DUKE UNIVERSITY HEALTH SYSTEM

Memorandum

To: All Users of Computing Equipment and Network Resources

From:

Re: Secure System Usage

Computer system security is everyone's responsibility. The information provided in this memo should be followed while using computer systems within the Duke University Health System (DUHS).

Passwords

Passwords are an important aspect of computer security. Misuse of a password can compromise sensitive data as well as the enterprise-wide network itself. All DUHS employees (full time, part time, and temporary) and non-employees (physicians, students, vendors, consultants, contractors, etc.) who obtain permission to access and / or utilize DUHS computing resources must create and use passwords that comply with the Duke Medicine Password Standard. Each individual is responsible for taking the appropriate steps, as identified below, to select and secure their password(s).

- An individual password is required to access computer system(s). The password is not to be shared with anyone.
- A shared password is considered to be a compromised password and must be changed immediately and reported to your supervisor or DHTS.
- Technical support staff does not need your password to troubleshoot your system. If you are approached by anyone claiming to need your password, contact DHTS immediately.
- Guard your password from shoulder surfers.
- Observe whether the date and time of the last login reported is reasonable when you login to a system that provides this information.

Only strong passwords are permitted. Please follow the criteria listed below:

- The minimum length for passwords is eight characters.
- The password must contain at least one capital letter, one lower case letter and one number.
- The password may not contain personal information (like your name) and is not a word in the dictionary.
- The password must be changed at least every 180 days or when it is believed or known to have been compromised, whichever comes first.
- The password may not be re-used within a 3 year time span.

DO NOT:

- Share your passwords with anyone, including administrative assistants, managers or I.T. staff.
- Use anyone else's user ID or password to access any DUHS system.
- Say a password in front of others or write a work related password down.
- Reveal a password on questionnaires or security forms.
- Use a Help Desk/initial system password more than once before changing it.
- Store passwords on any computer system (including on a Personal Digital Assistant/Smart Phone).
- Use the same ID and password for DRH work related accounts as for non-work related accounts (examples: personal Internet Service Provider accounts, bank accounts, on-line website accounts, etc.) Instructions for changing passwords on most common DUHS systems are available on the http://intranet.dukemedicine.org Web site under the DHTS tab. If you need assistance resetting your password, contact the DHTS Help Desk.

Workstation, Mobile Devices and Removable Storage Media Use

It is your responsibility to:

- Arrange computer monitors so that, as much as possible, they are facing only the individual using them.
- Retrieve printed sensitive information immediately upon printing and dispose of in confidential bins after use.
- Exit all programs and log off of the workstation or lock the workstation, (Alt+Ctrl+Delete and select 'Lock Workstation'), prior to leaving the workstation unattended.
- Ensure that any mobile device, (laptop computer, PDA, Smart Phone, etc.) is returned to a physically secure environment when not in use.
- Ensure that any mobile device or removable media (CD, memory stick, etc.) containing sensitive information is password protected and stores data in encrypted form.
- All Duke laptop computers must be encrypted in compliance with the Duke Medicine Mobile Computing Standard.
- Report any theft/destruction of computer equipment immediately to your Department Manager, the Information Security Office, as well as the DHTS Help Desk.
- Sensitive Electronic Information, SEI, including patient information, should not be stored on a local workstation, laptop computer or removable media.

Data Backups. Storing Sensitive Data such as Protected Health Information

Data backups are performed on all DUHS servers. User devices including workstations, laptop computers, Smart Phones and PDA's are not backed up, unless done so by the individual user. Sensitive or confidential data, including patient information, should not be stored on the hard drive of these devices. Always save your work to a network drive.

Stand Alone Media Disposal

Stand Alone media are any media that are not integrated into equipment. Examples include: CDs, Tapes, USB or flash drives, and Zip Drives. If you need to dispose of any stand alone media you

must deliver the media to the Information Systems department or contact Information Systems and arrange for pickup. Information Systems disposes of media in compliance with the Duke Medicine Media Disposal Standard.

Encryption

No form of data containing Sensitive Electronic Information, SEI, including confidential or protected health information from any computer system will be sent outside of the Duke protected network without encryption. Any SEI stored on portable or mobile devices must be encrypted. If you have questions about encryption, contact the Information Systems department for more information.

E-mail

E-mail containing SEI that is sent outside of Duke must be sent using the Secure Mail feature in the Duke E-mail system. Electronic mail may not be automatically forwarded outside of Duke Medicine.

Security Incidents

Examples of a security incident include but are not limited to:

- Misuse of DRH/Duke proprietary information
- Misuse of patient information
- Misuse of information pertaining to DRH or Duke community members or staff members
- Unauthorized use of DRH/Duke systems in ways that compromise system availability, performance, or integrity
- If you suspect someone knows your password, your last date and time noted on the login screen is not correct or your password has been locked
- You find sensitive data on a workstation, other computer media or unsecured printed reports

If you observe a Security Incident, contact your manager and the Information Systems department immediately.