# Designing a HIPAA-Compliant Digital Solution – Nine Key Considerations

CATALYST UX

By Katrina Destrée
*Sr. Data Privacy and Compliance Strategist*

The world of HIPAA compliance and regulations can be tricky if you are new to designing medical devices and digital solutions.

The Health Insurance Portability and Accountability Act (HIPAA) has had a significant impact on the design of today's digital health solutions. In this article, we not only cover what HIPAA is, but who should be concerned, what information is impacted, ways HIPAA impacts UX design in medical and life science digital solutions, how to protect your organization against data breaches, cyber threats, and more.

## What Is HIPAA?

HIPAA is the acronym for the Health Insurance Portability and Accountability Act that was passed by US Congress in 1996. The purpose of HIPAA is to reduce healthcare fraud and abuse, mandate industry-wide standards for healthcare information and electronic billing, and require protection and confidential handling of protected health information.

In addition, the HIPAA Privacy Rule established national standards to protect medical records and other Personal Health Information (PHI) and gave patients rights over their records.

## Who Does HIPAA Impact?

According to HIPAA, if your organization belongs to the category of "covered entities" or "business associates," and handles "protected health information (PHI)," there is a requirement to be HIPAA compliant. The definitions of these organizations are below.

If your company falls into one of these categories and you need to understand if you are compliant, contact us. One of our privacy specialists can walk through our guidelines with you, as those guidelines relate to UX and UI.

- **Covered entities** describes U.S. health plans, healthcare clearinghouses, and healthcare providers;
- **Health plans includes** HMOs, company health plans, health maintenance companies, Medicare, Medicaid, employers;
- **Clearing houses** includes billing services, community health information systems;
- **Healthcare providers** include physicians, surgeons, dentists, podiatrists, laboratory technicians, optometrists, hospitals, clinics, nursing homes, pharmacies;
- **Business associates** refers to any organization or individual who acts as a vendor or subcontractor with access to PHI; examples of business associates include: data transmission providers, data processing firms, data storage or document shredding companies, medical equipment companies, consultants hired for audits, coding reviews, electronic health information exchanges, medical transcription services, external auditors or accountants.

## Information and Considerations

### *Information Impacted*

So you may be asking, what type of information is affected by HIPAA? The answer is, any information included in a medical record that can identify an individual and was created and used while providing healthcare (e.g., diagnosis or treatment). PHI also includes:

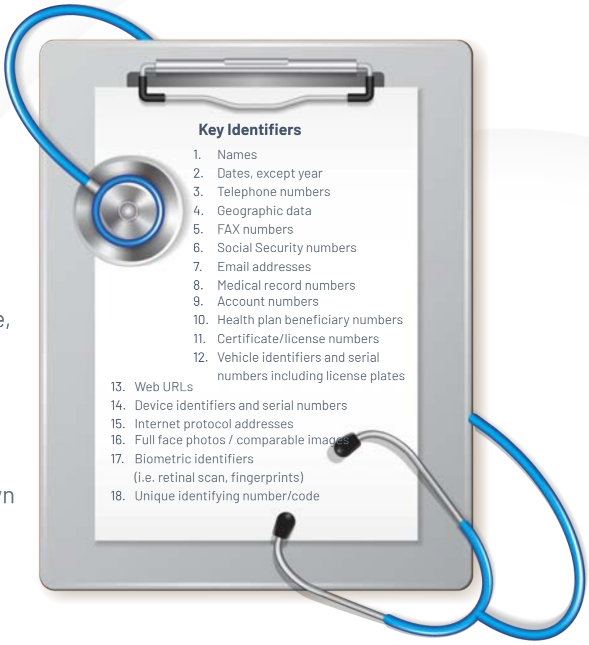
- Any conversation a patient has with a physician or nurse about his or her treatment;
- A patient's billing information;
- Medical information in the patient's health insurance company's database.

### *Considerations*

Given the above, when designing software in a HIPAA environment, you'll want to consider:

- A person's past, present, and future physical or mental health or condition;
- The provision of healthcare to the individual;
- The past, present, or future payment for the provision of healthcare to the person;
- Name, address, date of birth, Social Security number, etc.
- Biometric data (facial recognition, fingerprint, etc.).

In fact, there are actually 18 key identifiers that are always considered key health identifiers (see sidebar).



**Key Identifiers**

1. Names
2. Dates, except year
3. Telephone numbers
4. Geographic data
5. FAX numbers
6. Social Security numbers
7. Email addresses
8. Medical record numbers
9. Account numbers
10. Health plan beneficiary numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers including license plates
13. Web URLs
14. Device identifiers and serial numbers
15. Internet protocol addresses
16. Full face photos / comparable images
17. Biometric identifiers (i.e. retinal scan, fingerprints)
18. Unique identifying number/code

## Data Classification

Personal Health Information is personal data. For the purpose of this article, data refers to personal data. The first step in managing personal data is to classify it according to sensitivity; to rank data in terms of the potential harm a person could suffer if certain data elements were accessed by unauthorized users. Planned data classification enables efficient use and protection of personal data across the organization and contributes to risk management and compliance processes. Organizations determine their own data classes and governance. A typical example of how you might classify personal health information is below:

1. **Restricted** data is highly sensitive information that is never to be written down. For example, a Social Security number would be considered restricted data.

2. **Confidential** data is sensitive information such as financial information for making payments.

3. **Internal** data is nonsensitive information that is not released to the public. For example, a name of a patient and their dates of treatment.

4. **Public** information is data that is already in the public domain or approved for public access. This might include someone's professional status or activities.

## Data Access and Sharing

In terms of accessing data, HIPAA guidelines state that patients have the right to access their own health information, a right that is often misunderstood or not even realized.

But patient care is a complicated issue and often requires multiple stakeholders to collaborate and discuss sensitive issues related to the individual. There are rules on sharing PHI.

### *When can PHI be shared*

The following are times when an entity can share information:

- **To the Individual.** A HIPAA-covered entity may disclose protected health information to the individual who is the subject of the information.
- **Treatment, Payment, Healthcare Operations.** A covered entity may use and disclose PHI for its own treatment, payment, and healthcare operations activities. Other disclosures include provider treatment and payment activities.
- **Obtaining Consent.** Written permission from individuals to use and disclose their PHI for treatment, payment, and healthcare operations.
- **Uses and Disclosures with Opportunity to Agree or Object.** By asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object, a covered entity can get informal permission for a disclosure. An example of this may be when an individual is incapacitated.
- **Public Interest and Benefit Activities.** The HIPAA Privacy Rule permits use and disclosure of PHI without an individual's authorization or permission for 12 national priority purposes including those required by law, such as for victims of abuse, law enforcement purposes, etc.

### *Common violations*

Some common violations of accessing or sharing data as outlined in the HIPAA Journal include:

1. **Snooping on Healthcare Records.**
2. **Impermissible Disclosures of Protected Health Information.** This includes disclosing PHI to a patient's employer, potential disclosures following the theft or loss of unencrypted laptop computers, careless handling of PHI, disclosing PHI unnecessarily, not adhering to the "minimum necessary" standard, and disclosures of PHI after patient authorizations have expired.
3. **Improper Disposal of PHI.** When physical PHI and ePHI are no longer required and retention periods have expired, HIPAA Rules require the information to be securely and permanently destroyed.
4. **Denying Patients Access to Health Records/Exceeding Timescale for Providing Access.** The HIPAA Privacy Rule gives patients the right to access their medical records and obtain copies on request. This allows patients to check their records for errors and share them with other entities and individuals. Denying patients copies of their health records, overcharging for copies, or failing to provide those records within 30 days is a violation of HIPAA.

## Software Considerations for Data

Healthcare IT tools must correspond to all HIPAA requirements to make medical institutions integrate them. Following are elements that must be implemented in software for medical organizations to ensure HIPAA IT compliance:

- **Audits.** A HIPAA-compliant software should utilize these audits to analyze the compliance level of a particular medical organization and provide it with detailed information concerning risks and current errors.
- **Recovery Plan.** The above-mentioned audits will help forecast risks or detect errors related to HIPAA compliance. The software should be able to initiate a particular plan for a specific situation.
- **Documentation.** Required principles, for medical software in documentation processing include: comprehensibility; simplicity; strict structure; and; secure data storage.
- **Managing Relations With Business Associates.** HIPAA-compliant software must also handle the company's relationships with its business associates, including contractors responsible for managing ePHI.
- **Security.** Software must be able to detect those breaches, create a corresponding report, and apply preliminary measures to avoid further data "sharing." It also has to prevent data breaches by blocking the use of portable data storage devices.

**HIPAA-Compliant Software Features:**

- ✓ User authorization
- ✓ Access control
- ✓ Authorization monitoring
- ✓ Data backup
- ✓ Remediation plan
- ✓ Emergency mode
- ✓ Automatic logoff
- ✓ Data encryption and decryption.

## Standards for Storing Personal Health Information

Hospitals and other healthcare provider organizations rely upon a variety of computer systems to process billing records, health records, and patient tracking. All of these systems should communicate with each other (or "interface") when they receive or retrieve new information.

A set of international standards called Health Level Seven or HL7 International facilitates the transfer and interoperability of clinical and administrative data between software applications used by various healthcare providers.

These standards focus on the application layer, which is "layer 7" in the OSI model. The HL7 standards are produced by Health Level Seven International, an international standards organization, and are adopted by other standards issuing bodies such as American National Standards Institute and International Organization for Standardization.

## How to Protect Your Organization From Cyberthreats

HIPAA-compliant digital solutions often contain information that may cause significant harm if accessed by unauthorized individuals. To protect your organization:

- Assume your solution is a high value target and vulnerable to cyberthreats such as ransomware and data security breaches and plan accordingly.
- Most incidents and data breaches are due to human error. Role play scenarios where  unauthorized access to personal data may occur so as to raise awareness and plan on how to recognize areas of vulnerability. Tabletop exercises are best to demonstrate how easily personal data may be compromised by doing business as usual instead of implementing guardrails such as organizational and technical measures.
- Incidents of hacking, phishing, whaling, data theft, and some account management practices have resulted in some serious ramifications for patients and organizations.
- Develop, implement, and regularly review well defined processes to be followed so as to properly handle incidents and data breaches.

## How to Prepare for Incidents and Data Breaches of PHI

To prepare, follow the steps to plan for incidents, define what data constitutes a breach, and finally, to detect. See below:

- **Plan**. A plan on how to manage incidents and data breaches of all information, including PHI, should be stated in writing. A Standard Operating Procedure (SOP) should be established with a flowchart of steps to take in cases of a data incident (only determined to be a breach by a legal department). A data breach management and response playbook, including incident management response checklists are key elements of a robust privacy program.

- **Define**. What is a personal data breach? When personal information (relating back to a person) has been accessed or shared with unauthorized parties. This should include accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

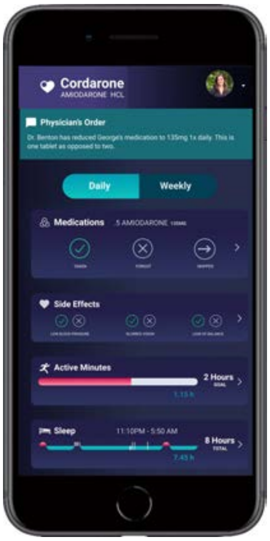
- **Detect**. Some aspects of the software should serve to help detect breaches and may include:
  - User authorization
  - Access control
  - Authorization monitoring
  - Data backup (storage)
  - Remediation plan
  - Emergency mode
  - Automatic logoff
  - Data encryption and decryption
  - Data auditing

## About PHI Audits

Change auditing is required. U.S. privacy laws and HIPAA require that detailed records be kept of who has accessed and changed patient records. Given this, here are some key points to consider when designing and developing HIPAA-compliant software:

- **Unique logins.** Each user must have their own unique login.
- **Standard Operating Procedure (SOP)**. Organizations should implement standard operating procedures for data governance of PHI including:
    - Categorizing and classifying file systems to determine where PHI lives.
    - Establishing file permissions for all of your data storage. Identifying files containing PHI and label as sensitive.
    - Correlate all data. For example you'll need permission structures, you'll need to classify sensitive data and build a comprehensive risk profile to continue the data governance process.
- **Reassess privileges.** Establish access based on least privilege access. For example, least privileged means that each user – person or service account – only has permissions they need to do their job.
- **Clean up stale data.** Some of the greatest risks in unstructured data is stale data that is no longer used or needed. Stale data make excellent targets for data bad actors/data thieves.

## How Does HIPAA Impact UX Design?



Dr. Benton has reduced George's medication to 135mg 1x daily. This is one tablet as opposed to two.

There are many considerations to take into account when designing medical products, some of which are not relevant when designing other types of applications.

### Importance of modular and scalable design

The shifting state and federal regulatory landscape can make building a streamlined, seamless experience difficult. To keep ahead of regulations, ensure that your designs are modular and scalable so new laws don't disrupt the experience. Wherever possible, reuse familiar patterns and allow workflows to accommodate various numbers of steps.

### Greater need to update legacy systems

Legacy systems in the healthcare sector make it particularly vulnerable to cyberthreats such as ransomware and data security. Industry watchdogs for HIPAA and the related HITECH have stricter rules aimed at curbing data breaches and other mishaps. Incidents of hacking, phishing, data theft, and lax account management practices have resulted in some serious ramifications for patients.

## Impact on content and communication

HIPAA not only regulates the content of messages but the channels that you send messages. Here are three things to consider when designing for customer communications:

- **Content.** System notifications via email can violate HIPAA regulations, so often notifications end up being summarized in a vague "daily digest" email once a day.

- **Channels.** HIPAA regulates what channels providers can use to communicate – if a provider writes to a patient within one portal, the patient can only read and respond to that message in the same portal (messages cannot be revealed over email).

- **Language.** Government regulations can also affect public-facing applications and websites; for instance, to have a Spanish translation on a healthcare website you would need a certain number of government-approved Spanish speakers on staff.

### *Ensuring backend data is compliant*

When designing your software, you'll also need to ensure that backend data meets HIPAA guidelines. For example:

- All PHI data should be isolated from other data and must be stored in a HIPAA-compliant environment which Microsoft Azure, Amazon Cloud Services, and Google Cloud can all provide.
- HIPAA-compliant functionality should be isolated from other functionality to allow for review and modification.
- Non-HIPAA-compliant data and functionality should be isolated such that changes and enhancements won't trigger a required HIPAA compliance review.

### *Meeting privacy requirements*

You'll also want to make sure your software or digital solution meets privacy requirements. As referenced previously, laws require that access to information is limited to users who actually need it. In addition, U.S. privacy laws require that detailed records be kept of who has accessed and changed patient records.

Finally, privacy laws preclude multiple users using the same login to access accounts as a default behavior. Instead, each user needs his or her own account with a separate login and password.

### *Protecting patient safety*

Regulations are designed to mitigate risk and protect the patient. Many of these regulatory requirements around designing and building a safe, risk-free product follow user experience best practices. For example, it is required that you identify every target audience (similar to UX personas). And for each target audience, you'll need to identify tasks with the goal of identifying and mitigating risk.

Not only is user and design evaluation a major component of the regulations, it's required. In fact, to obtain FDA approval you must provide results of at least one round of user testing, usually called human factors testing.

## Why you can’t ignore HIPAA

There are various regulations impacting usability, design, implementation, and data for any product in the healthcare industry. Being in the dark about these regulations can cause delays in product delivery, or furthermore, attract heavy penalties for not fulfilling safety standards. Worse, regulatory bodies may prevent you from launching the product.

Sources;
How HIPAA Regulations Apply to Key Patient Data Access Situations
The Most Common HIPAA Violations You Should Be Aware Of
What is Considered PHI Under HIPAA?
HIPAA Privacy Rule: Permitted PHI uses and disclosures
How to Make Your Software HIPAA-Compliant

# Getting started

CATALYST **UX**

The world of HIPAA compliance and regulations can be tricky if you are new to designing medical devices and digital solutions. If you are building a new product or updating a legacy system and you need guidance on whether you are meeting these requirements, **email us at business@catalystux.com**. We’ll hold a complimentary 30-minute meeting to go over HIPAA requirements and discuss points of potential failure in your software.

**Silicon Valley**
1700 South El Camino Real
Suite 404
San Mateo, CA 94402

**Vancouver**
2658 West Third Avenue
Vancouver, BC V6K 1M3

**Boston**
30 Newbury Street,
Third Floor
Boston, MA 02116

www.CatalystUX.com

✉ info@CatalystUX.com