Defending Your Office Against Medical-Data Hacking

Health care providers, health plans and related businesses continue to be prime targets for data hackers. From the start of the year through mid-March, more than 65 major breaches were reported to US Dept. of Health and Human Services (DHHS).

How big is the problem, really?

The two largest data hacks since January happen to be in Washington State, with one breach involving 970,000 records and another, 400,000 records. All told, more than 2.5 million individuals were affected in the year's first quarter. The screen shot shows just four weeks of the DHHS breach-reporting data base.

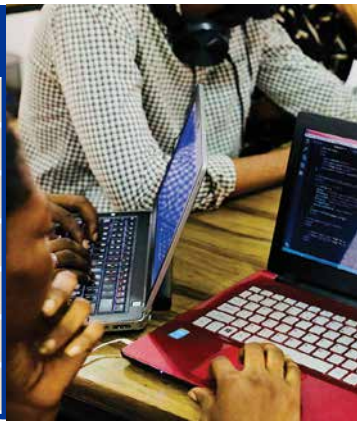
Recent health care data breaches of 500+ records.

Breach Report Results

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Direct Scripts	OH	Healthcare Provider	9319	03/06/2019	Hacking/IT Incident	Network Server
Maffi Clinics	AZ	Healthcare Provider	10465	03/06/2019	Hacking/IT Incident	Network Server
RSC Insurance Brokerage, Inc.	MA	Business Associate	2088	03/01/2019	Theft	Laptop
Pasquotank-Camden Emergency Medical Service	NC	Healthcare Provider	20420	02/28/2019	Hacking/IT Incident	Network Server
Rush University Medical Center	IL	Healthcare Provider	44924	02/28/2019	Unauthorized Access/Disclosure	Network Server
Humana Inc	KY	Health Plan	1447	02/27/2019	Hacking/IT Incident	Network Server
West Virginia Public Employees Insurance Agency	WV	Health Plan	1400	02/27/2019	Hacking/IT Incident	Network Server
Molina Healthcare	CA	Health Plan	895	02/22/2019	Hacking/IT Incident	Network Server
Delaware Guidance Services for Children and Youth, Inc.	DE	Healthcare Provider	50000	02/22/2019	Hacking/IT Incident	Desktop Computer, Electronic Medical Record, Email, Laptop
UConn Health	CT	Healthcare Provider	326629	02/21/2019	Hacking/IT Incident	Email
Rocky Boy Health Center	MT	Healthcare Provider	6000	02/21/2019	Theft	Other
Rutland Hospital, Inc. d/b/a/ Rutland Regional Medical Center	VT	Healthcare Provider	72224	02/20/2019	Hacking/IT Incident	Email
UW Medicine	WA	Healthcare Provider	973024	02/20/2019	Hacking/IT Incident	Network Server
Columbia Surgical Specialist of Spokane	WA	Healthcare Provider	400000	02/18/2019	Hacking/IT Incident	Network Server
OneDigital/Digital Insurance, LLC	GA	Business Associate	2763	02/15/2019	Theft	Laptop

Source: U.S. Department of Health and Human Services Office for Civil Rights, Breach Portal: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

INFORMATION TYPE	BLACK MARKET PRICE
Credit Card Number	$ 1.50
Date of Birth	$ 3
Social Security Number	$ 3
Mother's Maiden Name	$ 6
Employee Login Credentials	$ 10
Medical record information	$ 6-50
"DOS" - Ransomware	$133,000 – ransom and recovery



Why the persistent pursuit of medical data?

Why medical data? Because the data is valuable —more lucrative on the black market than a credit card or Social Security number. Medical record data can reap the hacker $6-50 per record.

What's the biggest danger?

For medical organizations, trojan malware seems to a major threat, even greater than ransomware. The malware (bad or malignant software) often arrives in an email, perhaps disguised as an invoice, payment or other familiar or official-looking message. Clicking a link or image in the "phishing" email downloads a malicious program to the system. Then, every time the system starts up, the malware searches for useful, valuable medical data to steal.

What steps can I take to avoid cyber-attacks?

- Recognize phishing attacks and report them (even from trusted sources)
- Don't click on links or open attachments unless you are expecting them
- Update your personal devices monthly to reduce vulnerabilities
- Use antivirus software on personal devices, including smart phones, Apple and Windows
- If you think your account has been compromised, report it to your help desk or customer support immediately
- Enable two-step authentication where possible

Designed by rawpixel.com / Freepik