Practical Tips on Good Password Practices for Workforce Members

2017

STOP | THINK CONNECT™

When it comes to safeguarding information, your patients and coworkers trust you to protect it. Safeguarding information is our shared responsibility. You can do your part by taking certain precautions by using these ***STOP.THINK.CONNECT.***™ *tips, developed by the Healthcare Information and Management Systems Society North America. HIMSS is a strong supporter of the National Cyber Security Alliance's* ***STOP.THINK.CONNECT.***™ *campaign which is the global online safety education and awareness campaign.*

STOP: *Take security precautions.* ***THINK:*** *Understand the consequences of your actions and behaviors to help safeguard information.* ***CONNECT:*** *Enjoy the benefits of the Internet, computers, and Internet-connected devices in healthcare.*

WORLD PASSWORD DAY2017

WHAT IS THE PURPOSE OF A STRONG PASSWORD?

- Protect the information and systems to which you have been granted access
- Allow authorized users in, keep unauthorized users out
- Prevent someone else from accessing systems and potentially modifying information under your own name and account
- Make the password difficult to be guessed or determined by brute force

WHAT ARE GOOD PASSWORD HABITS?

- Always follow your organization's policies first
- Do not reuse old passwords
- Never use passwords that contain your username or easy to identify personal information
- Avoid using the same or similar passwords on different systems
- Do not use the same or similar password for personal and work related accounts
- Avoid writing down passwords, especially if left in the open
- Never share your password with others
- Use complex passwords by combining uppercase and lowercase letters, symbols and numbers
- Never use dictionary words in a password
- Use longer passwords or passphrases
- Use a password which is easy for you to remember, but impossible for others to guess
- Change your password regularly

WHAT IS MULTI-FACTOR AUTHENTICATION?

When two or more factors are used to prove that you are who you say you are:

- » *Something you know*
- » *Something you have*
- » *Something you are*

It provides an additional layer of protection, in addition to username and password

- » ***Example #1:*** *One-time passcode generator + username-password combination*
- » ***Example #2:*** *Fingerprint scan + username-password combination*

WHAT ARE THE BENEFITS OF MULTI-FACTOR AUTHENTICATION?

- Greater assurance that the user is who he or she claims to be
- Reduces the possibility of unauthorized access

For additional information about keeping protected health information private and secure, please review the HIMSS privacy and security toolkits at: www.himss.org/library/healthcare-privacy-security. For more online safety tips, visit www.stopthinkconnect.org.

HIMSS transforming health through IT™

NATIONAL CYBERSECURITY ALLIANCE