Nurses Service Organization
Healthcare Providers Service Organization

RISK ADVISOR

FOR HEALTHCARE BUSINESS OWNERS

Healthcare Spotlight: Cyber threats likely to increase during coronavirus pandemic

Cybercriminals are attempting to prey on the fear and confusion caused by the coronavirus to target the healthcare sector and average Americans. The FBI and the Department of Homeland Security have issued alerts for both consumers and healthcare providers warning Americans to be alert to these phishing emails. “Scammers are leveraging the COVID-19 pandemic to steal your money, your personal information, or both,” the FBI stated in the alert. In a recent press release, the FBI warned that healthcare professionals are at an increased risk of receiving fraudulent telephone calls and emails related to COVID-19.

Suffering a ransomware attack can disrupt operations. Even sophisticated hackers have been using pandemic-related traps to spread their malware. These conditions are ripe for various types of cyberattacks, and healthcare providers and businesses should be aware of the risks.

Ransomware attacks on healthcare businesses are common because scammers hope that the urgent need to function will motivate employers and administrators to simply pay the ransom. Such attacks always pose a potential threat to the health and safety of patients. They are especially reprehensible during a pandemic that is straining the world's health care systems.

The potential consequences of a data breach range from sizeable monetary penalties (which are not necessarily covered by professional, property or general liability insurance policies) to negative publicity, disruption of routine, loss of public trust and possible patient harm, if medical data integrity is compromised. Both healthcare employers and employees must exercise the utmost care to protect themselves as well as confidential patient/client information. Here are some issues for employers and employees to understand in order to minimize the risk during this public health emergency.

WHAT ARE THE MOST FREQUENT CAUSES OF DATA BREACHES?

The HHS Office for Civil Rights categorizes data breaches into five groups, listed in declining order of frequency:

- Theft of paper records or electronic media, including computers and portable devices such as USB flash drives and smartphones.
- Loss of paper or electronic records, including laptops and data storage devices.
- Unauthorized access to protected health information (PHI), including external hacking, "malware" infection and illicit employee-related exposures.
- Human or technological miscues, including erroneous mailings and email or network server glitches.
- Improper disposal of paper records, generally involving errors made by a billing service or other vendor.

Approximately 20 percent of the reported incidents, comprising more than half of the total records disclosed, involve outside contractors hired by the covered entity. Loss or theft of unsecured data represents approximately 55 percent of breaches, compared with only 7 percent caused by hacker infiltration.

WHERE SHOULD I START TO ENHANCE DATA SECURITY AND IDENTIFY SYSTEM VULNERABILITIES?

The following basic measures constitute a useful starting point for organizational discussion of data breach prevention and response:

- ***Perform a cyber-risk assessment/Protected Health Information inventory.*** The critical first step in enhancing data security is to identify system vulnerabilities and account for how protected health information (PHI) is managed and secured within the organization. A variety of programs are available to assist in this task, including the Department of Homeland Security's Cyber Security Evaluation Tool (CSET®) and the OCTAVE® information security assessment approach. The Office of the National Coordinator for Health Information Technology (ONC) and HHS Office for Civil Rights (OCR) also provide a complimentary security risk assessment tool to help healthcare providers comply with the HIPAA Security Rule.
- ***Educate staff regarding the scope of federal and state privacy and notification requirements.*** Basic HIPAA regulations should be integrated into employee orientation and training. Training sessions should explain the causes of data breaches and describe the consequences of neglecting to observe established data security policies, such as:
    - Disclosing PHI to anyone outside the organization who does not have a right to know.

    - Removing PHI from the facility without permission.
    - Failing to log out when leaving a workstation.
    - Leaving confidential information displayed on a screen.
    - Sharing or writing down passwords.
    - Keeping laptops or storage devices in an unlocked vehicle or otherwise exposing them to theft.
- ***Safeguard record storage space.*** To reduce the possibility of theft or sabotage, periodically reevaluate and, if necessary, revise security measures for restricted areas.
- ***Implement a user monitoring system and effective access controls.*** The HIPAA Security Rule requires that IT systems log user access to PHI. These user logs should be carefully monitored. In addition, accounts should have suitably complex, unique, regularly changed passwords and should lock automatically after a designated number of unsuccessful log-ins.
- ***Examine agreements with business associates regarding data sharing and security.*** Contracts should expressly address PHI confidentiality issues in accordance with federal regulatory guidelines, and language should be reviewed and approved by legal counsel and IT specialists. Data shared with vendors and other business associates should follow the "minimum necessary" standard, as required by the HIPAA Privacy Rule.
- ***Adopt encryption technology, which renders protected information unreadable and unusable in the event of a security breach.*** Undecipherable information is not subject to HITECH reporting requirements. Though encrypted information could be compromised, its use greatly enhances privacy protection of PHI and financial data.
- ***Institute a post-breach response plan.*** In addition to complying with state and federal notification requirements, the plan should provide affected individuals with credit and medical identity monitoring services. For ethical and reputational reasons, it is generally advisable to inform all affected parties of a data breach, even if such notification is not required by law.
- ***Obtain adequate cyber liability insurance to address data and privacy-related coverage gaps.*** Such specialized products can provide coverage for third-party liability (e.g., certain fines, indemnity payments and associated legal expenses), as well as for certain reimbursement costs and first-party losses (e.g., notification costs, system restoration expenses and credit monitoring for affected parties, if warranted), as set forth in the policy.

In an age of electronic health records, stringent privacy regulations, and widespread concern about identity theft and Medicare fraud, information security has become a major risk management priority. Leaders of every type of healthcare entity should evaluate their overall cyber exposure, create a plan to

secure confidential information and minimize the impact of a potential breach, and obtain appropriate insurance coverage.

WHAT CORRECTIVE ACTIONS SHOULD I TAKE FOLLOWING A HEALTHCARE-RELATED DATA BREACH?

Inappropriate disclosures involving the medical and/or personal data are reported to the U.S. Department of Health and Human Services (HHS) in compliance with the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was enacted in 2009 as part of the American Recovery and Reinvestment Act. Under this law, the "covered entity" (i.e., a healthcare provider, healthcare plan or healthcare clearinghouse) is often required to take corrective actions following healthcare-related data breaches, which may include:

- Mitigating alleged or potential harm to patients or other parties.
- Imposing sanctions – which may include reprimands, suspensions or terminations – on staff members responsible for the breaches.
- Revising lax policies and procedures.
- Enhancing employee training.
- Correcting other problems identified during the investigation.
- Developing sound practices to challenge/test the post-breach response plan at least annually.

HITECH reinforces the HIPAA Privacy Rule by mandating prompt reporting of large-scale data breaches and annual reporting of smaller breaches. In the case of disclosures involving more than 500 individuals, HITECH requires informing not only HHS, as well as affected persons and local media outlets within 60 days of discovery. HITECH also empowers state attorneys general to sue for damages on behalf of state residents who have been threatened or adversely affected by violations of the law, as well as to enjoin statutory violations.

For more information about what constitutes a data breach, and actions that should be taken following a data breach, please refer to HHS guidance, as well as guidance from your state and local authorities.

WHAT ACTIONS SHOULD I ASK MY EMPLOYEES TO TAKE TO PREVENT A HEALTHCARE-RELATED DATA BREACH?

The following basic measures are a starting point for employees to prevent a data breach:

- ***Be Vigilant About Phishing Emails***
    - Watch for phishing emails designed to entice you to click on the latest and greatest offer related to coronavirus protections, or with urgent instructions from your employer, all with

the intent of getting you to unwittingly download malware onto your device and the company's systems.
    - If you have any question about the validity of an internal company email, don't hesitate to contact the sender — and certainly do so before wiring any money or following changed payment instructions.
- ***Practice Good Cyber Hygiene***
    - Ensure that your devices are current regarding their anti-virus protection and that you're using secure and known connections. Use multi-factor authentication on any accounts for which it is available. Follow your facility's guidelines on internet use and use of your own device.
- ***Only Use Secure WiFi***
    - Only work on secure, password-protected internet connections. If you have to use public WiFi, be sure to verify with the entity that the network to which you're connecting is their legitimate network and is secured through a password. Avoid accessing any confidential or sensitive information from a public WiFi network. Hackers will try to trick you by mimicking the name of a secure network, so look closely and verify to ensure that the network you're joining is legitimate. If you don't, you can give the hacker control and access over everything you do on the internet.
    - Consider implementation and use of a virtual private network (VPN) for accessing PHI and other confidential information while working remotely.
- ***Report Lost or Stolen Devices Immediately***
    - Remote work increases the potential for the loss or theft of your devices.
    - Report any lost or stolen device immediately to your employer's security personnel to minimize the risk of fraud.
- ***Closely monitor and secure remote access services***
    - Monitor all remote access logs to verify and confirm that only authorized users are accessing your systems. Verify that multi-factor authentication is enabled for any remote access services. If you're unsure how to enable these services, please contact your IT department or software/service vendor for instructions.

Additional Resources:

- The Federal Trade Commission also offers resources for small businesses to help protect against phishing and other cybersecurity threats at: https://www.ftc.gov/tips-advice/business-center/small-businesses

- Report scams at ftc.gov/complaint
- The U.S. Department of Health and Human Services has educational materials specifically designed to give HIPAA covered entities and business associates information on how to respond to the threat of cybersecurity incidents: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
- Additional guidance is available at HealthIT.gov

The information, examples and suggestions presented in this material have been developed from sources believed to be reliable, but they should not be construed as legal or other professional advice. CNA accepts no responsibility for the accuracy or completeness of this material and recommends the consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual situations. This material is for illustrative purposes and is not intended to constitute a contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. “CNA" is a registered trademark of CNA Financial Corporation. Certain CNA Financial Corporation subsidiaries use the "CNA" trademark in connection with insurance underwriting and claims activities. Copyright © 2020 CNA. All rights reserved.