GIVA'S ULTIMATE 10-STEP HIPAA COMPLIANCE CHECKLIST

HIPAA compliance is a necessity and legal requirement for any business and organization in the US healthcare sector. Having a quick-reference HIPAA compliance checklist will save you time, money, and a lot of worry.

It's strategically smarter, more cost-efficient, and a legal necessity to ensure you're HIPAA compliant. The alternative is risking fines, lawsuits, and being unable to work with other organizations in the healthcare sector.

Giva's Free 10-Step HIPAA Compliance Checklist

To ensure your organization is compliant, here is Giva's ultimate 10-point HIPAA compliance checklist for covered entities and business associates.

1. Privacy Rule

Does the HIPAA Privacy Rule affect your business?

Do you handle Protected Health Information (PHI) (in any form) directly, indirectly, verbal, electronic records, or written?

Business associates handling PHI are unlikely to have direct access to patients. So, adhering to the privacy rule should be covered by your Business Associate Agreement (BAA) with the covered entity. But, covered entities are not responsible (nor are they mandated to under HIPAA) for how you handle and safeguard patient data.

This means that ensuring HIPAA compliance is on you! You can quickly lose your business clients and risk fines and lawsuits if you fail to comply and adequately safeguard patient data.

Adhering to the Privacy Rule means having certain policies and procedures in place. Here are a few examples:

- A defined record-set policy
- Notice of privacy practices
- Authorization for disclosure policy
- Annual verification and HIPAA compliance reviews under the BAA with covered entity clients

2. *Security Rule*

Complying with the HIPAA Security Rule involves numerous other safeguards (administrative, physical, technical), and we cover these below. At the highest level, adhering to the security rule means ensuring the following is in place:

- A password creation and usage policy
- An access management policy, especially when it comes to any software or databases that contain patient data (PHI)
- 24/7 data backups and a disaster recovery policy

3. *Breach Notification Rule*

In the event of a data breach, covered entities and business associates need policies and procedures to notify those affected. This can include patients (data subjects) and any other organizations or vendors in the supply chain.

In practice, this means having the following in place:

- Incident response policy
- Mitigation policy
- Patient (PHI) notification policy
- Internal notification policy

4. *Business Associate Agreement for PHI Access*

As we covered above, a business associate is anyone, including vendors and other businesses, that has access to, or handles in any way, protected healthcare data (PHI).

Covered entities should always have Business Associate Agreements (BAA) in place for any new business relationship. At the same time, business associates that work with other vendors should also have them sign BAAs if they come into contact with PHI, even in a small way.

This way, every organization and vendor in the supply chain is compliant with HIPAA. Make sure you have:

- BAAs with any covered entity organizations or professionals you work with
- BAAs with any other vendors and professionals that have any kind of access to PHI

5. *Implement Administrative Safeguards*

Administrative safeguards include implementing the following:

- HIPAA-compliant data security risk assessments
- A designated person assigned to take responsibility for PHI data privacy and HIPAA compliance
- Mandatory HIPAA compliance staff training on patient data (needs to be renewed annually and given to any new staff)

6. *Implement Physical Safeguards*

Although cybersecurity is a serious concern, data breaches can and do happen when staff access systems physically and either misuse or steal data. Threats can be internal as well as external. Criminals may also attempt physical break-ins to steal data too, although these risks are much lower these days.

Safeguarding data for any eventuality means having the following in place:

- An alarm system
- Auditable keycards and access fobs for authorized personnel only
- Internal security systems, including cameras with cloud-based, encrypted recordings and 24/7 monitoring
- More advanced security for any physical access areas on-site where PHI data is stored (e.g., biometric security)
- If data is stored with vendors, they must be HIPAA compliant under a BAA, especially regarding physical, technical, and administrative safeguards and security systems

7. *Implement Technical Safeguards*

Technical safeguards are just as important. You need to implement the following to ensure HIPAA compliance:

- Data encryption systems and specific guidelines
- Multi-layered (external and internal) antivirus software
- Data protection audit controls
- Automatic log-off on devices

8. *Perform Multi-layered HIPAA Risk Assessments*

Before and after implementing HIPAA compliance, conduct physical, administrative, and cyber-based risk assessments and tests. You need to know:

- What are your vulnerabilities?
- How can you mitigate these risks and reduce them?

9. *Train Employees on HIPAA Compliance*

One area organizations risk falling short of is employee training. Staff and contractors with access to data need training to ensure they are meeting and understand HIPAA compliance requirements.

This is not something you can make a plan for and forget about. It needs someone to take ownership of training, onboarding new staff, and ensuring employees who are leaving cannot take any sensitive data with them.

Make sure you have the following in place:

- HIPAA compliance training for new employees
- HIPAA data access controls to prevent employees who are leaving from taking any sensitive data
- Annual HIPAA refresher training for all staff, including senior leadership
- HIPAA policies, training, and audit trails for any temporary or contract-based staff

10. *Ensure Continuous, Automated & Manual HIPAA Compliance Checks Are Performed*

Once everything is in place, ensure you have software and processes to implement continuous automated and manual compliance checks, including:

- Cybersecurity software to scan for external and internal data breaches
- Data audit software so you can see exactly who has access to data, how long it was accessed, and that it was retained on a secure work device (e.g., not forwarded or sent to a personal email)
- A manual review process on data audit trails to ensure compliance is being achieved consistently. This also verifies electronic records.

What is HIPAA Compliance?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was rolled out in several stages by the US government and is overseen and managed by the Department of Health and Human Services (HHS).

HIPAA was designed to "improve the efficiency and effectiveness of the health care system." This was needed with new advances in software in the medical sector that simplified the sharing of patient data. Congress realized that, despite numerous upsides, this meant patient data needed safeguarding and protection. Safety measures would include human, deliberate misuse or electronic interference, such as data breaches, cyberattacks, etc.

Hence, the implementation of HIPAA and the need for HIPAA compliance by any organization, professional, or business associate (a non-medical company that handles, stores, or processes patient data). HIPAA protects and safeguards Protected Health Information (PHI), also known as sensitive patient data.

HIPAA includes several core rules that are codified under the original act:

The Privacy Rule: Published December 2000, with compliance required since April 2003;

The Security Rule: Published February 2003, with compliance required since April 2005;

The Enforcement Rule: Published to simplify all of the associated administrative rules;

A final Omnibus rule that further simplified and aligned HIPAA with the HITECH Act, and incorporated the Breach Notification Rule.

It's worth taking a look at this to understand HIPAA compliance better: View the Combined Regulation Text - PDF (as of March 2013).

Why Your Organization Needs a HIPAA Compliance Checklist

HIPAA compliance is required for two types of businesses: covered entities and business associates. We will explain more about these next.

HIPAA compliance is mandatory if you handle PHI. Failing to comply with HIPAA legislation, laws, and rules means you risk incurring fines for breaches from the Department of Health and Human Services (HHS).

Alongside these fines, the Office of Civil Rights (OCR) can issue fines, too, and you would end up on OCR's "Wall of Shame”. Not only is this bad for business, it means you would risk gaining access to any more patient data from healthcare providers. Patients could also take civil actions, suing for damages, and this could cause serious reputational damage.

What is a HIPAA Covered Entity?

A "Covered Entity" under HIPAA is any organization or medical professional responsible for treating patients or is connected to them directly, including but not limited to:

- Doctors
- Nurses
- Dentists
- Hospitals
- Chiropractors
- Primary Care Clinics
- Pharmacies
- Psychologists
- Psychiatrists
- Healthcare providers
- Healthcare insurance companies

What is a HIPAA Business Associate?

Because the healthcare sector is vast, with thousands of service providers, many of whom have access to PHI — directly and indirectly, even if it's on secure encrypted, cloud-based servers and software — these organizations are also required to implement HIPAA compliance:

Business associates include (but are not limited to):

- Software providers (SaaS) with healthcare clients
- Hardware and cloud service providers with healthcare clients
- Data storage providers
- Billing and payment processing companies
- Attorneys with patients who are clients
- Attorneys with healthcare sector clients
- CPA and other businesses with access to PHI under HIPAA

Giva is HIPAA Compliant

Giva's HIPAA-compliant cloud help desk software protects electronic health & medical records. [Discover how Giva exceeds the key elements of HIPAA compliance]().

ABOUT GIVA

Founded in 1999, Giva was among the first to provide a suite of help desk and customer service/call center applications architected for the cloud.

Now, with hundreds of customer driven releases, the Giva Service Management™ Suite delivers an intuitive, easy-to-use design that can be deployed in just days and requires only one hour of training. Giva's robust, fast and painless reporting/analytics/KPIs quickly measure team productivity, responsiveness and customer satisfaction resulting in faster and higher quality decision-making. Customization and configuration are all point and click with no programming or consultants required to deliver a substantially lower total cost of ownership.

Giva is a private company headquartered in Sunnyvale, California serving delighted customers worldwide.

robust, fast & painless reporting for higher quality decision-making
deploy in days, train in 1 hour
highly customizable without programming or consultants
the Giva difference