CHC Webinar

April 24, 2024 @ 1 pm

Navigating Health Data Privacy: Putting Agency HIPAA Compliance into Practice

Liam Degnan
Senior Solutions Engineer
Compliancy Group

Jim Potter - Moderator
CHC Executive Director

Our company's mission & vision:

We simplify compliance so you can confidently grow your business.

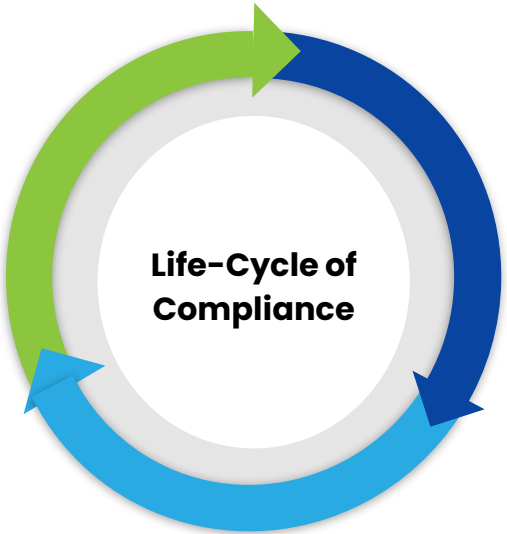
To be the affordable industry standard for simplified compliance.

Introduction to HIPAA Compliance

The Seven Fundamental Elements of an Effective Compliance Program

1. Implement written policies, procedures, and standards of conduct
2. Designate a person to ensure they're followed
3. Conduct effective training and education
4. Develop effective lines of communication
5. Conduct internal monitoring and auditing
6. Enforce standards through well-publicized disciplinary actions
7. Respond promptly to detected offenses and undertake corrective action

Where to Begin & How to Manage



HIPAA Compliance and Social Media

Business Associate Agreements

Business Associate Agreements are **mandatory** under the **HIPAA Privacy Rule**
Outlines what Business Associates **can** and **cannot do** when they access **Protected Health Information**

When is a BAA Required?

- If you provide services to a HIPAA business associate that involves PHI
- Your vendor is involved in creating, sending, storing, or receiving PHI
- Your vendor's services require that you disclose PHI to your vendor
- Your vendor accesses your PHI on a regular basis

Are These Platforms HIPAA Compliant?

Facebook

No. Facebook refuses to sign a BAA with healthcare organizations, which would ensure its HIPAA compliance.

Twitter

No. Twitter will not sign a BAA with healthcare organizations, which would ensure its HIPAA compliance.

Instagram

No. Instagram won't sign a BAA with healthcare organizations, which would ensure its HIPAA compliance.

Snapchat Video Results in Jail Time

In January of 2016, a nurse's assistant was sentenced to 30 days in jail for posting a video of a patient online.

The 21 year old uploaded a snapchat video playing tug-of-war with an Alzheimer's patient.

**HIPAA applies to all social accounts not just corporate ones!*

"Snapchat was found to be the most popular site for image and video sharing, although it is far from the only social media network used for sharing degrading and demeaning videos of patients"

-HIPAA Journal

HIPAA Compliant Advertising

1. Remove marketing pixels from apps and websites
2. Strip your data of any traces of PHI before pushing to ad networks
3. Create campaigns on broad targeting
4. Consider using a safe tag management system for better control
5. If your tracking tool captures IP addresses, that is a HIPAA violation

Facebook won't sign a BAA so advertising on this platform will need to be done without revealing any PHI.

Twitter (X) won't sign a BAA so advertising on this platform will need to be done without revealing any PHI.

Instagram won't sign a BAA so advertising on this platform will need to be done without revealing any PHI.

Google Ads and HIPAA Compliance

Google is HIPAA compliant because they are willing to sign a BAA with HIPAA-related entities.

However, according to HIPAA Included Functionality, Google Ads is **not covered** by Google's services that are willing to sign a BAA with HIPAA-related entities that use Google Ads' advertising platform.

Google Ads

Security Rule - Online Tracking Technology Guidance

Covered entities may not use tracking technologies (like the Meta/Facebook pixel feature, and Google Analytics) in a way that would result in a prohibited disclosure of PHI to third-party analytics and social media companies. Patient authorization is required for these disclosures.

HHS has not withdrawn this guidance, even in the face of a lawsuit filed by the American Hospital Association.

It is fair to expect that OCR will be bringing enforcement actions against providers who use tracking technologies to share PHI with third party analytics and social media companies without patient consent.

HIPAA Compliant Reputation Management

Social Media *Dos*

DO thank patients for feedback
DO keep your responses anonymous
DO take compliments offline - call the office
DO focus on the positive
DO have written consent if you use a patient's testimonial

Social Media *Do Nots*

DO NOT email/text a patient without consent
DO NOT alter consent
DO NOT repeat or use PHI
DO NOT reply or use PHI
DO NOT reply or post info that confirms the identity of a patient
DO NOT respond to patients sharing of a diagnosis or service

HIPAA Compliant Marketing

Marketing Policy Should Include:
Procedures for receiving patient authorization for marketing communications, what to do if you'd like to use patient testimonials or reviews for marketing, and opt out procedures.

Marketing Opt Out Should Include:
A way to easily unsubscribe from them. This may include an unsubscribe link in marketing emails, or the option to text STOP to opt out of text message marketing.

Marketing Restrictions:
The Privacy Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing.

HIPAA Compliant Marketing

Use PHI for marketing purposes by utilizing the following:

Authorization Forms:
Healthcare organizations need signed authorization forms from patients when their PHI will be used for marketing purposes.

Lookalike Audiences:
Analyze your patient data on your own by using a spreadsheet, and input ONLY the demographics that you identified as your target audience into your marketing tools.

*make sure your spreadsheet software is HIPAA compliant!

A HIPAA-Compliant Website

If your website stores or transmits protected health information, it needs to be HIPAA compliant to protect patient information from getting leaked.

Non-compliance has ramifications like loss of business, financial penalties, and loss of trust.

Is Your Website HIPAA Compliant?

There are several steps to take to ensure your website is HIPAA compliant and a majority of them stem from data security.

Take steps to guard PHI against accidental breaches.

Questions to Consider for a HIPAA Compliant Website:

1. What data is being collected/stored on your website?
2. Are your web forms HIPAA compliant?
3. Where does the data go to once collected?
4. Is the location your data is stored compliant?

HIPAA Compliant CRMs and Marketing Technology

Why a HIPAA Compliant CRM?

A HIPAA-compliant CRM integrates patient data, appointment scheduling, and communication tools

Healthcare professionals need a place to manage patient interactions efficiently and securely

How to Know if Your CRM is HIPAA Compliant

A CRM platform is HIPAA compliant if:

- It ensures all patient data remains confidential
- Is backed up and securely stored

A BAA is needed in order to be HIPAA compliant!

Having complete control over the data in your CRM is vital. Only transmit encrypted data - no unauthorized intake, access, creation, storage, or sharing of data

A HIPAA compliant CRM keeps all patient data secure and private

HIPAA Compliant Security Features

User Authentication:
Each employee is to have unique login credentials to access the platform. Use two-factor authentication for increased security.

Access Controls:
Access controls limit access to sensitive data, and should be set based on an employee's job function. Not all employees should have full access, access should only be granted to the data that they need to perform their job.

Audit Logs:
Shows access patterns of employees, letting administrators identify when an employee is accessing data excessively. Allows both insider and outsider breaches to be detected quickly.

End-to-End Encryption
E2EE prevents unauthorized access to data at rest and in motion by converting it to a format that can only be read with a decryption key.

CRM HIPAA Compliance Checks

1. Does the CRM have a Business Associate Agreement (BAA)?

   The CRM is considered a vendor under HIPAA. It's important to sign a BAA ensuring the vendor's responsibility to protect PHI

1. Is the CRM secure enough for PHI?

   Assessing the security of a CRM requires a thorough evaluation of security features like encryption protocols and role-based permissions

1. Do the Terms of Service affirm HIPAA compliance?

   The CRM should explicitly state in their Terms of Service that their platform is HIPAA compliant. HIPAA involves specific technical, physical, and administrative safeguards to protect PHI

HIPAA Compliant CRM Examples

caspio

keap

highlevel

salesforce

nexhealth

HubSpot

HubSpot is NOT HIPAA Compliant - will not sign a BAA

Mail Theft Statistics

USPS has claimed there are as many as 1.7 million cases of mail theft daily

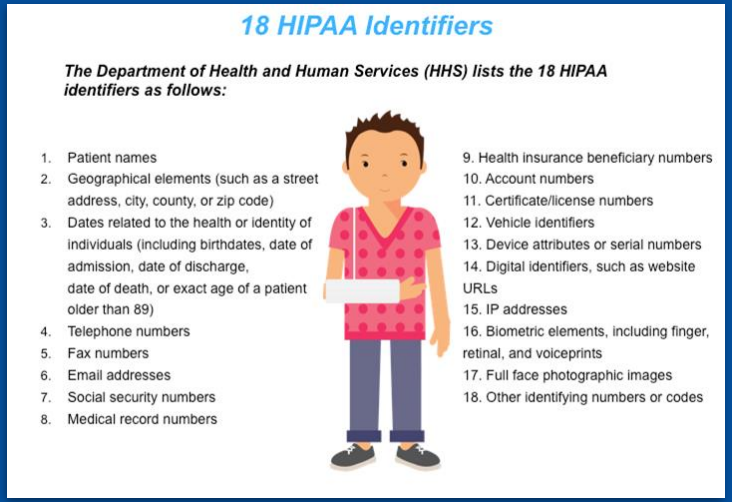
From 2018-2023, postal inspectors have arrested more than 9,000 suspects for theft of mail and packages

Over one third (36%) of all Americans who deal with the postal service have once experienced a mail theft case

What You Can Find in the Mail

1. Name
2. Address
3. Telephone Numbers
4. Email Addresses
5. Insurance Information
6. Treatment Records/Invoices
7. Many other potential identifiers!

*18 identifiers



THANK YOU

Liam Degnan
Senior Solutions Engineer
(855) 854-4722 ext. 530
ldegnan@compliancygroup.com