hcp | Healthcare Compliance Pros

Compliance solved.

SUPPORT

HIPAA

CORP.

OSHA

H/R

stress not included.

Training · Assessments · Support

THE TOP 10 Compliance Issues:

That You Should Be Looking at In Your Organization

Hello!

I’m Chad Schiffman,

Director of Client Services at
Healthcare Compliance Pros,
You can find me at **chad@hcp.md**

hcp | Healthcare Compliance Pros

Now’s your chance, ask away…

Too shy? You can also:
Call me at 855-427-0427 or
Email me: chad@hcp.md

The Top 10 Compliance Issues That You Should Be Looking at In Your Organization

1. Security Risk Analysis – Including "not sufficient" (EMR or checklist).
2. Cybersecurity - including malware, targeting attacks, blurring of business and personal functions.
3. Social Media Policy and Procedure missing or not being followed.
4. Exclusion screenings not being performed correctly, or at all.
5. Failing to have implemented auditing and monitoring in place.
6. Mobile Devices - including lack of security, control over text messaging.
7. Missing mechanisms for employee and patient complaints.
8. Failing to implement regular, effective education and training programs.
9. Not tracking or reporting suspected breaches or other incidents.
10. Compliance program deficiencies and/or findings not being communicated or corrected.

1. Security Risk Analysis - Including "not sufficient" (EMR or checklist)

A HIPAA Requirement

- The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities and its business associates conduct a risk assessment (analysis) of their healthcare organization.
- A risk assessment (Security Risk Analysis) helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards.

1. Security Risk Analysis - Including "not sufficient" (EMR or checklist)

A HIPAA Requirement (cont.)

- A Security Risk Analysis should help reveal areas where your organization's protected health information (PHI) could be at risk.
- Yet, organizations are facing challenges fulfilling this important requirement.

1. Security Risk Analysis - Including “not sufficient” (EMR or checklist)

Common OCR Finding

- 2018 was a record year for HIPAA enforcement actions. The Office for Civil Rights (OCR) settled 10 cases and one case was granted summary judgment. In total, these actions eclipsed $28 million dollars!
- A review of the OCR findings revealed a common theme: SRAs were not sufficient, and in some cases, not even being performed at all!

1. Security Risk Analysis - Including "not sufficient" (EMR or checklist)

Our recommendations to address this issue

1. An initial SRA and subsequent reviews thereafter – at least annually should not ever be considered optional.

2. A HIPAA Complaint SRA is a healthcare organization's best defense:
   - This means avoid using "checklist" options when performing your SRA
   - Even if you have installed and implemented a certified EHR, you must perform a full SRA

1. Security Risk Analysis - Including "not sufficient" (EMR or checklist)

Our recommendations to address this issue (cont.)

3. Once deficiencies are identified, create an action plan to address them prior to your next SRA submission.
4. Consider having a certified professional perform or review your SRA.
5. Remember, a HIPAA Compliant SRA is a living and breathing process of identifying risks, establishing a corrective action plan, and reassessing - when there are updates in policies procedures, IT systems, etc., and at a minimum if nothings changes, reviewing on an annual basis.

2. Cybersecurity - including malware, targeting attacks, blurring or business and personal functions

Current Cybersecurity Trends

Most cybersecurity experts agree, there are at least three trends healthcare professionals need to be aware of:

1. Blurring of personal activities and business activities performed online
2. Malware and targeted phishing attacks will be on the rise
3. An increase in identify theft

2. Cybersecurity - including malware, targeting attacks, blurring or business and personal functions

Blurring of activities

How many of you know someone who uses their work email address for personal things, such as making a purchase from Amazon?

Or the worker who accesses social media and posts updates while not thinking about tracking?

2. Cybersecurity - including malware, targeting attacks, blurring or business and personal functions

What's the risk?

Most employees don't believe that it's actually a problem, when it really it could be. The door could be left open to an organization for cyber criminals to target an organization, send phishing emails, etc., making it hard to decipher what's real.

Think about it this way. Have you ever looked at something on the internet and see it show up as a suggestion in your social media? While this not be a problem on a personal account it could be for a healthcare organization.

2. Cybersecurity - including malware, targeting attacks, blurring or business and personal functions

Speaking of Phishing

It is estimated that mobile device phishing attacks are up 85%, year-after-year, since 2011.

What’s the cause?

It has to do with the increasing amount of data collected by every site and app visited on your mobile device, and not having proper safeguards in place on your devices.

This can be problematic for healthcare organizations who allow mobile devices to access networks, health records, or transmitting PHI (such as text messages). More on this later in the presentation.

2. Cybersecurity - including malware, targeting attacks, blurring or business and personal functions

Increase in Identity Theft

According to a report by Experian, in 2017 nearly 158 million social security numbers and just over 14 million credit card numbers were exposed.

What about the healthcare industry?

- 27 percent of those thefts belonged to the healthcare industry.

These numbers are expected to rise in 2019.

2. Cybersecurity - including malware, targeting attacks, blurring or business and personal functions

Did you know?

On average, breaches can cost $400 or more per patient.

- Yet, it is estimated that only 33 percent or organizations had plans on how to defend against a cyberattack.
- Only 25 percent conducted training on the issue.
- And just under 10 percent participated in drills or exercises intended to prevent a cyberattack.

2. Cybersecurity - including malware, targeting attacks, blurring or business and personal functions

To address these issues, we recommend:

1. Perform a **security risk analysis**
2. Establish a **risk management program**
3. Maintain an **inventory and identify** device and network vulnerabilities
4. **Train employees** to better identify suspicious emails and other messaging technologies that could introduce malicious software into the organization
5. Have an implemented **Social Media Policy**

3. Social Media Policy and Procedure
missing or not being followed

To address these issues, we recommend:

Social media usage is commonplace in our day-to-day lives and most of us use various types of social media platforms.

In 2018, there were over 240 million social media users in the United States!

Social Media is fun and convenient providing quick access to, and posting of information, ideas, personal messages, and other content.

Unfortunately, there are some bad actors lurking on social media platforms

3. Social Media Policy and Procedure
missing or not being followed

Recent example of bad actors lurking on Social Media

Not too long ago, a breach was reported by Timehop. As a result, there was a compromise of personal data, including names and emails, of 21 million users. While the information that was breached did not include financial data, private messages, direct messages, user photos, user social media content, social security numbers, or other private information, their network was compromised by a cybercriminal.

An attacker accessed Timehop and gained access to their systems without their permission.

3. Social Media Policy and Procedure missing or not being followed

Organizations Can Protect Themselves with a Sufficient Social Media Policy

Healthcare employees must be educated on potentially hazardous mistakes while using social media. Social Media can be a powerful tool for your office, but it starts with an implemented Social Media policy.

3. Social Media Policy and Procedure
missing or not being followed

The policy should:

- Instruct employees to post with caution: never post any pictures, stories, or status updates about what goes on in the office, especially if it involves patients who have not authorized the post (even then, proceed with caution).
- Advise employees to use extreme caution and sound professional judgment if permitted to utilize social media for work related purposes. For example, when posting a response to a question use limited information and suggest another communication method.
- Set expectations for when and how social media can be used.
- Provide steps to take if there is a suspected breach, risk of compromise, etc., on a Social Media platform. More on the importance of breach reporting later in this presentation.

4. Exclusion screenings not being performed correctly, or at all

Most healthcare professionals are aware of the Office of Inspector General (OIG) List of Excluded Individuals/Entities (LEIE).

However, exclusion list screening is not being performed correctly and for some providers, employees, vendors, etc., who should be – it is not happening at all.

Caution! It’s not a question of if, but when: if you employ or contract with excluded individuals or entities you will be subject to fines and penalties.

4. Exclusion screenings not being performed correctly, or at all

New This Year: CMS Preclusion List

The Centers for Medicare and Medicaid Services (CMS) has developed a tool associated with the Medicare Provider Enrollment Process effective

April 1, 2019.

The CMS Preclusion List includes providers and prescribers who are precluded from receiving payment for Medicare Advantage (MA) items and services or Part D drugs furnished
or prescribed to Medicare beneficiaries.

4. Exclusion screenings not being performed correctly, or at all

New This Year: CMS Preclusion List

CMS will make the Preclusion List **available to Part D sponsors and the MA plans** beginning **JANUARY 1, 2019**. EFFECTIVE **APRIL 1, 2019**:

- Part D sponsors will be required to reject a pharmacy claim (or deny a beneficiary request for reimbursement) for a Part D drug that is prescribed by an individual on the Preclusion List.
- MA plans will be required to deny payment for a health care item or service furnished by an individual or entity on the Preclusion List.

The Preclusion List will not be made available publicly. However, CMS will provide notification by email and follow up with a written notice through mail to the impacted provider in advance of his or her inclusion on the Preclusion List and their applicable appeal rights.

5. Failing to have implemented auditing and monitoring in place

One of Seven Components of a Compliance Program

The OIG, CMS, Plan Sponsors, and others have repeatedly stressed the importance of auditing and monitoring activities.

The confusion sets in for healthcare organizations understanding the difference between auditing and monitoring, as well as to who should be doing what and how often.

5. Failing to have implemented auditing and monitoring in place

Monitoring Includes

Think of Monitoring as regular reviews performed as part of normal operations, to confirm ongoing compliance.

This includes an ongoing process and method of detecting compliance risk issues associated with an organization's operations.

Means keeping current with changes in rules, regulations and applicable laws.

It includes monitoring policies and procedures and making sure your organization and employees are complying with them.

It also includes monitoring claims for accuracy – including documentation, proper billing, coding, etc.

5. Failing to have implemented auditing and monitoring in place

Auditing Includes

Auditing includes formal reviews of compliance, with particular set of standards as base measures.

Auditing entails reviewing the ongoing monitoring activities to verify their effectiveness.

Audits should be independent and objective – whether they are performed internally or externally.

For example, external auditors may be used to review your compliance program’s effectiveness; billing, coding and documentation accuracy; or an audit of systems to ensure there no physical or security risks.

5. Failing to have implemented auditing and monitoring in place

HCP Recommendations

Ultimately your Compliance Officer and Compliance Committee should ensure that both the monitoring and auditing is taking place and doing what is necessary to address (and improve) identified deficiencies.

We recommend both internal monitoring and auditing. From there, a baseline audit should be performed (preferably an external audit). Then, ongoing auditing should be performed, and determined by risk level or accuracy.

6. Mobile Devices - including lack of security, control over text messaging

Mobile Device Usage is Commonplace in Healthcare Facilities

Cell phones and other mobile devices are used by patients, employees, providers and others in waiting areas, and other areas in a healthcare facility.

Failure to have policies in place related to technology can lead to serious concerns pertaining to PHI and breaches.

6. Mobile Devices - including lack of security, control over text messaging

Consider the following OCR Settlement

Not too long ago, a judge ruled in favor of the OCR and ordered The University of Texas MD Anderson Cancer Center (Anderson Cancer Center) to pay over $4.3 million in civil monetary penalties.

The judgment came after the Anderson Cancer Center lost two unencrypted universal serial bus (USB) drives and an unencrypted laptop from the residence of an employee.

Anderson Cancer Center had previously identified the need for encryption on devices during a security-risk analysis and, despite having written policies outlining the need for encryption, failed to ensure that mobile electronic devices contained the appropriate security measures.

6. Mobile Devices - including lack of security, control over text messaging

Mobile Devices are Continually being used

Mobile devices present a unique challenge to the healthcare industry:

- On one hand, they are increasingly being used by medical providers including the use of voice-capture, email, text messaging, remote access to medical records systems and video conferencing.
- Smartphones, tablets, and laptops offer the means of streamlined communication and collaboration by making modern health IT solutions accessible and easy to use. USB drives make data storage and transfer effortless.
- On the other hand, despite the benefits of this technology, there are increased risks associated with mobile devices that are used to store or access ePHI.

6. Mobile Devices - including lack of security, control over text messaging

Organizations often fail to address risks and implement policies

Lost, misplaced and stolen portable devices are one of the leading causes of healthcare security breaches. Yet, organizations fail to address mobile devices as part of their risk assessment.

Policies and security measures are not implemented that address when and how they can be used. Additionally, the policies and measures may not consider all risks that could arise when using personal mobile devices such as to storage or access of ePHI. Yes, this includes the storage of text messages that contain PHI.

- If you choose not to allow mobile devices used, your policies must address that.
- If you do permit the use of mobile devices, there are several things to consider.
- Here are 10 of them…

10 TIPS Healthcare Organizations Should Consider

1. Implement policies and procedures regarding the use of mobile devices in the work place – especially when used to create, receive, maintain, or transmit ePHI.
2. Install or enable automatic lock/logoff functionality.
3. Require authentication to use or unlock mobile devices.
4. Regularly install security patches and updates.
5. Install or enable encryption, anti-virus/anti-malware software, and remote wipe capabilities.
6. Use only secure Wi-Fi connections.
7. Use a secure Virtual Private Network (VPN).
8. Reduce risks posed by third-party apps by prohibiting the downloading of third-party apps, unless the app has been approved.
9. Securely delete all PHI stored on a mobile device before discarding or reusing the mobile device.
10. Train all employees how to securely use mobile devices

6. Mobile Devices - including lack of security, control over text messaging

Organizations often fail to address risks and implement policies

Mobile devices present a unique challenge to the healthcare industry:

- On one hand, they are increasingly being used by medical providers including the use of voice-capture, email, text messaging, remote access to medical records systems and video conferencing.
- Smartphones, tablets, and laptops offer the means of streamlined communication and collaboration by making modern health IT solutions accessible and easy to use. USB drives make data storage and transfer effortless.
- On the other hand, despite the benefits of this technology, there are increased risks associated with mobile devices that are used to store or access ePHI.

7. Missing mechanisms for employee and patient complaints

Employee and Patient Complaints

The OIG has said for a compliance program to work, employees must be able to ask questions and report problems. The healthcare organization, board, or Compliance Committee of the organization should determine there is a process in place to encourage such constructive communication.

Yet, many organizations do not have mechanisms in place for employee complaints. In addition, patients are not advised of how to file a complaint and who to file a complaint with.

7. Missing mechanisms for employee and patient complaints

Mechanisms that Should be Considered

For patients, it often begins with the Notice of Privacy Practices (NPP). The notice should include language advising the patient he or she can complain if they feel their rights have been violated.

Under Section 1557, healthcare organizations should post a nondiscrimination as well as taglines of the top 15 languages in your state.

This notice must inform patients how and who to report a complaint with as well as how to obtain language assistance – if needed.

7. Missing mechanisms for employee and patient complaints

Consider a Hotline and/or Suggestion Boxes

The maintenance of a process, such as a hotline, to receive complaints and the adoption of procedures to protect the anonymity of complainants and to protect whistleblowers from retaliation is essential for a compliance program.

- A hotline and suggestion box can be for patients and employees
- Doesn't need to be used just for compliant purposes
- Hotlines and suggestion boxes can lead to ideas for an organization
- And many employees, providers, etc., receive compliments for a job well done

7. Missing mechanisms for employee and patient complaints

Don’t Forget Your Grievance Procedure

If Section 1557 applies to you and if you have 15 or more employees, you must designate a responsible employee as your organization’s Section 1557 coordinator to investigate grievances.

This includes investigating when any person who believes someone has been subjected to discrimination on the basis of race, color, national origin, sex, age or disability has filed a grievance under the Section 1557 Procedure.

We have sample notifications available in our forms library for our clients so that they can comply with all Section 1557 requirements.

8. Failing to implement regular, effective education and training programs

Effective Training and Education

During our discussions with healthcare organizations across the country, we learn how many do not have an effective training and education program.

An effective training and education program is one of the seven fundamental elements of an effective compliance program.

What types of training should be included?

8. Failing to implement regular, effective education and training programs

OIG Recommendations for Determining Training Needs

According to the OIG, education is an important part of any compliance program and is the logical next step after problems have been identified and the practice has designated a person to oversee educational training.

Training and education programs should be tailored to the healthcare organization's needs, specialty and size and will include both compliance and specific training (e.g., on policies and procedures).

- Determine who needs training.
- Determine the type of training that best suits the practice's needs.
- Determine when and how often education is needed and how much each person should receive.

8. Failing to implement regular, effective education and training programs

A Basic Outline of What Most Healthcare Organizations Need

1. **Training on Policies and Procedures:** at time of hire, when there are updates, and reviewed annually thereafter.
2. **HIPAA Privacy and HIPAA Security Training:** at time of hire, when there are updates, and refresher training annually thereafter.
3. **Corporate Compliance Training (i.e., code of conduct, FWA, etc.):** at a minimum anyone involved in the claims process (including front office, back office, admin, etc.) at a minimum should be trained at time of hire, when there are updates and annually thereafter.
4. **OSHA:** at time of hire, when there are updates, and refresher training annually thereafter.
5. **Additional relevant training topics including:**
   - Harassment and Discrimination
   - Active Shooter
   - CLIA training (if applicable)
   - And others

9. Not tracking or reporting suspected breaches or other incidents

OCR Settled with Presence St. Joseph Medical Center for $475,000

This was OCR's first case against a healthcare organization for unreasonably delay in reporting a HIPAA breach.

- Presence St. Joseph Medical Center discovered that its paper-based operating schedules were missing from its surgery center.
- The schedules contained PHI of 836 individuals, including names, birthdates, procedure information, and medical record information.
- Because the breach involved more than 500 individuals the breach should have been reported to HHS and local media when they notified affected individuals.
- However, due to a mis-understanding by their workforce members, the breach was not reported to HHS, to the media or affected individuals until over 100 days after the breach was discovered.

9. Not tracking or reporting suspected breaches or other incidents

By Definition

A breach is: an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information (PHI).

- An impermissible use or disclosure of PHI is presumed to be a breach unless the healthcare organization demonstrates that there is a low probability that the PHI has been compromised.
- Or has determined an exception of a breach applies.

9. Not tracking or reporting suspected breaches or other incidents

Reporting Requirements

If you experience a HIPAA breach affecting 500 or more individuals it is critical the breach is investigated, mitigated (as much as possible) and reported "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach."

Less than 500 affected individuals, you have more time to report to HHS (within 60 days of the end of the calendar year in which the breach was discovered).

What's important is making sure have followed the breach notification rule requirements without unreasonable delay.

Failing to do so, is a serious compliance issue that could result in significant HIPAA fines and result in an extensive corrective action plan for your organization.

10. Compliance program deficiencies and/or findings not being communicated or corrected

Involve Compliance Committee, Board & Other Relevant Employees

It's a common issue for Healthcare Organizations not fully know how to when it comes to develop and measure their compliance program with benchmarks and measurable goals.

- The success of a compliance program involves communication of risks to the organization, audit results, and any investigations.
- Buy-in, involvement and feedback from the Compliance Committee, then communicating to the Board or Relevant employees, is key for meeting the goals of the organization and assessing whether the compliance program has sufficient support or funding.

10. Compliance program deficiencies and/or findings not being communicated or corrected

Importance of a Corrective Action Plan

Correcting identified deficiencies is critical for the success of a compliance program. For example, as part of your organization’s risk analysis or a billing and coding audit you may identify opportunities for improvement.

- During a risk analysis, it may be missing policies or procedures or a lack of safeguards
- During a billing and coding audit you may find providers are not documenting enough to support codes being submitted

In Conclusion:

Not too long ago, when the DOJ Criminal Division published their guidance titled ***"The Evaluation of Corporate Compliance Programs,"*** Assistant Attorney General Brian A. Benczkowski said:

"Effective compliance programs play a critical role in preventing misconduct, facilitating investigations, and informing fair resolutions."

In Conclusion:

The 10 TIPS Healthcare Organizations Should Consider we discussed today are essential elements to of an effective compliance program.

Each of the **10 TIPS** help you, in the event of an investigation, to demonstrate your program is well-designed, effectively implemented and works in practice.

Now’s your chance, ask away…

Too shy? You can also:
Call me at 855-427-0427 or
Email me: chad@hcp.md

hcp | Healthcare Compliance Pros