SANS Securing The Human

Protecting Healthcare Data

1. What Healthcare Data Is Targeted?

Protected Health Information: This is information which relates to the physical or mental health condition, payment or provision of healthcare that can be associated with an individual.

Financial Information: This is financial or monetary information associated with an individual. This could include their bank account or credit card.

Intellectual Property: This is information such as patentable inventions, trade secrets and copyrighted works. This can include medical research, software we have created, medical device innovation and even confidential know-how about our healthcare operations.

Cyber Security Awareness Poster Series

This series of posters is designed to help people create a more cyber secure home and enable healthcare organizations to better protect their confidential and sensitive information. For more information and resources to help protect yourself, your family and your healthcare organization, please visit:

www.securingthehuman.org

Winter 2015 | 34th Edition

2. Why We Protect Healthcare Data

Healthcare organizations are responsible for protecting people's most private and personal healthcare information. Unlike credit card numbers or online accounts, private records about a person can never be replaced after a breach. Out of respect and dignity for the patients we care for, it is critical that we protect their data.

In addition, as a result of the HIPAA Privacy and Security Rules and the HITECH Act, we are required by federal law to safeguard healthcare data. Fortunately, there are easy, practical steps you can take to help protect this valuable information.

3. Where Is Healthcare Data Located?

Healthcare data can reside in places you might least expect. As such, it is critical you protect any devices and media you are using for work. In addition, be sure you do not forget or lose them. Finally, before you reuse or dispose of these devices and media, make sure you follow our procedures for secure destruction of the data.

- Desktop and Laptop Computers
- Smartphones and Tablets
- External or Portable Hard Drives
- USB Flash Drives and SD Memory Cards
- DVDs and CD-ROMs
- Biomedical Devices
- Printers, Copiers and Fax Machines

4. Top Tips for Securing Healthcare Data

Passwords: Use a strong, unique password or passcode to protect mobile devices, laptops or computers. Whenever possible, use two-step verification. Never share your passwords with anyone, including a supervisor, coworker or the help desk.

Control: Keep healthcare data in your personal control at all times and locked inside cabinets or drawers when not in use. Never leave healthcare data unattended, such as in a vehicle. Never take any healthcare data out of our facility, whether in electronic, paper or other form, unless you have prior authorization.

Encryption: Healthcare data should be encrypted whenever you are storing or transmitting it. For example, when accessing healthcare data online, make sure your browser's connection is encrypted. Check to confirm the website starts with HTTPS and there is a closed padlock next to it.

Sharing: Never share any healthcare data through social media or text messaging. In addition, you must have prior authorization to use Cloud services, such as Dropbox or Google Docs.

Policies: Be sure you understand and follow our policies on how we protect healthcare data. If you have any questions on how to handle healthcare data, ask your help desk, information security team or supervisor.

About the Poster

This poster was developed as a community project by the following healthcare information security professionals:

Lee Kim, HIMSS - Nassar Nizami, Yale New Haven Health System - Michael Cecil, Tucson Medical Center - Jennifer Gilreath, HealthPartners - Kelli Tarala, Enclave Security - James Tarala, Enclave Security - Roberto Rodriguez, MySherpa - Barbara Filkins, skWorks

For digital copies of this and other security awareness posters, visit www.securingthehuman.org/resources/posters