# HIPAA Compliance Checklist



#### 19 Steps to Ensure Cybersecurity Compliance



#### **Delegate**

Assign HIPAA compliance, privacy, and security responsibilities.



## Risk Assessments

Perform PHI data security risk and HIPAA compliance risk assessment.





#### **Gap Analysis**

Perform gap analysis and identify gaps in PHI security and patient privacy.





#### 4 Remediations

After the gap analysis, prioritize remediation targets.





#### Add Safeguards

Deploy administrative, physical, and technical safeguards utilizing a security framework such as NIST CSF to protect the ePHI from unauthorized access.

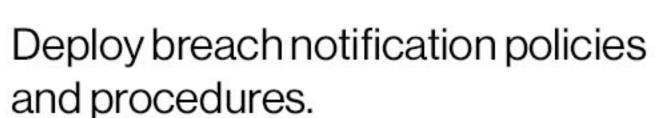


# Privacy Process Implementation



Deploy privacy policies and procedures.







#### DID YOU KNOW?

2019 Saw more HIPAA data breaches than any previous year

Breaches went up over 37% from the previous year, and trends show they are on the rise.



### **HIPAA Training**

Ensure that a HIPAA compliance officer provides annual HIPAA training for all personnel.



Personnel



Incident & **Breach Training** 

Provide annual incident response and

breach response training to all personnel.



# Stay Up-to-Date

Provide periodic security and privacy updates.



#### **12** Access Controls

Ensure HIPAA policies and procedures

are documented, disseminated, and

acknowledged by all personnel.



Monitor ePHI access logs regularly and deploy controls to detect unauthorized PHI access.

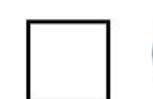








Retain all policies and procedures documentation for at least six years from the date of creation or the date when policies were put into effect, whichever is later.



#### 15 Privacy Notices



At least once in three years, inform all individuals covered by the entity of the individual's rights, availability of privacy notice, and on how to obtain the document.



#### PENALTIES

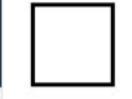
Perform vendor due diligence and

enact an annual review of vendor

and business.

2019 Saw more HIPAA data breaches than any previous year

Breaches went up over 37% from the previous year, and trends show they are on the rise.



### 16 PHI Storage

Retain all forms of PHI for at least six years.

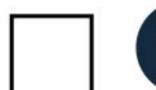


**PHI Email** Storage

six years.



Retain emails containing PHI for at least



# 18 Emergency Plans

Perform vendor due diligence and enact an annual review of vendor and business.



## 19 Annual Audits



Perform annual HIPAA compliance audits to ensure you are still compliant, present systems are working, and to avoid breaches.

#### HIPAA ADVISORY SERVICES

Patient data protection and privacy is critical to your business. Get advised on compliance, audits, vulnerability scanning, and internal procedures and training.