Let's forget about a Cyber Attack for Now

The following Healthcare/HIPAA companies should have a big cyber worry besides ransomware and other cyber-attacks

Doctor Office*

Dentist Office*

Hospital*

Nursing Homes

Pharmacies*

Chiropractors

Psychologists

Health Ins. Co.

Storage Co.

HMOs

Government (pay)

- Medicare & Medicaid

- Military healthcare

- VA healthcare

U.S. Department of Health and Human Services monitors and develops standards for the Health Insurance Portability & Accountability Act of 1996. Congress incorporated into **HIPAA** provisions that mandated the adoption of Federal privacy protections for individually identifiable health information. HHS published a final privacy rule 12/2000.

Since 2003, HHS' Office for Civil Rights (OCR's) enforcement activities have obtained significant results that have improved the privacy practices of covered entities. The corrective actions obtained by OCR from covered entities have resulted in systemic change that has improved the privacy protection of health information for all individuals they serve. HIPAA covered entities were required to comply with the Security Rule beginning on April 20, 2005. OCR became responsible for enforcing the Security Rule on July 27, 2009.

As a law enforcement agency, OCR does not generally release information to the public on current or potential investigations.

* Please note that a number of companies have multiple regulations. All marked above besides HIPAA these companies also have PCI regulations.

HIPAA fines can range from $100 to **$50,000 per violation**, with a maximum penalty of **$1.5M** per year for each violation. **The two must damaging penalties for companies not complying is losing your vendor contract and or your practice that is forced into bankruptcy & closing.**

Other regulations

- **Cyber Insurance policy coverage** requires plans, policies, specific training of employees
- More vendor contracts now **require proof** of a cyber security program
- **Other- PCI,** NY State, California, Gramm-Leach-Bliley, ENISA &GDPR (EU)

Cyber Attacks is only ½ the story!

Cyber fines from HIPAA, PCI or DFARS can and has put SMB companies out of business

New York and Presbyterian Hospital (NYP) and Columbia University, $4.8 million

In a joint case, **the two organizations were fined** after 6,800 patient records were accidently exposed publicly to search engines. The breach was caused by an improperly configured computer server that was personally owned by a physician.

Columbia University

Columbia University (CU) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, including **a $1,500,000 monetary settlement a**nd corrective action plan to address deficiencies in its HIPAA compliance program.

Indiana Medical Rec. Service Pays $100K to Settle HIPAA Breach - May 2019

Medical Informatics Engineering, Inc. (MIE) has paid $100,000 to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services and has agreed take corrective action to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. MIE is an Indiana company that provides software and electronic medical record services to healthcare providers.

Powered by ACS

Ultimate **Risk** Services

SAVINGS THRU SAFETY & SECURITY

2874 W Ridge Pike | Norristown, PA 19403

610-755-0728 | www.ultimateriskservices.com