PHISHING FOR PHI

THERE'S A REASON WHY HEALTHCARE LEADS ALL INDUSTRIES IN DATA BREACHES

AND IT'S PROBABLY BECAUSE OUR PATIENTS' PHI IS ALL THAT PHISH *AND* A BAG OF CHIPS!

Valuable
HR Records
Authentications
System IP Addresses
Security Investigations
Device Identifiers
Floor Plans

Precious
Mom's Maiden Name
Home Phone/Address
Credit Card Numbers
Date/Place of Birth
Driver's License
SSN

Priceless
Often, all of your PII
PLUS
Medical Records
Beneficiary Info
Insurance Info
Prescriptions

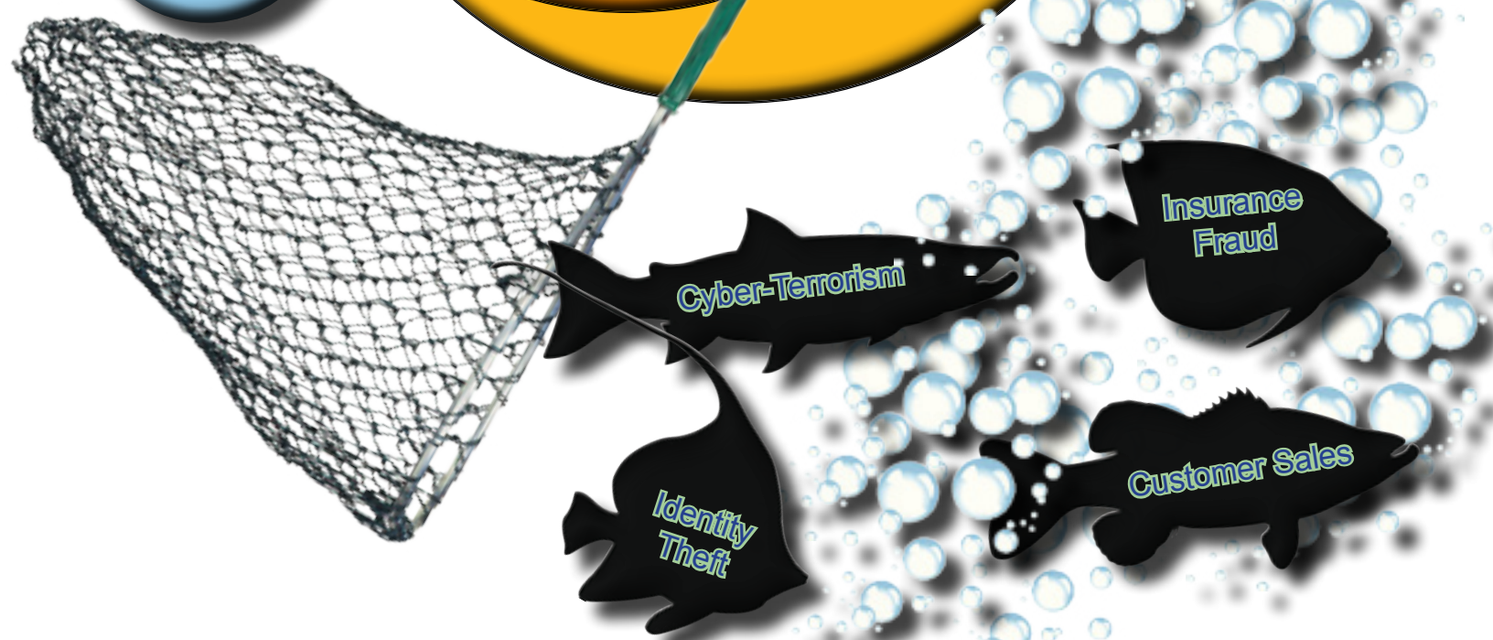
Sensitive Information
(Check out the IHS *Indian Health Manual*, Part 8 Chapter 12, IT Security)

PII Personally Identifiable Information
(Check out the Privacy Act of 1974)

PHI Protected Health Information
(Check out the HIPAA Privacy Rule)
PHI contains most of an individual's (and sometimes their relatives') identity profile, along with their medical history. PHI thieves can blackmail their victims, steal their insurance coverage, or jeopardize the integrity of their data files.

PII can be used for identity theft. The volume of details in a person's identity profile can aid criminals in stealing money, good credit, and positive reputation.

Sensitive information like personnel records can be used to steal identity-related resources. Other sensitive information about IT resources could put our networks and systems at risk for compromise.



Cyber-Terrorism

Cyber-terrorism is a growing threat facing United States organizations. Foreign and state-sponsored agents seek to undermine the faith in American organizations by publicizing their weaknesses.
Domestic terrorists, too, may simply want to cause embarassment or psychological trauma to their victims.

Identity Theft

There is no question about the lucrative benefits for identity theft criminals. Healthcare systems are notorious for being less secure, and the PII within health records allows criminals to access another person's financial resources and open lines of credit. Fraudulent activities can cause the victim endless grief and bad credit.

Customer Sales

Without a doubt, to cyber criminals, the most valuable asset of a healthcare database is the sheer volume of patient information that can be obtained.
Not only are there hundreds or thousands of records in a database worth ten times that of a credit card number, there are also hundreds or thousands of contacts to sell to marketers and other spammers.

Insurance Fraud

Thieves who steal our patients' health insurance information can use it to file reimbursement claims, to access narcotics, and to qualify for government services.
Fraudlent claims can lead to exceeded coverage caps or loss of coverage. They can also lead to dangerously mishandled medical care when the victim's diagnosis and treatment history have been altered by a fraud.

"Healthcare data are valuable because medical records can be used to commit several types of fraudulent activities or identity theft. Their value in the hacking underground is greater than stolen credit card data." - InfoSec Institute

HHS has one of the largest repositories of PHI in the country. You can do your part to safeguard the security of patient information by following some security best practices. Don't disclose PHI to anyone who doesn't have authorization to access it. Keep your account passwords a secret. Don't allow anyone to use your account to access IHS systems. Exercise caution when emailing and browsing the Internet, and don't be reeled in by phishers. If you suspect a breach may have occured, report it immediately!

Report security breaches, phishing attempts, and other security violations to the Incident Response Team at irt@ihs.gov.