HIPAA COMPLIANCE CHECKLIST

Copper Penny Consulting, LLC

Where Do I Start?

With thousands of pages of regulation, it can be confusing to know how to start or maintain a HIPAA program in a practice. So, where do you start?

Start by realizing that you can't do everything at once, but you can focus your time and finances on the biggest threats first and make continuous improvements over time.

Instead of overwhelming yourself with trying to do everything at once, let's break it down into manageable items that you can tackle.
In it's simplest form, HIPAA can be broken down into three aspects: People, Process and Technology. In each of these categories, you must decide what is reasonable and appropriate for your practice. Keep in mind that "reasonable and appropriate" doesn't mean to never implement because you don't want to pay for it. In some cases, you may be able to offset a risk in the interim in another way until you can correct the vulnerability properly.

This is in no way a comprehensive list, and you should consult with a HIPAA professional, but this checklist is a good place to start thinking about some of the risks and vulnerabilities in your practice.

Copper Penny
Consulting, LLC

01

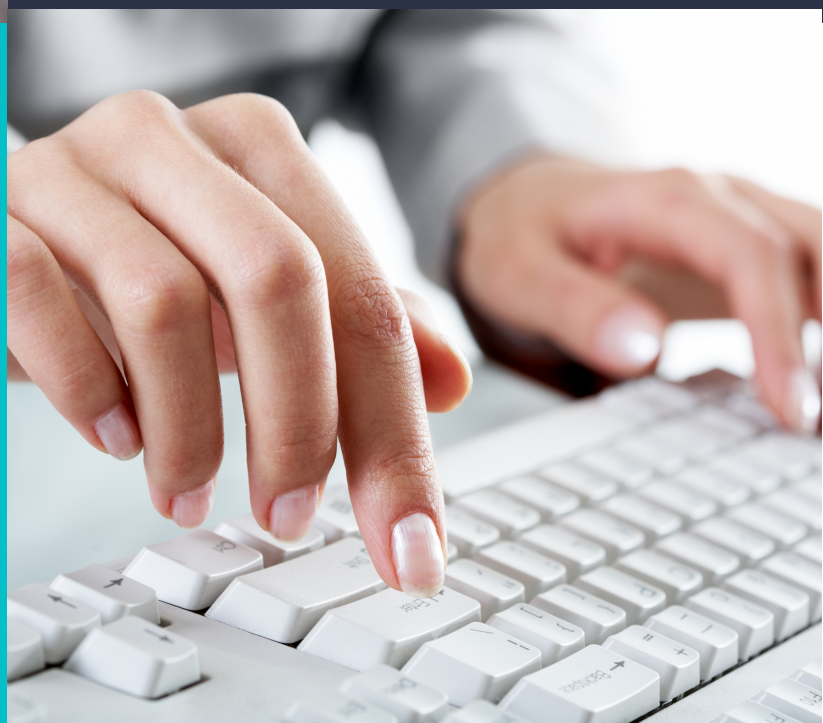
PEOPLE

02

PROCESS

03

TECHNOLOGY



PEOPLE

01

Choose a HIPAA Officer or HIPAA Officers

Often times in smaller practices, one person is both Privacy and Security Officer and has support from a HIPAA Consultant and IT Provider.

- [ ] Choose Privacy Officer
- [ ] Choose Security Officer
- [ ] Train Officer(s)

02

Workforce Training

- [ ] All employees and doctors must be trained annually.
- [ ] All new employees must be trained prior to being provided access to computers or paper files containing Protected Health Information.
- [ ] Training must include Privacy, Security and Cybersecurity information

03

Minimum Necessary

- [ ] All workforce members must adhere to the Minimum Necessary standard.
- [ ] Modify user settings within Practice Management program for job role.
- [ ] Train users on written policy and enforcement.

04

Business Associates and BAA's

- [ ] Make a list of all Business Associates (vendors and contractors that create, receive, maintain or transmit Protected Health Information).
- [ ] Vet all Business Associates to ensure they will properly safeguard your Protected Health Information.
- [ ] Review and sign a Business Associate Agreement with each Business Associate prior to granting access to your practice or computer systems.

05

Risk Analysis and Security Risk Assessment

- [ ] Perform an annual Risk Analysis or hire a professional to perform a Risk Analysis that includes the following:
    - [ ] Security Risk Assessment
    - [ ] Business Associates
    - [ ] Privacy

PROCESS

01

Polices & Procedures

- [ ] Create and implement HIPAA Polices and Procedures, including a Sanction Policy.
- [ ] Have all workforce members review policies and procedures.

02

Notice of Privacy Practices

- [ ] Implement current Notice of Privacy Practices in English and Spanish. Model template found here: **https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html**.
- [ ] Provide Notice of Privacy Practices to new patients at their first appointment.
- [ ] Have patients sign Acknowledgement of Receipt of Notice of Privacy Practices.
- [ ] Upload Notice of Privacy Practices on your website.

03

Consent

- [ ] Implement a photo consent for education, study clubs, social media and in-office reproductions of patient photos.

04

Communication

- [ ] While HIPAA typically covers communication as part of Treatment, Payment and Operations, various state laws have additional laws surrounding email and cell phones. If your state requires, utilize a Communication Consent form to ensure you are allowed to call a cell phone, leave a voicemail, email, text and with whom you can communicate with on behalf of the patient.

05

Voicemail

- [ ] Check with your state laws to ensure you obtain proper consent to leave voicemail, especially on cell phones.
- [ ] Utilize the Minimum Necessary Rule when leaving voicemail.

TECHNOLOGY

01

IT Security

- [ ] Minimum IT Standard Of Care: Anti-virus, Backups, Firewall and Patching.
- [ ] Adding new programs should be done by IT.
- [ ] Decommissioned computers, servers and devices should be properly sanitized for re-use or disposal.

02

Email

- [ ] Utilize an encrypted email.
- [ ] Ensure your inbox is properly protected for any unencrypted emails that may be sent to you.
- [ ] Train all workforce members on how to properly utilize encrypted email.

03

Passwords

- [ ] All workforce members must adhere to your password policy.
- [ ] Utilize a password manager that separates users.
- [ ] Use different passwords at work and home.
- [ ] Minimum standards for passwords:
    - [ ] 8-12 characters
    - [ ] Upper & Lower Case
    - [ ] At least one symbol
    - [ ] Avoid: kids, spouse, pets names, address, phone number, birthdates, etc.

04

Encryption

- [ ] Encrypt server.
- [ ] Encrypt laptops.
- [ ] Encrypt cell phones.
- [ ] Encrypt portable backup drives.
- [ ] Encrypt thumb drives/USB sticks.

05

Devices

- [ ] Devices should be reviewed to ensure security.
- [ ] IoT, or Internet of Things devices should be reviewed for security vulnerabilities prior to installation.
- [ ] Wifi Segmentation should be implemented for each device.
- [ ] Defer to IT for installing devices.

Copper Penny
Consulting, LLC

CYBERSECURITY

01

Scams

Scams come in many shapes and sizes. There is no single type of scam. Users need to be made aware of different types of scams that can affect your practice.

02

Email Scams

- Check to see if the email is who you think it's from.
- Hover your mouse over the link to see where the link actually goes.
- Be wary of email attachments if the email looks off.
- Involve IT if you are unsure.

03

Phone Scams

- Be aware of phone scams asking to log in to your computer.
- Be aware of phone scams asking for money or sensitive information.

04

Social Media

- Ensure you have consent from patients before posting photos.
- Be cautious of friend requests that are duplicates or unknown people.
- Limit connecting with patients on personal social media pages.

05

Ransomware

Ransomware, a form of computer malware is rampant in all businesses, especially small healthcare practices.

- Train all workforce members to know what to look out for in email attachments to prevent ransomware.
- Test backups to ensure your expectations align with how your backups perform. Upgrade to newer types of on-site and off-site backups if necessary.
- Obtain Data Breach/CyberLiability/CyberCrime Insurance.

Copper Penny
Consulting, LLC