CYBERSECURITY for HEALTHCARE PROVIDERS

This publication contains information on cybersecurity awareness and advice on how to mitigate cyber threats for healthcare providers. Hospitals and healthcare providers are frequently targeted by cyber criminal hackers because of the value of stolen health care information. The Northern California Regional Intelligence Center's (NCRIC) Cyber Unit encourages its Partners in the healthcare community to review this information and their organization's policies.

HIPAA and Cybersecurity

When it comes to protecting personal information, healthcare professionals have additional legal responsibilities to consider. The Security Rule of the Health Insurance Portability and Accountability Act of 1995 (HIPAA) established a national set of security standards for protecting individually identifiable health information that is held or transferred in electronic form (e-PHI). Covered entities are required to maintain reasonable and appropriate administrative, technical, and physical safeguards in protecting e-PHI. As an end-user with access to sensitive e-PHI, you play a significant role in protecting this information. Review your organizations security policies, maintain good cyber hygiene, and report any possible disclosure or compromise of your systems as soon as possible.

General Cyber Hygiene Tips

Individual users can take some basic steps to improve their cyber hygiene. Although this will not protect them from all cyber attacks, it will make them a harder target.

- Create strong passwords of at least 12 characters that includes numbers, letters and special characters. Think of a passphrase instead of a simple word.
- Use unique passwords for every site or database. The compromise of one set of credentials should not compromise all of your accounts.
- Go beyond passwords by using Two-Factor Authentication when available.
- Do not click on links or open attachments from unknown senders and verify that known senders are who they say they are (see Social Engineering) .
- Do not browse to or type any sensitive information when connected to public or open WI-FI access points.
- Do not use personal devices or email to send or access e-PHI or other sensitive data as these methods may not have adequate encryption (HIPAA).
- Only access e-PHI from you own account. Accessing someone else's account is prohibited by HIPAA guidelines.

Social Engineering

Social engineering is the use of deception to manipulate people into providing sensitive information or to do things they may not otherwise do.

- Phishing emails: Emails designed to get the user to click on malicious links or to provide confidential information such as your password. May appear to come from a known individual or trusted organization.
- Smishing texts: SMS or text messages attempting to get recipients to click on links or to respond with personal information.
- Vishing: Phone calls used to solicit information on organization practices or to gain personal information.

Malicious actors may use information from public sources, including information you post on your social media accounts to better craft their attempts to solicit information.

Think before you click and verify before you provide passwords or other personal information.

CYBERSECURITY for HEALTHCARE PROVIDERS—Continued

How Do I know If I've Been Hacked?

Often, individual end-users may be unaware that their systems have been hacked until their IT administrator alerts them to abnormal activity. There are, however, some signs that may signal that you have been hacked:

- Frequent and random popups
- New toolbars or programs installed on your computer
- Email contacts receiving fake emails from your account
- Passwords to databases and online accounts being changed without your knowledge
- Being redirected to unknown websites
- Computer runs slower than usual
- Warning popups appearing saying your files are locked
- Your mouse moves automatically
- Unexplained withdraws or activity on your personal banking or credit cards.

Who Do I Report to if I think I've been Hacked?

- Report any suspected compromise to systems or healthcare information **IMMEDIATELY** according to your organization's policies. This may include reporting directly to the IT administrator, calling a helpdesk, or notifying your supervisor. Provide as much information as possible.
- Law enforcement, such as local police or the FBI, can be contacted directly or a report can be made on the Internet Crime Complaint Center website IC3.gov. After reviewing the complaint, the Center will forward the complaints to the appropriate law enforcement agency.
- Suspicious cyber activity can also be reported to the NCRIC Cyber unit. The NCRIC can provide information on current cyber threats, provide cyber mitigation strategies, and coordinate the notification of cyber incidents to the relevant law enforcement agencies.

Organization Policies

Review your organization's IT policies and guidelines regularly as they may change. These policies and guidelines will most likely explain acceptable use of equipment and resources, credential or password expectations, and the use of external devices.

RESOURCES

IC3.org-Internet Crime Complaint Center, established by the FBI. Visitors to the site can report suspected Internet crimes and get information on current scams.

HealthIT.gov—Office of the National Coordinator for Health Information Technology (ONC) website that provides information for healthcare professionals, patients, and researchers regarding information safety and privacy.

Stopthinkconnect.org— Stop.Think.Connect is an online safety awareness campaign that provides tips and advice for all end-users.

StaySafeOnline.org—Associated with the Stop.Think.Connect campaign, this site provides additional resources on protecting personal information and keeping devices clean.

NCRIC Cyber UNIT

NCRIC Partners can submit suspicious cyber activity as a Suspicious Activity Report (SAR) on the **NCRIC.org** website or directly to the Cyber Unit at **cyber@ncric.ca.gov**.