HIPAA

Guide to Health Information Privacy

Sean Montgomery, Co-Founder & CTO

XANO

Disclaimer

This document is for informational purposes only and does not constitute legal or regulatory advice. Xano makes no representations or warranties regarding the accuracy or completeness of this content. You should consult qualified legal counsel to understand your specific obligations under HIPAA or any other applicable laws.

Furthermore, utilizing Xano's platform and services, including the HIPAA-compliant hosting plan, does not, in and of itself, make a customer's application or organization HIPAA compliant. Compliance is a shared responsibility, and the customer remains fully responsible for ensuring their specific application architecture, data handling processes, and administrative policies meet all HIPAA requirements.

Foreword

For organizations entrusted with sensitive health data, protecting that information is more than a regulatory requirement, it's a business foundation. Every piece of personal health information represents a promise: to keep it private, secure, and respected. At Xano, we take that promise seriously, and we know our customers do too.

This guide was created to help Xano users confidently implement backend features aligned with HIPAA best practices. Whether you're building a telehealth platform, managing electronic records, or powering patient-facing applications, this ebook outlines the foundations and best practices needed to safeguard Protected Health Information (PHI) in Xano and beyond.
Our goal is not only to provide secure tooling, but to provide clarity on how to use it effectively. From configuring environments and encrypting data, to applying access controls and maintaining audit logs, each section in this guide is designed to help you turn HIPAA's principles into actionable, scalable practices.

Security and compliance are not achieved through checklists alone; they require thoughtful architecture, clear procedures, and the right partners. We're proud to serve as that partner for teams innovating in healthcare and digital wellness.

Thank you for trusting Xano as your platform. We're committed to helping you build systems that are not only powerful and scalable, but also private, secure, and worthy of your users' trust.

Stay innovative, stay secure.

Sean Montgomery

Co-Founder & Chief Technology Officer at Xano

Table of Contents

Table of Contents

Overview of HIPAA

The **Health Insurance Portability and Accountability Act (HIPAA)** was enacted in 1996 to protect the privacy of health information and establish national standards for electronic healthcare transactions. In response to increased digitization of medical records, HIPAA has been amended over time to address cybersecurity challenges.

Please note that regulatory timelines and final provisions are subject to change. This information is current as of the document's publication date, but you must consult the official HHS website for the most current and authoritative information.

Privacy Rule (2003)

Defines Protected Health Information (PHI) and outlines patients' rights regarding access, disclosure, and confidentiality of medical data.

Security Rule (2006)

Mandates administrative, physical, and technical safeguards for electronic PHI (ePHI)

Breach Notification Rule

Requires organizations to notify individuals, the Department of Health and Human Services, and in certain cases the media, in the event of a data breach.

HITECH Act (2009)

Encourages the adoption of electronic health records (EHR) and penalizes HIPAA violations, extending liability to software providers handling PHI on behalf of covered entities.

2025 HIPAA Privacy Rule Updates

Staying informed about the latest updates to the HIPAA Privacy Rule is essential for maintaining compliance and safeguarding data. The Department of Health and Human Services (HHS) regularly publishes new and proposed regulations, reflecting the evolving landscape of healthcare privacy and security. For the most current information on these developments, see the HHS website directly. Recent updates and proposed rulings include:

→ **Enhanced PHI access:** HHS has issued a finlal rule on this matter. Covered entities must allow individuals to inspect their health records in person, take notes, and receive documentation within 15 days (reduced from 30 days).

→ **Expanded patient rights:** This change has not been fully implemented yet. Individuals will have the ability to direct covered entities on how to share electronic health records (EHR), including coordination between providers.

New Categories of Protected Information

→ **Substance Use Disorder (SUD) records:** *HHS* has issued a final rule on this matter. Previously governed separately, now fully protected as PHI under HIPAA.

→ **Reproductive health information:** *HHS*. Now classified as specially protected PHI with additional restrictions on disclosure, particularly for legal investigations.

HIPAA Penalty Structure

The new penalty structure adopted in 2019 following the Notice of Enforcement Discretion is currently in effect but is not yet legally binding.

→ Following a 2019 Notice of Enforcement Discretion, OCR adopted a new penalty structure with different maximum penalties across the four tiers of violations.

→ This change may be made official in 2025, though a Notice of Proposed Rulemaking will be needed first.

→ These updates reflect a significant evolution in HIPAA regulations to address modern cybersecurity challenges and enhance patient privacy protections.

2025 HIPAA Security Rule (Proposed Overhaul)

The most recent key proposed changes include:

→ **Mandatory security controls:** The proposed rule would make multi-factor authentication (MFA) a requirement.

→ **Technology asset inventory and network map:** Organizations must develop and maintain an inventory of IT assets and network maps showing ePHI movement, with reviews required at least every 12 months.

→ **Enhanced risk analysis requirements:** More specific requirements, including review of technology assets and assessment of risk levels for identified threats.

→ **Contingency planning with time limits:** A proposed 72-hour limit for system and data restoration following cybersecurity incidents.

- **Mandatory annual audits:**
  HIPAA-covered entities and business associates must conduct internal Security Rule compliance audits at least every 12 months.
- **Encryption requirements:**
  All ePHI must be encrypted both at rest and in transit.
- **Device security:** Technical safeguards must be applied to mobile devices and tablets, with requirements for encryption, remote wipe capabilities, and access control.

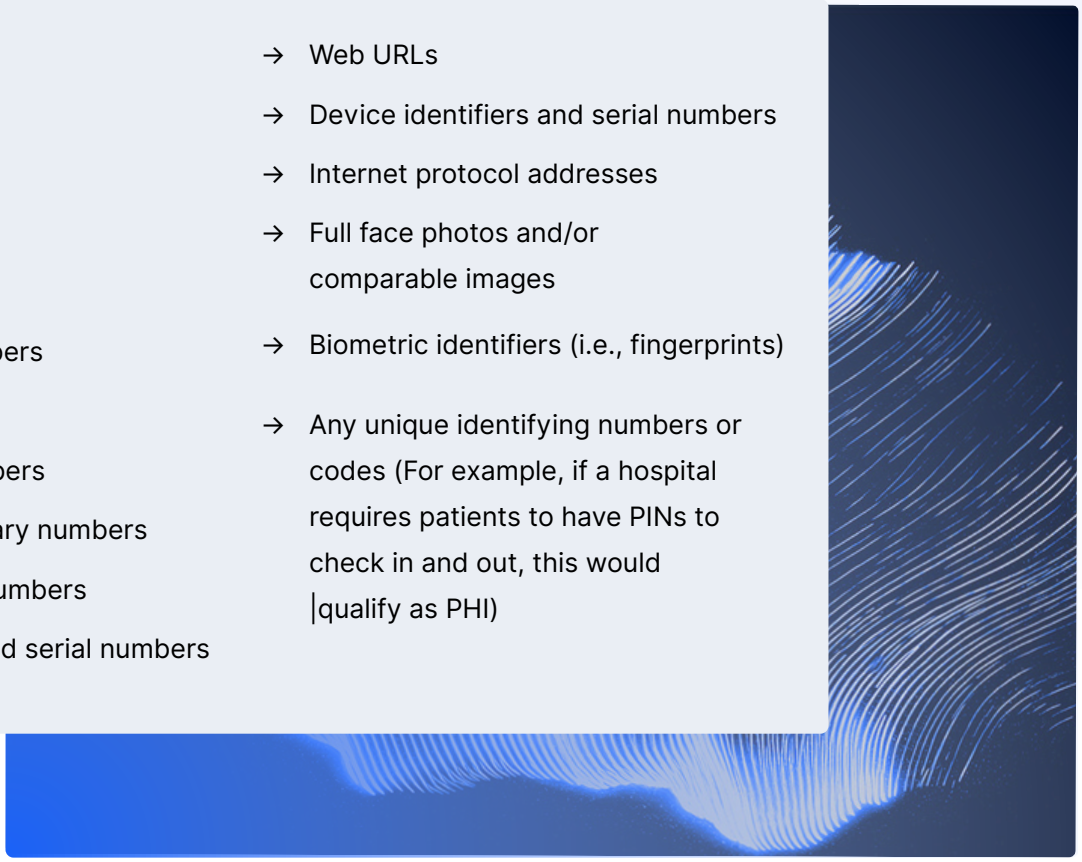
Key Terminology

- **Covered Entities:** Health plans, health clearinghouses, and healthcare providers who transmit health information electronically.
- **Business Associates:** Organizations or individuals that maintain, store, collect, or transmit PHI on behalf of a covered entity. Business Associates must execute Business Associate Agreements (BAAs) when working with PHI.
- **Protected Health Information (PHI):** Any individually identifiable health information, including names, contact details, medical record numbers, and more. HIPAA recognizes many unique identifiers that qualify information as PHI.
- **Electronic Protected Health Information (ePHI):**
  Any protected health information that is created, stored, transmitted, or received in any electronic format or media.
- **Minimum Necessary Standard:** A HIPAA principle requiring covered entities to make reasonable efforts to limit PHI use, disclosure, and requests to the minimum amount necessary to accomplish the intended purpose.
- **Breach:** The acquisition, access, use, or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the information.

PHI Identifiers

Protected health information consists of any data that can identify an individual and is linked to their health status or care. Common PHI identifiers include the following:

- → Names
- → Dates
- → Telephone numbers
- → Geographic data
- → FAX numbers
- → Social Security numbers
- → Email addresses
- → Medical record numbers
- → Health plan beneficiary numbers
- → Certificate/license numbers
- → Vehicle identifiers and serial numbers
- → Web URLs
- → Device identifiers and serial numbers
- → Internet protocol addresses
- → Full face photos and/or comparable images
- → Biometric identifiers (i.e., fingerprints)
- → Any unique identifying numbers or codes (For example, if a hospital requires patients to have PINs to check in and out, this would qualify as PHI)



Safeguards Required by HIPAA

To ensure the protection of PHI, HIPAA's Security Rule outlines a set of required safeguards that organizations must implement. These safeguards are divided into three primary categories: technical, administrative, and physical. Together, these safeguards create a comprehensive framework for maintaining the confidentiality, integrity, and availability of PHI.

Technical Safeguards

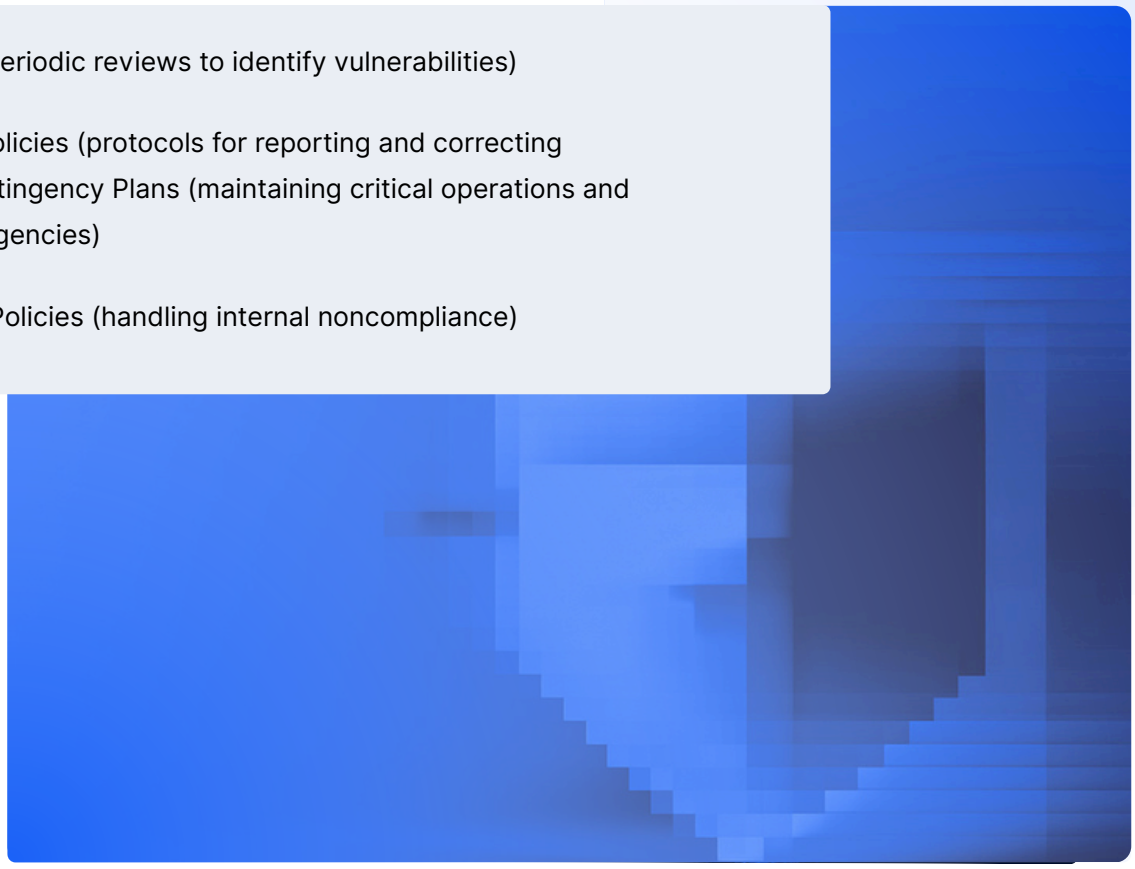
Technical safeguards ensure the secure processing, transmission, and storage of ePHI through measures such as:

- → Access Control (unique user IDs, emergency access procedure)
- → Activity Logging and Audits (tracking and recording system interactions)
- → Data Encryption (both at rest and in transit)

Administrative Safeguards

Administrative safeguards focus on policies, procedures, and workforce training to manage security risks. Namely, the following documentation is crucial for HIPAA compliance:

- → Risk Assessments (periodic reviews to identify vulnerabilities)
- → Risk Management Policies (protocols for reporting and correcting security issues) Contingency Plans (maintaining critical operations and PHI security in emergencies)
- → Employee Sanction Policies (handling internal noncompliance)



Insights on HIPAA Compliance for Mobile Applications

Scope of HIPAA for Mobile Apps

If your application handles PHI (e.g., health records, insurance numbers, personal identifiers), it is subject to HIPAA requirements. Mobile healthcare apps must protect against unauthorized access, disclosure, and other security vulnerabilities.

Educational Foundations

Familiarize yourself with covered entities, business associates, and other HIPAA definitions. The FTC "Mobile Health Apps Interactive Tool" can help determine which regulations apply.

Technical & Security Considerations

- → **Local Session Timeout:** Prompt users to re-authenticate after inactivity.
- → **Avoid PHI in Push Notifications:** Only alert patients to log in for details instead of displaying sensitive content.
- → **Robust SSL Encryption:** Encrypt data from end-to-end when transferring medical information.

Validating Security

- → **Dynamic and Static Testing:** Detect vulnerabilities before deployment.
- → **Penetration Testing:** Employ reputable third parties to confirm application security.

HIPAA Considerations in Software Development

PHI and Covered Entities

Any software used by a covered entity (e.g., healthcare provider, health plan, or clearinghouse) or a business associate (someone who handles PHI on behalf of a covered entity) that stores or transmits PHI is subject to HIPAA requirements. Examples of essential security measures include encryption, user authentication, and robust access controls.

Core Laws and Rules

HIPAA is built on a framework of laws and regulations designed to protect sensitive health information and ensure its secure handling across healthcare and related industries.

- → **HIPAA Privacy Rule:** Defines who must comply (covered entities and business associates) and limits the permissible uses and disclosures of PHI.
- → **HIPAA Security Rule:** Requires administrative, physical, and technical safeguards (e.g., rigorous access controls, data encryption) to protect electronic PHI.
- → **HITECH Act:** Enhances HIPAA enforcement, increases penalties for violations, and encourages the use of electronic health records.

Key Steps for HIPAA-Ready Software

Building HIPAA-compliant software requires a proactive approach to security, data management, and regulatory adherence. Below are key steps to help ensure your software meets HIPAA requirements:

Administrative safeguards focus on policies, procedures, and workforce training to manage security risks. Namely, the following documentation is crucial for HIPAA compliance:

- → **Expert Consultation:** Engage attorneys or professionals with extensive knowledge of HIPAA regulations. Their expertise helps minimize compliance risks and interpret complex legal obligations.
- → **Data Separation & Encryption:** Segment Protected Health Information (PHI) from non-sensitive data. Apply robust encryption algorithms (e.g., AES-256) for data both in transit and at rest, reducing the likelihood of unauthorized access.
- → **Logging & Monitoring:** Maintain comprehensive system logs to track user activity, data access, and security events. This practice supports compliance audits and allows quick identification of suspicious activities.
- → **Testing & Maintenance:** Conduct both static and dynamic security testing after major updates or changes. Ongoing maintenance includes applying patches, reviewing configuration settings, and validating that all security controls remain effective.

Xano's Responsibilities: Security of the Platform

As defined in our BAA, Xano is responsible for implementing and maintaining reasonable and appropriate administrative, technical, and physical safeguards for the core platform. This ensures the protection of the underlying infrastructure that powers your backend. These safeguards are designed to:

- **Secure the Core Infrastructure:** We manage the security of the platform's operating environment, which resides within physically secure data centers with environmental and access controls.
- **Protect Platform Data:** We implement measures to protect data on the platform, including encryption for data in transit between your client and our services and for data at rest on the physical storage media.
- **Maintain Platform Integrity and Availability:** We employ security practices to protect the core Xano services against unauthorized access and ensure the platform remains available. This includes managing the security of the host operating systems, the virtualization layer, and having processes in place for the availability and recovery of the core platform.

Your Responsibilities: Security & Compliance IN Your Application

Xano provides the secure foundation and compliant tools. As stated in our BAA, each party is solely responsible for the decisions it makes regarding the safeguarding of PHI. It is your responsibility to use our tools correctly to build, manage, and operate a secure and compliant application.

Some of your responsibilities include:

Application-Level Access Control:

- Implementing robust authentication to verify user identities.
- Designing and enforcing granular authorization and role-based access logic to ensure users can only access the specific PHI they are permitted to see, in adherence with the Minimum Necessary Standard.

Secure API and Business Logic:

- You are solely responsible for the security of the API endpoints and business logic you create. This includes ensuring they do not inadvertently expose PHI and have strict authorization checks before returning any data.

Data Governance and Management:

- Properly identifying, classifying, and managing PHI within your database schema and application workflows.
- Ensuring your use, disclosure, and retention of PHI within your application complies with HIPAA rules.

User and Client-Side Security:

- Managing your application's end-users, including password policies, account lockout procedures, and session management.
- Securing your front-end application (web or mobile), as it is the primary interface for your users to interact with the backend you've built on Xano.

Your Organization's Administrative Safeguards:

  - Conducting your own Security Risk Analysis for your unique application and organization.
  - Developing and enforcing policies and procedures for your workforce regarding the proper handling of PHI.
  - Training your employees and monitoring activity within your application. Xano provides tools, such as request history logs, which can be a valuable component of your overall monitoring and auditing strategy.

Key Customer Responsibilities in Application Design

In addition to the safeguards already mentioned, your application design must account for several critical HIPAA requirements. The responsibility for implementing the following rests entirely with you:

- **Application-Level Audit Trails**: HIPAA requires detailed logging of access to ePHI. You must build logic within your application to create a specific audit trail for who accesses what data and when. Xano's request logs can support this, but they are not a substitute for this required application-level feature.

- **Data Backup and Recovery**: You are solely responsible for backing up your application's data. Xano's platform availability and disaster recovery do not cover point-in-time recovery of your data due to application or user error. You must implement and test your own data backup and restoration plan.

- **Data Retention and Disposal**: You must design your application to manage the entire data lifecycle according to your own retention policies and HIPAA rules, including the secure and permanent deletion of ePHI when it is no longer required.

- **Incident Management**: If a security incident or data breach occurs within your application (e.g., due to a compromised user account), you are responsible for leading the investigation, risk assessment, and all required notifications to individuals and HHS. Xano will provide cooperation as defined in our BAA.

Recommended Steps Toward Compliance

Achieving HIPAA compliance involves not only technical safeguards but also organizational policies and procedures that ensure proper handling of protected health information. The following steps can help establish a strong compliance foundation:

1 | **Policy Development & Enforcement:** Draft clear, standardized procedures governing access control, employee training, breach response, and user account management. Formalizing these policies reduces the risk of inconsistent practices.

2 | **Training & Awareness:** Conduct ongoing education that highlights HIPAA obligations and proper handling of Protected Health Information (PHI). Emphasize the importance of individual accountability within your organization.

3 | **Execute Business Associate Agreements (BAAs):** Establish formal BAAs with third parties and vendors that handle PHI on your behalf. These agreements assign responsibilities, detail handling procedures, and define liability.

4 | **Monitor for Compliance:** Conduct routine internal audits and maintain meticulous documentation of all compliance-related tasks. Keep logs for system access, security incidents, and breach responses to facilitate quick incident identification and response.

5 | **Validate Security Regularly:** Schedule both internal and external testing (run/review penetration tests, vulnerability scans, and logs). This approach helps identify gaps before they evolve into real threats.

Implementing Security & HIPAA Compliance in Xano

Xano offers a serverless backend platform, making it a powerful option for rapidly deploying HIPAA-sensitive applications. Below are some highlights:

Data Architecture

Designing a secure data architecture is essential for protecting PHI and ensuring compliance with HIPAA regulations. Best practices include:

- → **Segregate PHI:** Store PHI in logically or physically separate databases or tables.
- → **Robust Access Controls:** Enforce role-based authentication, limiting PHI endpoints to authorized users only.
- → **Encryption:** Utilize encryption (e.g., AES-256) for data at rest and TLS for data in transit.

Configuring Environments

Designing a secure data architecture is essential for protecting PHI and ensuring compliance with HIPAA regulations. Best practices include:

- → **Separate Environments:** Maintain distinct development, staging, and production infrastructures to mitigate security risks.
- → **Secure Hosting & Variables:** Employ hosting configurations that protect environment variables. Apply strict permissions to personnel with access to critical infrastructure.
- → **Regular Audits:** Continuously review environment configurations and user permissions for potential vulnerabilities.

Business Associate vs. Subcontractor

Under HIPAA, **Business Associates** are entities that perform services involving PHI on behalf of a Covered Entity, such as cloud service providers, billing companies, or consultants.

- → Xano would be considered a Business Associate when it directly contracts with a Covered Entity (such as a healthcare provider or health plan) to provide services involving the use or disclosure of PHI. In this scenario, Xano would sign a Business Associate Agreement (BAA) with the Covered Entity, committing to appropriately safeguard PHI, maintain confidentiality, and handle data in compliance with HIPAA regulations.

Subcontractors, on the other hand, are third parties engaged by a Business Associate to carry out functions or services that also involve PHI.

→ Xano would be classified as a Subcontractor when it provides services to another Business Associate rather than directly to a Covered Entity. In this case, Xano would sign a Business Associate Subcontractor Agreement (BASA) with that Business Associate, agreeing to the same restrictions and conditions that apply to the Business Associate with respect to PHI handling.

Both Business Associates and their Subcontractors are required to sign agreements that ensure compliance with HIPAA regulations. A signed Business Associate Agreement (BAA) or Business Associate Subcontractor Agreement (BASA) must be executed between your organization and Xano before you may store, process, or transmit any PHI on the Xano platform. If you have upgraded to a HIPAA package, please reach out to security@xano.com to execute your agreement.

Reminder: Use of Xano's HIPAA-compliant infrastructure does not by itself ensure your application is HIPAA compliant. You are responsible for proper configuration, development, and data management.

Further Resources

Building HIPAA-compliant applications within Xano requires careful consideration of data security, privacy regulations, and best practices across various aspects of your infrastructure. From ensuring proper data architecture and secure environment configurations to implementing robust workflows, these steps form the foundation of a secure and compliant solution.

For more comprehensive information on secure Xano implementation, explore our detailed "Building Securely in Xano" E-book.