HIPAA Guard HERALD
YOUR MONTHLY NEWSLETTER ON SURVIVING HIPAA

ISSUE 04 March 2018

LATEST ON HIPAA

Healthcare and Social Media

Opportunities, Challenges and HIPAA Compliance

The World Wide Web has indeed evolved, new technologies continue to rise up and applications and platforms, such as "social media," continues to grow its popularity and these are creating new opportunities for healthcare organizations but is also raising privacy and security challenges.

In a document provided by the HIMSS, the following are seen as the purpose why individuals and organizations use social media:

1. *Delivery of Pre-Developed Content*
2. *Engagement of People into Interactions*
3. *Communication Management*

Health care organizations are using social media to deliver existing information and data in a more engaging and speedy manner than emails or website posts.

Brand awareness, customer satisfaction, and people connection through collaborations, reviews and interactive dialogs about opinions is another purpose for social media.

Social media is also found to be a great means of consolidating and managing communications with families and friends.

The challenges faced by organizations in using social media are:

1. Ethical Challenges
2. Privacy Challenges
3. Security Challenges

Ethical Challenges

Ethical focus continues in healthcare and not only HIPAA requirements are being considered but also Sarbanes-Oxley Act of 2002 (SOX); The National Center for Ethics in Healthcare (1991) and World Health Organization Ethics and Health Initiative in 2002.

Privacy Challenges

With the birth of HIPAA and the rise of use of social media in the healthcare industry, your ITC department are now waging a new battlefield where the protection of sensitive personal, private, health information from cyber hackers and attackers , malwares and spywares , viruses and cookies are now the main focus. And the ITC department must also consider addressing the risk of employee theft of PII, PHI, and intellectual property.

Security Challenges

The risk of publicly exposing information that are warranting protection such as PHI and ePHI are apparent with the use of social media. This challenge we call as "data leakage". This as we know can bring about negative impact to the confidentiality of the data and the privacy rights of the individuals affected.

Therefore to prevent and minimize the risks brought about by using social media tools in the healthcare industry the following are suggested to be put in place within the organization.

Social Media Policy

One policy should be focused on the human behavioral aspects of social media and another policy should be focused on how the organization plans to use social media.

Risk Mitigation Strategies

This is the systematic reduction of the extent in the exposure to a risk and/or the likelihood of this event from happening.

It is apparent that the two main risk we are about to face in using social media in the healthcare industry are the Human Behavior and the Technology risks.

The HIMSS paper has explained in detail the "*common social media technologies and platforms, the challenges that arise, and provided strategies as to how these can be used effectively, while protecting the healthcare organization from risk and respecting patient's individual privacy*."

Violations over Social Media & the Internet Due to Lack of HIPAA Safeguards

Phoenix Cardiac Surgery

A $100,000 settlement amount and a corrective action plan that includes a review of recently developed policies and other actions taken to come into full compliance with the Privacy and Security Rules was undertaken by Phoenix Cardiac Surgery due to physician practice was posting clinical and surgical appointments for their patients on an Internet-based calendar that was publicly accessible.

Complete P.T., Pool & Land Physical Therapy, Inc.

Settlement of $25,000, adoption and implementation of a corrective action plan, and annual reporting of compliance efforts for a one year period was sanctioned against the practice when it posted patient testimonials, including full names and full face photographic images, to the company website without obtaining valid, HIPAA-compliant authorizations.

REMINDERS !!

Remember these DO'S AND DON'TS in social media and remain HIPAA Compliant

List of What Your Organization May Post in Social Media

- ✓ Health tips that might be useful to patients
- ✓ Upcoming events of your organization or other companies that might interest your patients
- ✓ New research or findings related to your industry or specialization
- ✓ Honors or awards your organization has been given
- ✓ Your organization's Staff Profile
- ✓ Advertisements of your services as long as they DO NOT CONTAIN THE PROTECTED HEALTH INFORMATION of any of your patients (including names, photos, or any other personally identifiable information)
- ✓ Promotions i.e. Discounts or special offers on services you provide

FREE Course by Udemy on "Social Media for Healthcare Providers"

Learn the following from this FREE 36-min. on demand video:

- ❑ How the HIPAA Privacy Rule and HIPAA Security Rule apply to social networking
- ❑ Understand the advantages and benefits of social media communications to health care professionals
- ❑ Learn about permitted disclosures, the minimum necessary requirement and rules on endorsements
- ❑ Hear examples of prior HIPAA violations that resulted in fines from Dept. of Health & Human Services

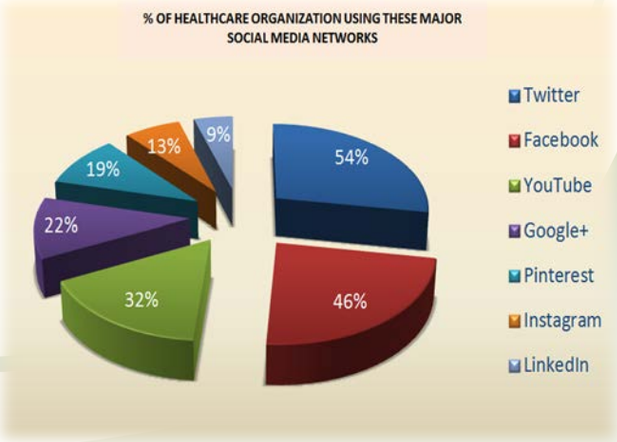
Click here:
https://www.udemy.com/hipaa-compliance/

HHS Social Media Policies Checklist

Download and printout this checklist which explains the most common policies and standards that impact the use of social media and ensure your organization is compliant with HIPAA guidelines on the use of social media.

⇩ DOWNLOAD NOW

% OF HEALTHCARE ORGANIZATION USING THESE MAJOR SOCIAL MEDIA NETWORKS



UPCOMING

March

March's Top 4 HIPAA Initiatives:

Greetings EMPOWER Family,

Great start for the year towards our journey to complete HIPAA COMPLIANCE! Let us continue to implement and advocate these monthly major HIPAA Initiatives. 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!

EDUCATING YOUR WORKFORCE
IS NOT ONLY A REQUIREMENT OF HIPAA,
IT IS A CRITICAL COMPONENT TO YOUR SECURITY PROGRAM

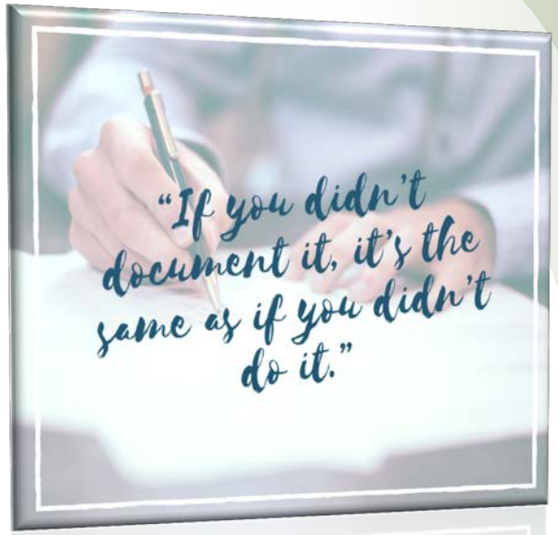
contact HIPAA Guard-
your partner in day to day HIPAA Compliance.

ISSUE 04
March 2018

REBOOT KEEPING COMPUTING SIMPLE HIPAA GUARD

DOCUMENTATION

For providers and healthcare organizations good documentation practices are more important than ever before!



REMOTE USER SECURITY

Guidelines on How to Tighten Security for Remote Workers

✓ Protect Remote Worker's Devices and Equipment

- ❑ Bar personal web browsing and emailing by workers on work stations
- ❑ Use security software & activate automatic update to fight Malware infections
- ❑ Use latest versions of all applications
- ❑ Install new security patches soonest & use patch-management tool
- ❑ Install whole-disk encryption software to keep unauthorized people from accessing company data

✓ Use cloud applications

- ❑ Make sure your CSP enter with you on a Business Associate Agreement
- ❑ Perform Risk Analysis on Cloud computing Platforms (45 CFR §§ 164.308(a)(1)(ii)(A))
- ❑ Establish Risk Management Policies in relation to the service and ensure identified risks are managed and reduced at a reasonable & appropriate level (45 CFR §§ 64.308(a)(1)(ii)(B)).
- ❑ Read on the Recommendations on Cloud Computing by NIST here.

UPCOMING

PASSWORD REQUIREMENTS

Here are some Good Password Practices

1. Use Strong Passwords
   - o *Must be at least 8 characters long*
   - o *Require use of capital letters, special characters and numbers*
   - o *Consider use of passphrases*
2. Change passwords periodically - every 60 to 90 days.
3. Do increase the number of times passwords must not be re-used
4. Don't keep passwords where it can be easily found
5. Don't share passwords

INTERNAL SECURITY CHECK UPS

Perform regular, scheduled internal security checkups in as many areas as possible.

Related Policies on Internal Security Check Ups

S1 Security-Information Security Strategy Policy

S18 Security-Technical Safeguards: Audit Controls Policy

Policy S1 requires organization to establish the administrative processes and procedures to implement a comprehensive security program.

Security Program will consist of the following:

- Risk Analysis
- Risk Management Plan
- Sanction Policy
- Information System Activity Review

Policy S18 requires implementing hardware, software , and/or procedural mechanisms to record/examine activity in information systems with sensitive information.

Audits are conducted periodically to:

- Ensure the confidentiality, integrity, and availability of sensitive information
- Investigate possible security incidents & ensure conformance to covered entity's security policies
- Monitor user or system activity , where appropriate

Reference:

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf