Ransomware **Attacks** on Healthcare: The Cost of **Data Breaches**?

Office of Information Technology
Division of Information Security
AUGUST 2023

The Indian Health Service (IHS) takes its mission to raise the physical, mental, social, and spiritual health of American Indians and Alaska Natives to the highest level very seriously. Protecting the patients we serve is more important than ever since cyber criminals increasingly target healthcare information. The healthcare industry faces unique challenges in implementing and maintaining robust cybersecurity measures given the industry's highly regulated nature and the complexity of healthcare systems.

The U.S. Department of Health and Human Services has reported that in 2022, the US saw more than 28.5 million breached healthcare records, an increase of over 35% from 2019's 21.1 million breaches. According to data from the Ponemon Institute, in 2022, the average cost of a data breach in healthcare was $10.1 million, more than double the industry average of $4.4 million.

Cybercriminals can access patient information in various ways. The most common techniques for accessing PHI are physically accessing login credentials or records, and executing successful phishing attacks. Cybercriminals generally launch phishing attacks on the health care industry with the objective of obtaining access to protected health information (PHI) or of delivering ransomware.

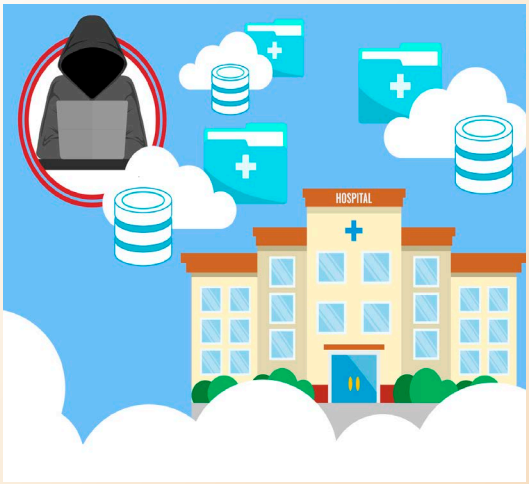
Access PHI

PHI is now a more valuable commodity on the black market than financial information. A study conducted by PrivacyAffairs.com found that cybercriminals sell full credit card details with their associated data for between $10 and $100 on the dark web, whereas a medical record is worth $250. This is because criminals can use medical records to create false identities, obtain free medical treatment, and commit highly lucrative insurance fraud, all at the expense of an innocent victim.

Ransomware

Cybercriminals target healthcare systems for ransomware because, once it has been installed on a healthcare organization's network, they can demand significant ransoms for the encrypted files to be unlocked. Healthcare companies generally decline to pay ransom given that paying is no guarantee that the criminals holding information will unlock the files or refrain from selling that information on the dark web.

Just this month, Prospect Medical Holdings, a private equity backed hospital owner based in Culver City, California, has had 16 of their 17 hospitals affected



by a ransomware attack, including causing them to shutter emergency departments, divert ambulances to other facilities, and close outpatient services. This breach appears to have been caused by the hacking of a user with administrative privileges.

Other examples include the breaches of Australian insurance company MediBank and PharMerica, a US-based pharmacy services provider. Combined, these two breaches exposed over 15.5 million patient records. Neither company paid the ransom, and some or all of their stolen records have been sold on the dark web. The ransomware breach of Illinois-based SMP Health System left the hospital unable to bill insurance, Medicaid, or Medicare for more than three months and eventually caused them to permanently close St. Margaret's Health hospital.

What can you do?

As healthcare professionals, every IHS employee, contractor, and US Public Health Service member is responsible for protecting patient data and IHS systems and networks. You can do your part by keeping the following tips in mind:

- **Guard your credentials:**
  - Never click on a link in an email or text without first verifying its authenticity.
  - Never enter your credentials where someone can see you by "shoulder surfing."
  - Never leave your personal identity verification card (PIV) unattended or lend it to anyone else.
  - Never give your login information to anyone else. IHS requires that anyone accessing IHS systems or devices have their own login credentials.
  - Never walk away from your system without setting the screen lock and removing your PIV card.
- **Guard patients' records:**
  - Never access a patient record where anyone unauthorized can see you by "shoulder surfing."
  - Never access a patient record unless you have a need to do so for your job duties.
  - Never leave a patient's record unattended.
  - Never send patient information using unencrypted email. If you must email patient information, use the Secure Data Transfer Service and make sure that you're sending it to the correct recipient.
  - Never let anyone into a secure area without badging in with their own PIV card. It may be polite to hold the door for the person behind you, but it isn't secure.
  - Never fax patient information without verifying that the recipient is available to receive the information immediately.
  - Never discuss a patient in a public area.

If you have any questions regarding this newsletter, please contact Cybersecurity@ihs.gov.

NOTE: *Products mentioned in this document are for informational purposes only and do not signify an endorsement.*