privacy Act (FERPA)
17. HIPAA FAQs
18. LastPass FAQ
19. Phishing Alerts
20. State of North Carolina General Statute 14-113.20 (definition of Identity Theft)

Contact Information

Duke Medicine Information Security Office (DHTS): Email - infosec@dm.duke.edu

Duke University IT Security Office (OIT): Email - security@duke.edu

Duke Medicine Service Desk: Phone - 919-684-2243; Web - https://duke.service-now.com

Duke University Police Department: Phone - 919-684-2444