HIPAA Guard HERALD

YOUR MONTHLY NEWSLETTER ON SURVIVING HIPAA

ISSUE 02 January 2018

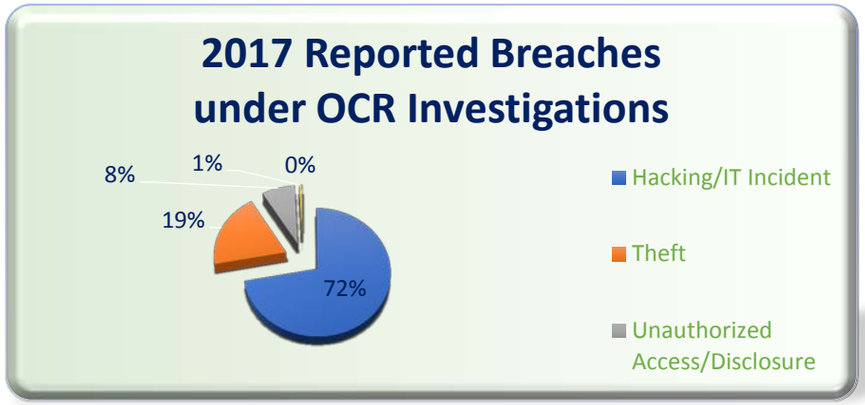
LATEST ON HIPAA

How the Healthcare Industry Scored in 2017's Data and Security Breaches

The year 2017 is almost behind us, how do you think the healthcare industry is faring? Based on OCR's list of Breach of Unsecured Protected Health Information as required by section 13402€(4) of the HITECH Act, OCR has shown this alarming and increasing number of PHI and ePHI breaches undergoing investigation. Consistent with that of the past years' stats, the leading cause of breach is Hacking/IT Incident (72%) with a Network Server (62%). There seems to be no slowing down in the amount of breaches being experienced by healthcare community. More importantly, as reported in the 2017 Ponemon Cost of Data Breach Study by IBM, by industry, the Healthcare breaches is the most costly and that is for the 7th year in a row.

Healthcare data breaches cost organizations $380 per record, more than 2.5 time the global average cost across industries which is $141 per record. Nonetheless, alarming as it might seem, there is nothing insurmountable so long as everyone works together in this.

In that same report, the top factors sighted that helped reduce cost of a breach are having updated and organized Incident Response, Encryption and Education of everyone concerned. Having an Incident Response team, for example, has brought down the cost by $19 per lost or stolen record, followed by extensive use of Encryption with $16 reduction per record and Employee Training with $12.50 reduction per record.



Top 6 Best Response on Data Breach

UPCOMING

4 Major Compliance Changes

January'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.

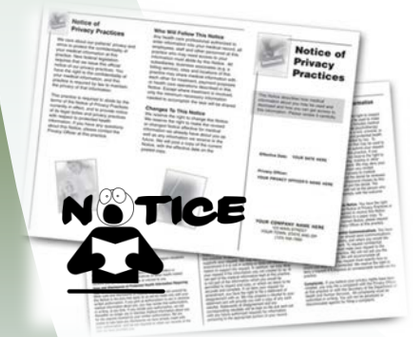
ISSUE 02
January 2018

NO CLOUD STORAGE:

Ticket and stop using 3rd party storage such as Dropbox, ICloud, etc. unless they can and have provided a BAA.

NO FLASH DRIVES:

Ticket and stop using any USB or flash drives. IT can set up a shared drive as a workaround.



NOTICE OF PRIVACY PRACTICES:

Insure updated privacy practices, and other HIPAA required notices are posted and offered, distributed to patients.

ENCRYPTION:

Send all emails that contain PHI with encryption. Avoid sending emails internally, when a shared file can be utilized. However, all departments at all sites MUST send all emails encrypted if the transmission contains any personal identifiable information of employees or patients.

UPDATES

Privacy and Security Risk Self Assessment Tool

Free Download of Self Evaluation Of HIPAA Privacy and Security Compliance

The Privacy and Security Risk Self Assessment Tool is designed to provided covered entities with an idea of how they might fare in a HIPAA Audit. It contains basic questions answerable with YES, NO and UNCERTAIN. This self assessment is split into two sets - Privacy Rule Section and Security Rule Section.

Access the free tool here:

https://hipaaguard2017.wixsite.com/survivinghipaa/hipaa-self-assessment

FREE E-learning Courses by HIPAA Guard

Member organizations of HIPAA Guard shall have access to free online trainings of the following courses:

- HIPAA Awareness Course Training
- HIPAA Privacy Rule Course Training
- HIPAA Security Rule Course Training

These trainings are accessible via Moodle Cloud. For more information on how to attend these trainings, kindly contact your Privacy or Compliance Officers or email us at *info@hipaa-guard.com*

ISSUE 02
January 2018

TIPS

Protecting ePHI and PHI in Computer Monitor Screens from Visitors in Waiting Room or When Walking thru Hospital

Both Laptops and desktop computers can be a way you store PHI. It is vital that you consider how you can help to protect patient confidentiality these and all other electronic equipment as mandated by HIPAA:

- Create a password to secure access to electronic health records
- Turn monitors away from patient path or traffic areas to prevent accidental release of information not needed by the patient
- Properly place computer monitors in areas or at angles that minimize viewing by persons who do not need the information

Simon Watson / Getty Images

- When the monitor is not in use, make sure a blank or black screensaver is shown and when beginning to use it, a password will be required.
- All must be reminded not to store ePHI on thumb drives or other removable media devices unless they meet your organization's encryption standards

Connect With Us

Wish to share content, find answers, post and view jobs, make business contacts, and connect with industry experts relating to HIPAA?
Then let's build a valuable community in "Surviving HIPAA" LinkedIn group. **JOIN US TODAY!!!**