HIPAA & GDPR Compliance:

Your Checklist for Building a Robust Data Protection Framework

Where do **our sensitive data** flows start and end?

What are the **key security requirements**?

How are **HIPAA** and **GDPR** different?

Do we need to comply **with both** - or **just one**?

HIPAA & GDPR Compliance: Your Checklist for Building a Robust Data Protection Framework

Many companies run into the same roadblocks:

- ❌ Not enough in-house expertise
- ❌ Tight budgets for GDPR/HIPAA compliance projects
- ❌ Unclear which documents and tools are actually required
- ❌ No solid system in place to monitor ongoing compliance.

ℹ️ This checklist is your practical roadmap to navigate both regulations — helping you identify risks, strengthen processes, and build a privacy culture that keeps your data (and reputation) safe and effective.

HIPAA

HIPAA (Health Insurance Portability and Accountability Act) is a US federal law that sets national standards for protecting medical information — known as Protected Health Information (PHI).

Who it's for:

🏥 **Covered Entities:** healthcare providers, health plans, and clearinghouses.

💼 **Business Associates:** companies that handle PHI on behalf of covered entities (e.g., billing services, cloud storage providers, software vendors).

ℹ️ HIPAA compliance is essential for any organization operating in or serving the U.S. healthcare sector, even if it does so indirectly.

Part 1.
Who Must Comply GDPR Applicability

GDPR Applicability

GDPR applies to **any organization** — whether a business, non-profit, or public authority — anywhere in the world if it processes the personal data of individuals located in the EU, regardless of their nationality.

You fall under GDPR if:

- 🤝 You offer **goods or services** to people in the EU, even without payment.
- 📊 You **monitor user behavior** within the EU (for example, through cookies, analytics, or marketing tracking).

ℹ️ Even if your organization only runs surveys, research, or collects data for analytics involving EU residents — you're still covered by the GDPR.

Part 1.
Who Must Comply GDPR Applicability

HIPAA Applicability

HIPAA applies to organizations operating in the **US healthcare ecosystem** that handle **Protected Health Information (PHI).**

Who it's for:

- **Covered Entities:** healthcare providers, health plans, and clearinghouses.
- **Business Associates:** companies that handle PHI on behalf of covered entities (e.g., billing services, cloud storage providers, software vendors).

Even if your company isn't directly involved in healthcare, you may still be subject to HIPAA if you process or store PHI for a healthcare client.

Part 2.
The Three Layers of GDPR Compliance

The Visible Layer (Customer-Facing)

- 👉 Cookie banners with real user choice (accept/reject).
- 👉 Clear Privacy Policy and Terms of Use, available on every page.
- 👉 Consent boxes that are not pre-ticked and written in plain language.
- 👉 Transparency about what data you collect, why, and for how long.

The Operational Layer

☝️ **Principles to embed in daily operations:**

- 👉 **Lawfulness & Transparency:** Explain how and why you process data.
- 👉 **Data Minimization:** Only collect what's necessary.
- 👉 **Accuracy:** Keep data up-to-date and correctable.
- 👉 **Storage Limitation:** Delete data when it's no longer needed.

Part 2.
The Three Layers of GDPR Compliance

The Technical Layer

☝️ **What the user doesn't see — but what protects your business:**

- 👉 Encryption in transit and at rest.
- 👉 Access control and role-based permissions.
- 👉 Regular backups and incident response plans.
- 👉 Pseudonymization or anonymization of personal data.
- 👉 Two-factor authentication (2FA).

Part 3.
HIPAA Compliance Framework

The Visible Layer (Customer-Facing)

- 👉 Cookie banners with real user choice (accept/reject).
- 👉 Clear Privacy Policy and Terms of Use, available on every page.
- 👉 Consent boxes that are not pre-ticked and written in plain language.
- 👉 Transparency about what data you collect, why, and for how long.

Focuses on technical and administrative safeguard

- ☝️ **Principles to embed in daily operations:**
- 👉 **Lawfulness & Transparency:** Explain how and why you process data.
- 👉 **Data Minimization:** Only collect what's necessary.
- 👉 **Accuracy:** Keep data up-to-date and correctable.
- 👉 **Storage Limitation:** Delete data when it's no longer needed.

Part 3.
HIPAA Compliance Framework

The Technical Layer

☝️ **What the user doesn't see — but what protects your business:**

- 👉 Encryption in transit and at rest.
- 👉 Access control and role-based permissions.
- 👉 Regular backups and incident response plans.
- 👉 Pseudonymization or anonymization of personal data.
- 👉 Two-factor authentication (2FA).

Part 4.
Eleven Steps for GDPR & HIPAA-Ready Compliance

Step 1. Assign Responsible Staff

Designate a Data Protection Officer (DPO) or a compliance lead. For HIPAA, you'll also need a Privacy Officer and a Security Officer.

☝️ **They oversee:**

- 👉 Risk assessments
- 👉 Employee training
- 👉 Data protection strategy and policy updates.

Step 2. Conduct a Data Audit

- 👉 Inventory all data types and systems (CRM, EMR, HR, analytics, etc.).
- 👉 Document how data enters, moves, and exits your organization (data flow maps).
- 👉 Tag and classify data as PHI, personal data, or sensitive data.
- 👉 Keep this inventory updated after system or vendor changes.
- 👉 Create a **Record of Processing Activities (RoPA)** for GDPR and a **Risk Analysis Report** for HIPAA.

Step 3. Ensure Lawful Basis for Processing

You need a legal reason to process data — otherwise, it's a compliance breach.

👩 HIPAA:

Processing PHI is allowed under specific circumstances:

- 👉 **Treatment:** delivering healthcare.
- 👉 **Payment:** billing, claims, reimbursements.
- 👉 **Healthcare Operations:** administrative, quality improvement, or auditing tasks.
- 👉 Keep this inventory updated after system or vendor changes.
- 👉 Create a **Record of Processing Activities (RoPA)** for GDPR and a **Risk Analysis Report** for HIPAA.

ℹ️ For any activities beyond these (e.g., marketing or research), explicit patient authorization is **required.**

🔒 GDPR:

There are six lawful bases for processing personal data:

1 Consent	4 Vital interests
2 Contract	5 Public task
3 Legal obligation	6 Legitimate interest

Health data almost always requires **explicit** consent unless it falls under vital interests or healthcare provision by professionals.

Checklist

- ✅ Identify and document the lawful basis for each processing activity.
- ✅ Keep consent logs (when, how, and for what purpose consent was given).
- ✅ Enable users to withdraw consent easily.
- ✅ Review your data processing justifications annually.

Step 4. Publish and Maintain a Privacy Policy

Individuals must be aware of what happens to their data.

👩 HIPAA:

You must provide a Notice of Privacy Practices (NPP) explaining how PHI is used and shared. It must be available at the point of care or via your website.

🔒 GDPR:

A **Privacy Notice** must clearly explain:

1. What data you collect
2. Why you collect it
3. User rights (access, correction, erasure, portability, objection).
4. Who you share it with
5. How long you keep it

Checklist

- ✅ Write your privacy policy in plain language (no legal jargon).
- ✅ Include contact info for your Privacy Officer or DPO.
- ✅ Update whenever processes or vendors change.
- ✅ Keep version control for audit purposes.

Step 5. Ensure Access Control & Authentication

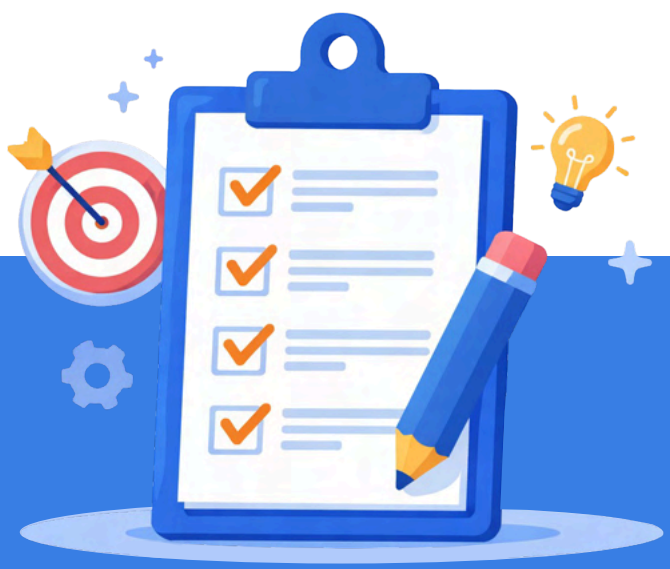
Limit data access strictly to those who need it.

👩‍⚕️ HIPAA:

Access to PHI must be **role-based** — only those involved in patient care, billing, or operations should have access.

🔒 GDPR:

Access to personal data should follow the **principle of least privilege.**



Checklist

- ✅ Define user roles and access levels.
- ✅ Enforce Multi-Factor Authentication (MFA).
- ✅ Automatically deactivate inactive or terminated accounts.
- ✅ Maintain access logs and review them monthly.
- ✅ Use unique user IDs — no shared credentials.

Step 6. Set Up Data Security Measures

🔒 Protect data from unauthorized access, breaches, or loss.

ℹ️ **Both HIPAA & GDPR** require strong **technical and organizational safeguards.**

Checklist

- ✅ Encrypt all PHI/personal data in transit (TLS/SSL) and at rest (AES-256).
- ✅ Use secure, HIPAA-compliant cloud services (AWS, Azure, GCP with signed BAAs).
- ✅ Implement firewalls, intrusion detection, and anti-malware tools.
- ✅ Regularly test and patch vulnerabilities.
- ✅ Apply device management policies (MDM) for laptops, phones, USBs.
- ✅ Conduct annual penetration testing.

Step 7. Minimize Data Collection

Collect **only what is needed** — and **delete what's not.** Keep PHI only as long as required by law or as necessary for business purposes. No explicit time frame is defined, but retention should follow state or organizational policy.

GDPR: Requires strict data minimization and storage limitation principles.

Checklist

- ✅ Review data collection forms and eliminate unnecessary fields.
- ✅ Define data retention schedules (e.g., delete records after 7 years).
- ✅ Securely erase data using certified tools.
- ✅ Review retention policy annually.

Step 8. Configure Your Website and Apps

- ✅ Use a GDPR-compliant cookie banner with real consent options
- ✅ Include clear explanations in every form about why data is being collected
- ✅ Provide an easy way for users to withdraw consent
- ✅ (For HIPAA-covered apps) Ensure all data transmission is encrypted and PHI is never exposed to third-party analytics.

Step 9. Create Internal Policies and Procedures

Include:

- 👉 Data Handling and Protection Policy
- 👉 Data Breach Response Policy
- 👉 Retention and Deletion Policy
- 👉 Department-specific procedures (e.g., HR, Marketing, IT).

ℹ️ Also, be prepared to detect, contain, and report data breaches fast.

👩‍⚕️ HIPAA:

Notify affected individuals, the HHS, and (if >500 records) the media within 60 days.

Document all breaches and mitigation steps.

🔒 GDPR:

Notify the supervisory authority within 72 hours of discovery.

Notify affected individuals if there's a high risk to their rights and freedoms.

Checklist

- ✅ Maintain an Incident Response Plan (IRP).
- ✅ Define clear roles: who investigates, communicates, and documents.
- ✅ Train staff on how to recognize and report incidents.
- ✅ Keep a breach register (even for non-reportable incidents).
- ✅ Conduct post-incident reviews and update policies.

Step 10. Train Employees

☝️ **Every employee who handles personal data must understand:**

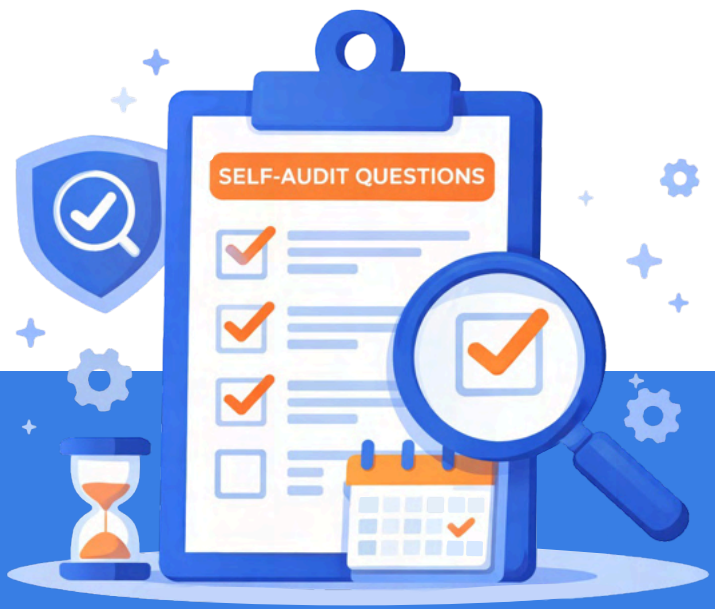
- 👉 What counts as personal or sensitive data
- 👉 How to securely handle it
- 👉 How to recognize and report a breach

Step 11. Set Up Data Subject / Patient Request Processes

- 👉 Provide a contact channel for access, deletion, or correction requests.
- 👉 Respond within the required timeframes (30 days for GDPR, 60 days for HIPAA).
- 👉 Document all requests and responses.

Part 5.
Quick Self-Audit Questions

- 👉 Do we have an up-to-date data map of all PHI/personal data? _____ (yes/no)
- 👉 Can we prove lawful processing for every activity? _____ (yes/no)
- 👉 Are all vendors under signed BAAs/DPAs? _____ (yes/no)
- 👉 Is data encrypted end-to-end? _____ (yes/no)
- 👉 Do we have tested breach and response procedures? _____ (yes/no)
- 👉 Can users efficiently exercise their rights? _____ (yes/no)
- 👉 Are staff trained regularly on privacy and security? _____ (yes/no)



Part 6.
Continuous Compliance

☝️ **Compliance isn't a one-time setup. Just like maintaining a car, it requires regular check-ups:**

- 👉 Review your policies every 6–12 months.
- 👉 Test data breach response drills.
- 👉 Monitor regulatory updates (EU, UK, US).
- 👉 Update documentation when you introduce new data tools or vendors.

Compliance done right = fewer risks, more trust.

Get a free one-on-one session with our data protection specialists to ensure your company meets HIPAA and GDPR standards efficiently.

Schedule a free consultation with BotsCrew