

JOHNS HOPKINS HIPAA SECURITY AWARENESS

Introduction to Information Security

Johns Hopkins processes a lot of information. Most of what we do—whether in education, patient care, benefit administration or research and operations—demands that we protect sensitive information throughout various systems. We need that information to be accurate and on hand, and we must be able to trust that it will be used only by those who need it.

Since we use computers in our daily work duties, we should follow the best computer security practices. Our use of computers must be:

- Legal and ethical
- Considerate of others
- Proper in order to limit security problems

HIPAA

The Health Insurance Portability and Accountability Act is referred to as “HIPAA”. The HIPAA privacy regulations protect individually identifiable patient and health plan member information, no matter what form it is in—paper, oral, or electronic. This information is called Protected Health Information or PHI. The HIPAA security regulations cover only electronic forms of this information called Electronic Protected Health Information or E-PHI. The HIPAA security regulations are enforceable as of April 20, 2005. How you use your computer can impact the security and privacy of patient and plan member information.

To protect E-PHI, follow these steps:

- Avoid disclosing unencrypted E-PHI in e-mails and shared files over the Internet.
- Avoid saving E-PHI to your computer hard drive. Save files on a Johns Hopkins server.
- Never share your login with another user.
- Never store E-PHI on a handheld device that lacks strong security controls.
- Use only the E-PHI needed to do your job.
- Log off or lock your computer when you are not using it.
- Report computer security problems quickly.

Many computer systems track your actions. Be aware that inappropriate actions on computers can cause damage, and that such actions may be traced to a specific user.

Authorization to Use E-PHI

To do your job, you may be given access to some computer applications with E-PHI. But first, the security administrator of the computer applications must get authorization from your management. Also, you may have to go to computer training and sign a confidentiality agreement before access is given.

If you change jobs within Johns Hopkins, your computer access may change. You may be given access to other computer applications, and/or your existing access may be increased, reduced or removed.

User IDs and Passwords

Computer applications ask you to prove who you are before giving access. Proving who you are before you can do something is called “authentication.” For most computer applications, authentication consists of a user ID (for example, jsmith1) and a password. Good passwords can be effective security controls when you follow these steps:

- Make passwords that are at least eight (8) characters long.
- Make your passwords hard to guess. Use a mix of letters, numbers and special characters (!@#%).
- Do **not** use names or other words found in a dictionary as your password.
- Adding a number at the beginning or end of a word does not make it a hard to guess password.
- Try using the first letters of a phrase that you will not forget and put in some special characters and numbers (e.g., Four Score and Seven Years Ago can become FS^a7YA).
- Do **not** write down your password in your work area.
- Do **not** share your password with anyone other than your computer or LAN administrator to fix or maintain your computer.
- Change your password at least every 90-180 days.
- Avoid re-using old passwords.
- Change your password if you think someone knows your password or has used it. Also, tell your LAN administrator or Help Desk.

Preventing Viruses

Computer viruses are designed to damage or destroy a computer, even without you knowing it. It is standard practice to use and maintain anti-virus software on your computer. Follow these steps to help limit viruses:

- Make sure anti-virus software is on your computer. Use the software and update it often.
- Your computer should protect against new viruses or tell you when updates are available. Every Johns Hopkins user can get this software at <http://www.jhu.edu/anti-virus/>.
- Question all e-mail attachments. The attachments ending in *.doc* and *.xls* (Microsoft Word or Excel documents) are mostly safe, but virus writers may trick users by using them.
- Do **not** open any e-mail attachments with extensions of *.exe*, *.vbs*, *.js*, *.hta*, *.pif* and *.shs* unless you know the sender and the contents of the file.
- Do **not** assume that all e-mails and attachments are virus free, even if the e-mail appears to come from someone you know.
- Be careful downloading programs from the Internet and ask your LAN administrator if you have questions.

Reporting Incidents

Even with good security habits, there will be incidents from time to time that need a response. An incident could be:

- Unauthorized access to gain the ability to monitor computer activity
- Unauthorized access to steal or alter data
- Tampering with or destroying a computer, handheld device or server
- A computer virus
- Belief that someone used your account when you were not using it (for example, when on vacation)

Incident reporting is important. You should watch for unusual activity and tell your LAN administrator or HELP Desk.

What You Can Do

You need to be aware of how you use computers. You need to think of how your actions might create a security issue. Report incidents and unusual activity. And, if you are not sure of what to do, always ask your LAN administrator.

JOHNS HOPKINS COMPUTER SECURITY TIPS

www.insidehopkinsmedicine.org/hipaa

- * Keep your user ID and password to yourself.
- * Make your password hard to guess and change it frequently.
- * Use only the computer systems, programs and files you are authorized and required to access to perform your job.
- * Avoid sending protected health information (PHI) in e-mails over the Internet.
- * Save PHI only to a secure network, not to your local PC drive or portable device.
- * Beware of downloading or opening software, documents or e-mail attachments from unknown, untrustworthy sources.
- * Log off or lock your computer when not in use.
- * Seek approval from your systems administrator before installing computer programs.
- * Use and update antivirus software regularly.
- * Report all security incidents to your Help Desk or LAN administrator.