HIPAA Guard HERALD
YOUR MONTHLY NEWSLETTER ON SURVIVING HIPAA

ISSUE 03 February 2018

LATEST ON HIPAA

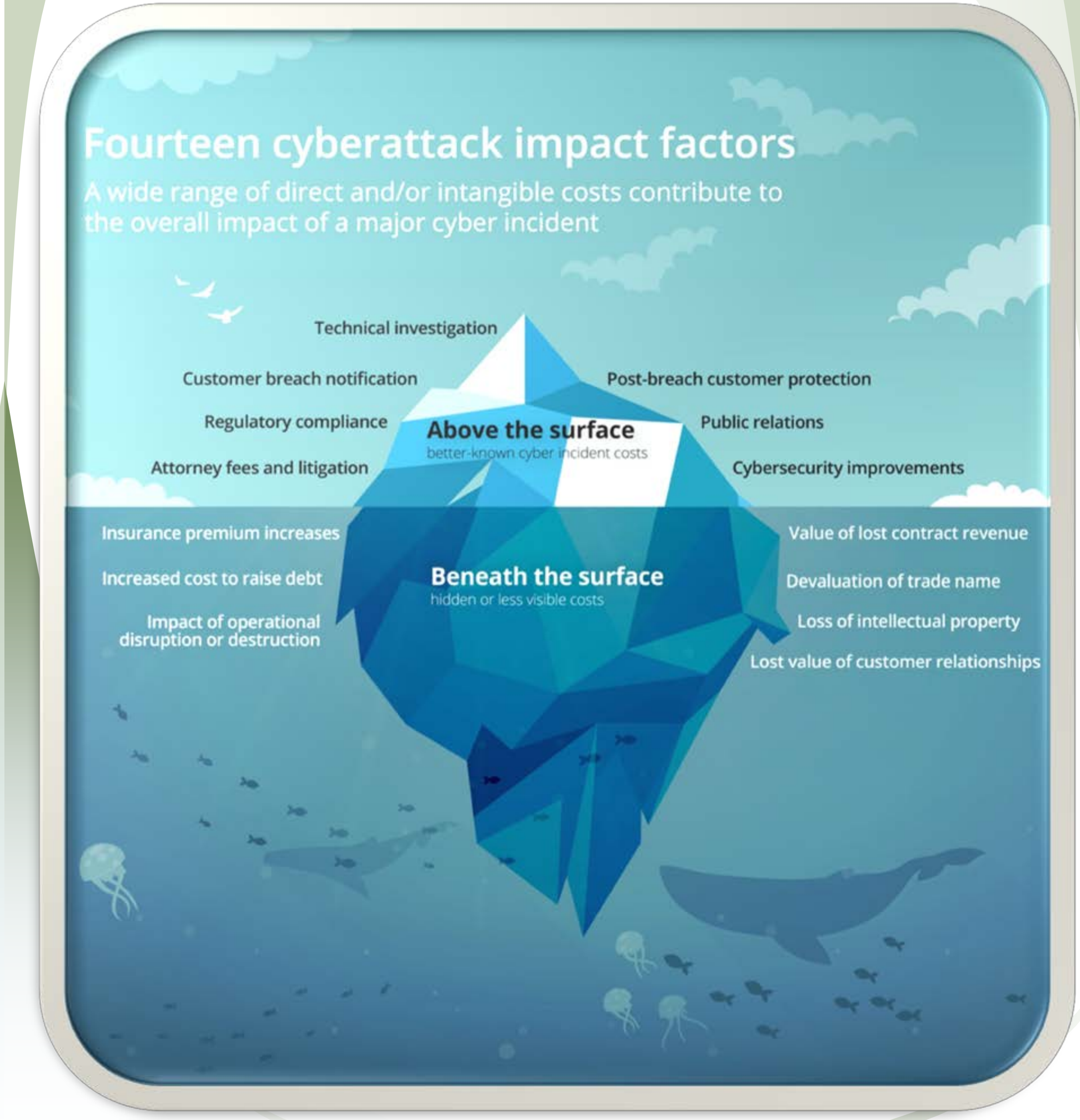
How much does a data breach cost?

In a study conducted by Deloitte entitled "Beneath the Surface of a Cyberattack: A Deeper Look at the Business Impacts" , Deloitte identifies 14 business impacts of a cyberattack, which are categorized as "**above the surface**" or well-known incident costs, and "**below the surface**" or hidden or less visible costs. Deloitte believes the current market valuation of cyber incidents is greatly underestimated, since the public focuses on the above the surface impacts – the far smaller percentage.

In recent updates, the Office of Civil Rights (OCR) of the Department of Health and Human Services (HHS) has announced its first settlement of a HIPAA breach in 2018.

The settlement arose from five separate breaches by five different entities owned by **Fresenius Medical Care**, a large provider of products and services for people with chronic kidney failure. The breaches involved stolen computers, a stolen USB drive, and a missing hard drive, all occurring within a five-month span in 2012.

The organization has agreed to pay $3.5 million to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), and to adopt a comprehensive corrective action plan, in order to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules.

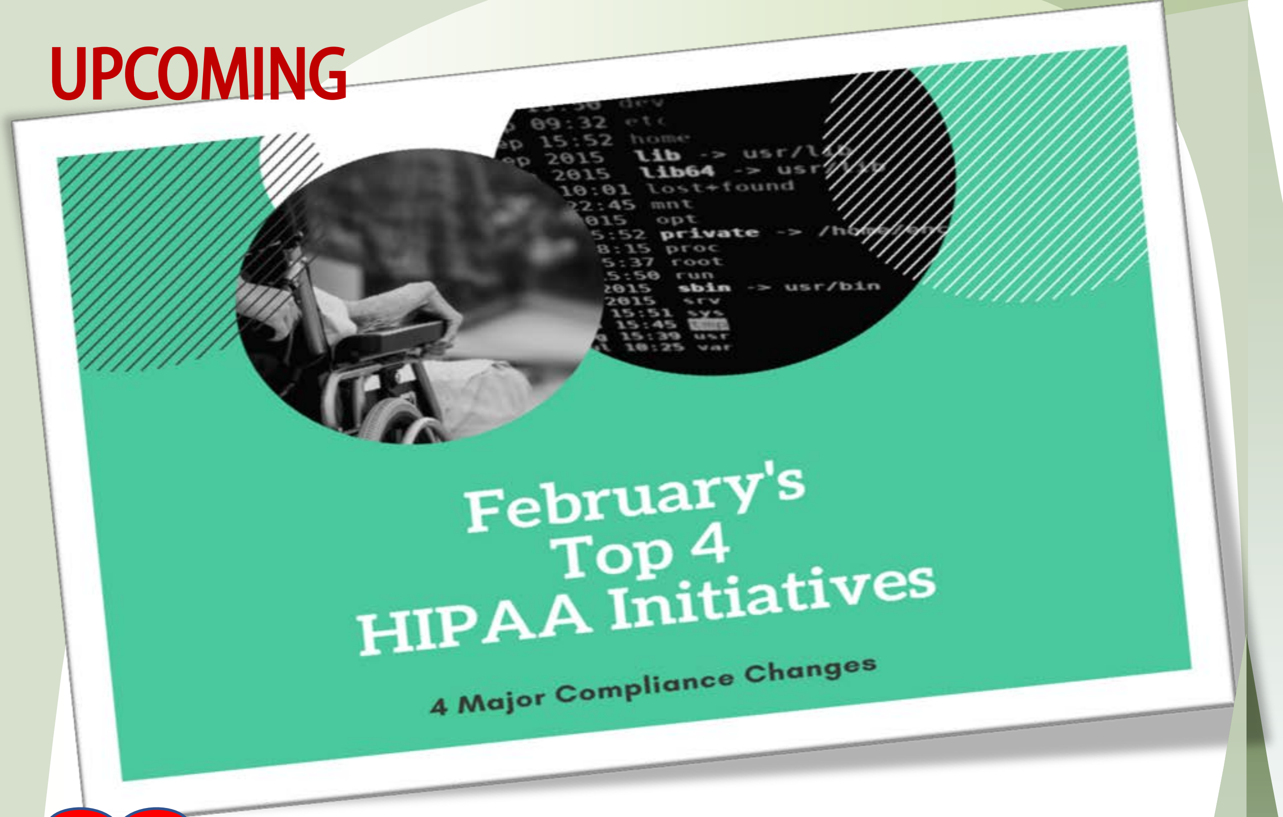


Fourteen cyberattack impact factors

A wide range of direct and/or intangible costs contribute to the overall impact of a major cyber incident

Technical investigation
Customer breach notification
Post-breach customer protection
Regulatory compliance
Above the surface
better-known cyber incident costs
Public relations
Attorney fees and litigation
Cybersecurity improvements
Insurance premium increases
Value of lost contract revenue
Increased cost to raise debt
Beneath the surface
hidden or less visible costs
Devaluation of trade name
Impact of operational disruption or destruction
Loss of intellectual property
Lost value of customer relationships

UPCOMING



February's Top 4 HIPAA Initiatives

4 Major Compliance Changes

February's Top 4 HIPAA Initiatives:

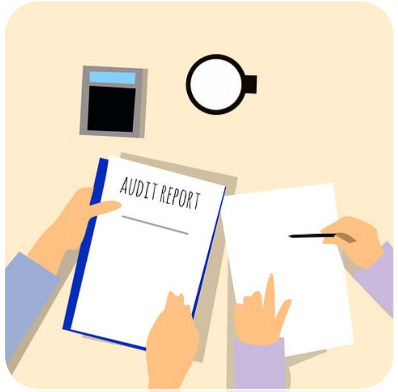
Hello EMPOWER Family,

We are making tremendous headway in the journey to complete HIPAA COMPLIANCE! Each month, in 2018, HIPAA Guard will lead you in making 4 major Compliance changes. Please do your part to help with the 4 initiatives each month, and at the end of this year, we will be compliant in 48 more areas!

For tips and/ or training on any of these areas,

contact HIPAA Guard-

your partner in day to day HIPAA Compliance.



Systematic audit log monitoring for EHR:

Audit Controls, Access and Privacy Monitoring

Distribute and Educate all Employees on HIPAA Violation Sanction Policy:

Sanctions, Enforcement and Discipline for Security or Privacy Violations

Each Employee completes the Standardized Comprehensive HIPAA Training course:

HIPAA Security and Privacy Awareness Workforce Training Policy

Digital Copies and Device Privacy:

Guidelines for managing digital devices

INITIATIVES

Audit Controls, Access and Privacy Monitoring

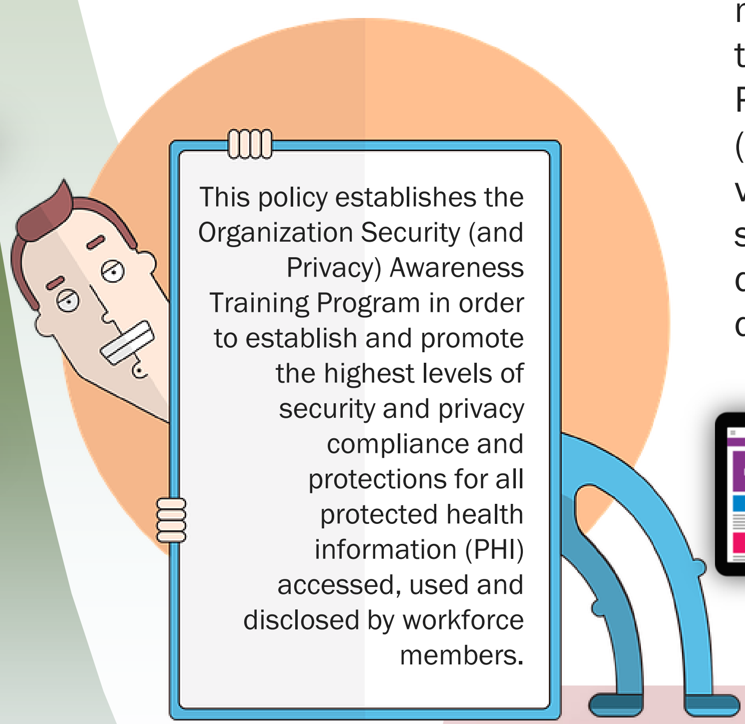
To define the policy for on-going audit controls, as well as privacy and security auditing measures to identify suspicious activity and/or breaches of information and monitoring functions as a deterrent to workforce members from seeking inappropriate access to PHI/ePHI.

Sanctions, Enforcement and Discipline for Security or Privacy Violations

To define and educate each workforce member of the Policy and Procedures to be followed for Enforcement and Discipline (also known as “Sanctions”) related to HIPAA Security and/or Privacy Violations and Breaches.

ISSUE 03
February 2018

HIPAA Security and Privacy Awareness Workforce Training Policy



This policy establishes the Organization Security (and Privacy) Awareness Training Program in order to establish and promote the highest levels of security and privacy compliance and protections for all protected health information (PHI) accessed, used and disclosed by workforce members.

START
THE POP
QUIZ!

Try your hand at HIPAA Guard’s HIPAA pop quiz to find out whether you and your staff make the grade when it comes to protecting patient privacy.

Guidelines for Managing Digital Devices

To define guidelines for managing digital devices with the intent to prevent Protected Health Information (PHI) breach and / or HIPAA violations arising from PHI storage on the hard disk drives or memory of these digital devices.

*printers, copiers, faxes should be in secure areas only

*set up physical barriers as needed/locks/signage, limit & define usage

*settings to track users/unique user codes if possible

*all settings on these devices should have audit logs and the highest security setting

*perform systematic audits of their use and report any suspicious activity