CHECKLIST

securitymetrics®

HIPAA Compliance in a Year

Never have a false sense of security.™

> HIPAA Compliance should be an ongoing process and effort. This suggested handout divides HIPAA Compliance into monthly tasks, so you can pace your HIPAA efforts year-round.

Table of Contents

Note

This handout aims to assist those who are new to HIPAA compliance. This suggested guideline aims to direct and organize your HIPAA tasks into a year-round task list. This is not a comprehensive handout, and HIPAA compliance should be addressed based on how your organization handles PHI.

01

JANUARY

Identify PHI

HIPAA compliance begins with identifying how PHI flows in and out of your organization and documenting your findings. Create inventories and diagrams that document how PHI is created, stored, transmitted, or received in your organization.

- [ ] **Find where your protected health information (PHI) is located by identifying:**
  - [ ] All processes your data goes through
  - [ ] Computers your data sits on
  - [ ] Everyone who touches your data
  - [ ] Any technology that has access to your data
- [ ] **Interview every department that touches PHI in any way, including third parties**
  - [ ] Talk to different people within each department
  - [ ] See if they can uncover processes and technologies that no organization chart, tool, or previous data analysis can expose
- [ ] **Identify and document:**
  - [ ] How data enters your environment
  - [ ] Where it goes after entering the environment
  - [ ] Where it's stored:
    - [ ] If it's sent off to a third party
    - [ ] If it's printed and stored
    - [ ] If it's recorded straight into the electronic health record (EHR) system
  - [ ] Workforce members who can extract PHI from the EHR system
  - [ ] How employees store PHI after they download it from the EHR system
  - [ ] How data is encrypted in every place it is stored, even temporarily
- [ ] **Ensure you understand how technology and personnel affect PHI by documenting every:**
  - [ ] Network device
  - [ ] Server

↑ Table of Contents

- [ ] Medical device connected to the Internet
- [ ] Workstation
- [ ] Mobile device (tablet/laptop/smartphone)
- [ ] Employee BYOD smartphone used to interact with PHI

- [ ] **Document what you've learned and consider:**
  - [ ] Drawing diagrams
  - [ ] Making lists
  - [ ] Recording the who, what, when, where, how, and why of your PHI

- [ ] **Process and organize your PHI information by:**
  - [ ] Crafting a PHI flowchart for each different PHI flow

- [ ] **Ensure your PHI flowchart documents every instance in your environment where PHI could:**
  - [ ] Enter
  - [ ] Exist
  - [ ] Exit

FEBRUARY

02 Conduct a Risk Assessment

With your intimate knowledge of your systems, technologies, and processes (from January), locate the risks, threats, and vulnerabilities that currently exist in your organization to create your HIPAA Risk Analysis.

- [ ] **Analyze these questions to locate problem areas:**
  - [ ] What vulnerabilities exist in your systems, applications, processes, or people?
  - [ ] What threats exist for each of those vulnerabilities?
    - [ ] Internal
    - [ ] External
    - [ ] Environmental
    - [ ] Physical

↑ Table of Contents

- [ ] What is the probability of each threat triggering a specific vulnerability?
- [ ] Do you use the cloud?
  - [ ] What are the implications there?
- [ ] How are physical copies of PHI stored?
- [ ] Is encryption implemented throughout the entire organization?
- [ ] Do third parties use multi-factor authentication when using remote access into your environment?
- [ ] When employees leave workstations, do they turn on a password-protected screensaver?

- [ ] **Capture each vulnerability, recording:**
  - [ ] Potential impact
  - [ ] Probability
  - [ ] Risk rankings resulting from probability and impact
- [ ] **Document your entire process using a known risk assessment framework, such as FAIR, OCTAVE, or NIST 800-30**

03

MARCH

Create a Risk Management Plan

Your risk management plan should address prioritized risks discovered during your risk assessment. Spend February crafting a thorough risk management plan by working with your directors, IT, security administrators, and anyone else who should be involved.

- [ ] **As you prioritize, ask yourself:**
  - [ ] What are the most critical parts of your risk management plan?
  - [ ] Which vulnerabilities are most likely to be exploited this year?
  - [ ] Where are our highest threats?
- [ ] **Pick the top five problems at your organization**
  - [ ] Resolve these issues first
- [ ] **Remediate the rest of your threats and vulnerabilities**

↑ Table of Contents

APRIL

04 Start Regular Employee Training

Workforce members are the front line of healthcare security. Successful security training and awareness programs help people do their jobs in a way that doesn't lead to a breach of patient information.

- [ ] **During your planning phase, consider these recommendations:**
  - [ ] Tailor training to be relevant to specific roles
  - [ ] Require training before workforce members access PHI
  - [ ] Implement small, regular training sessions throughout the year
  - [ ] Place security reminders near where errors might occur, such as email banners reminding employees not to click on links
- [ ] **Decide how often you'll train employees and which methods you will use**
- [ ] **Schedule workforce member training sessions**
- [ ] **Document your employee training**

MAY

05 Create an Incident Response Plan

With a better understanding of the most likely scenarios for your environment, you can personalize your incident response plan. Even if you already have an incident response plan, you can update it with your current systems, processes, and assigned personnel.

- [ ] **Use the information gleaned from your risk analysis and risk management plan to create your incident response plan**
- [ ] **Ensure your employees are properly trained regarding their incident response roles and responsibilities in the event of a data breach**
- [ ] **Develop incident response drill scenarios**
  - [ ] Regularly conduct mock data breaches to evaluate your incident response plan
- [ ] **Ensure that the elements of your incident response plan (training, execution, hardware and software resources, etc.) are:**
  - [ ] Approved by your organization
  - [ ] Funded in advance

↑ Table of Contents

- [ ] **Record answers to these questions if breached:**
  - [ ] When did the event happen?
  - [ ] How was it discovered?
  - [ ] Who discovered it?
  - [ ] Have any other areas been impacted?
  - [ ] What is the scope of the compromise?
  - [ ] Does it affect operations?
  - [ ] Has the source (point of entry) of the event been discovered?
- [ ] **Disconnect affected devices from the internet**
- [ ] **Devise a prevention plan for the future**
- [ ] **Update and patch your systems**
- [ ] **Review your remote access protocols**
- [ ] **Change all user and administrative access credentials**
- [ ] **Harden all passwords**
- [ ] **Find and eliminate the cause of your breach**
  - [ ] Securely remove malware
  - [ ] Ensure no trace of malware remains
- [ ] **Restore and return affected systems back into your business environment**
- [ ] **Answer these questions to ensure you make a full recovery**
- [ ] **When can systems be returned to production?**
  - [ ] Have systems been patched, hardened and tested?
  - [ ] Can the system be restored from a trusted back-up?
  - [ ] How long will the affected systems be monitored and what will you look for when monitoring?
  - [ ] What tools will ensure similar attacks will not reoccur? (e.g., File integrity monitoring, intrusion detection/protection)

↑ Table of Contents

- [ ] **Develop realistic example situations using these questions:**
  - [ ] What types of security precautions are in place?
  - [ ] What is the protocol if an employee suspects a data breach?
  - [ ] Internally and externally, who should be notified if an incident occurs?
  - [ ] Do employees know their responsibilities before, during, and after an incident?
  - [ ] What if a co-location or business associate is involved in the incident?

JUNE

06 Get Business Associates On Board

Follow up with every third party that could potentially impact the security of your patient data by having them sign a business associate agreement (BAA) containing language specified in the HIPAA regulations.

- [ ] **Implement or update your BAA template to make sure it follows the language outlined by HHS, which in general:**
  - [ ] Establishes the permitted and required uses and disclosures of PHI
  - [ ] Provides that the BA will not use or disclose PHI other than as permitted or required by the contract or by law
  - [ ] Requires the BA to implement appropriate safeguards to prevent unauthorized use or disclosure of the information
  - [ ] Requires the BA to report to the covered entity any use or disclosure of the information not provided for by its contract, including breaches
  - [ ] Requires the BA to adhere to additional requirements specified in the regulations
- [ ] **Follow up with business associates on the state of their HIPAA compliance**
- [ ] **Establish policies and procedures requiring due diligence prior to engaging with new business associates to make sure they will protect PHI and comply with HIPAA**

↑ Table of Contents

07

JULY

Update Policies

To maintain HIPAA compliance, update your current policy and procedure documentation, and ensure employees are appropriately trained.

- [ ] **Update your breach notification policies by including documentation of:**
  - [ ] Members and contact information of your breach response team
  - [ ] State and federal breach response laws
  - [ ] Who to notify in case of a breach (e.g., stakeholders, the HHS, law enforcement, patients, and the public)
  - [ ] Response timelines
- [ ] **Update your security policies in your business plan by including:**
  - [ ] Firewall configuration standards
  - [ ] Job descriptions
  - [ ] Network time protocol (NTP) configuration procedures
  - [ ] Physical security procedures
  - [ ] Security awareness training procedures
  - [ ] Workstation functions
- [ ] **Update your privacy policies in your business plan by including (as applicable):**
  - [ ] Accounting of disclosures of PHI
  - [ ] Patient access to PHI
  - [ ] Authorization for release of PHI
  - [ ] Minimum necessary for uses and disclosures of PHI
  - [ ] Safeguarding and storing PHI
  - [ ] Destruction of PHI
- [ ] **Ensure your employees are appropriately trained to follow policies and procedure**

↑ Table of Contents

- [ ] **Review policies on a regular basis and ensure they are updated with:**
  - [ ] System
  - [ ] Personnel
  - [ ] Technology changes

08
09

AUGUST & SEPTEMBER

Test Your Employees

The best way to analyze the effectiveness of your security training program is through employee testing to learn how your employees respond to security threats in a controlled environment.

- [ ] **Complete a Social Engineering training:**
  - [ ] Hire an ethical social engineer (or third party agency) to see if employees will question or report someone who doesn't belong in their work environment
    - [ ] Record how your employees react
  - [ ] Document your results by answering the following questions:
    - [ ] How was the test conducted?
    - [ ] Who participated in the test?
    - [ ] When was the test conducted?
- [ ] **Complete phishing training:**
  - [ ] Ask your IT team (or hire a third party) to create a fake phishing email
  - [ ] Send your staff the fake phishing email
  - [ ] Track the number of people who fall for the phishing email
  - [ ] Document your results by answering the following questions:
    - [ ] How was the test conducted?
    - [ ] Who participated in the test?
    - [ ] When was the test conducted?

↑ Table of Contents

- [ ] **Create a future plan to mitigate the results from both of your tests**
  - [ ] When you test workforce members on security topics, gaps in their knowledge should be used to improve your program, not punish the learner
- [ ] **Consider outlining the statistics of your training to present to your board of directors**

10

OCTOBER

Test Your Incident Response Plan

Through comprehensive testing, you'll be able to answer the question that really matters: does your incident response plan actually work?

- [ ] **Schedule a day to test your incident response plan**
- [ ] **Use the scenarios developed previously to test for:**
  - [ ] How your employees work together
  - [ ] How your employees make decisions in stressful situations
  - [ ] How fast your employees resolve issues
  - [ ] If your employees follow your plan and policies
- [ ] **Document both failures and successes during your test**
- [ ] **Use your results to adjust your incident response plan or training as needed**

11

NOVEMBER

Evaluate Your Technical Security

Performing automated/manual scans and penetration tests can help you identify and remediate issues as they appear.

- [ ] **Conduct regular vulnerability scans**
- [ ] **Research penetration testing providers**

↑ Table of Contents

- [ ] Choose a pentester by verifying that:
  - [ ] They follow industry best practice standards
  - [ ] They communicate their testing methodologies
- [ ] **Consider using this Penetration Testing Timeline**
- [ ] **Determine your pentest date by answering these questions:**
  - [ ] Is the pentest starting early enough to leave time for remediation later?
  - [ ] Is this during a busy time of the year?
  - [ ] Will office operations be interrupted?
  - [ ] How much notice should we give everyone?
- [ ] **Conduct a penetration test**

12

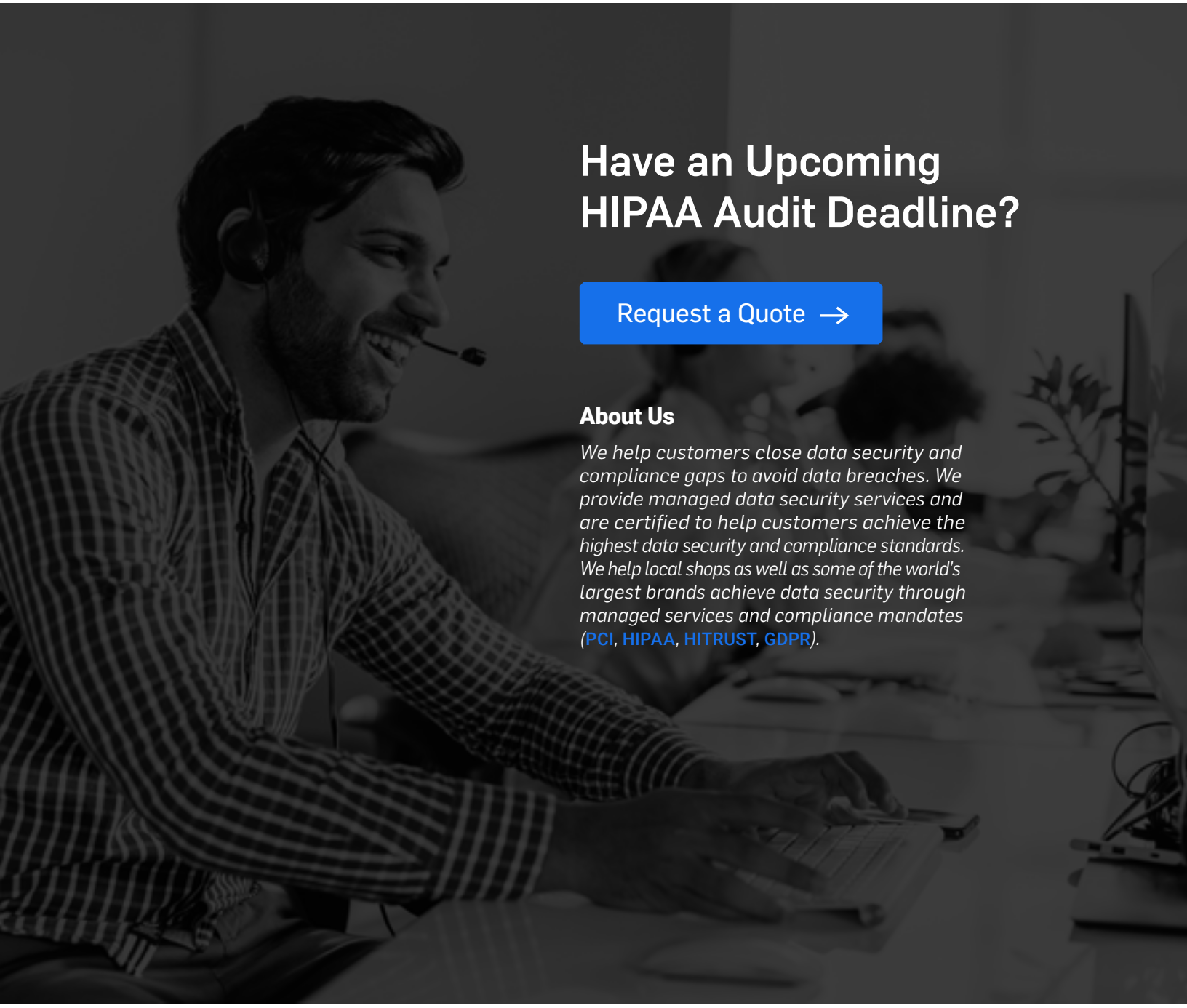
DECEMBER

Assess Your Process

HIPAA is not just an annual process but an ongoing one. Your HIPAA compliance should be reanalyzed every year and updated continuously based on changes in your organization.

- [ ] **Assess where you are and how far you've come**
- [ ] **Set HIPAA goals and milestones for next year**
- [ ] **Plan out employee training based on risks and vulnerabilities you found during your risk assessment this year**
- [ ] **Remember to document your plans for next year**

↑ Table of Contents



Have an Upcoming HIPAA Audit Deadline?

Request a Quote →

About Us

We help customers close data security and compliance gaps to avoid data breaches. We provide managed data security services and are certified to help customers achieve the highest data security and compliance standards. We help local shops as well as some of the world's largest brands achieve data security through managed services and compliance mandates (PCI, HIPAA, HITRUST, GDPR).

↑ Table of Contents