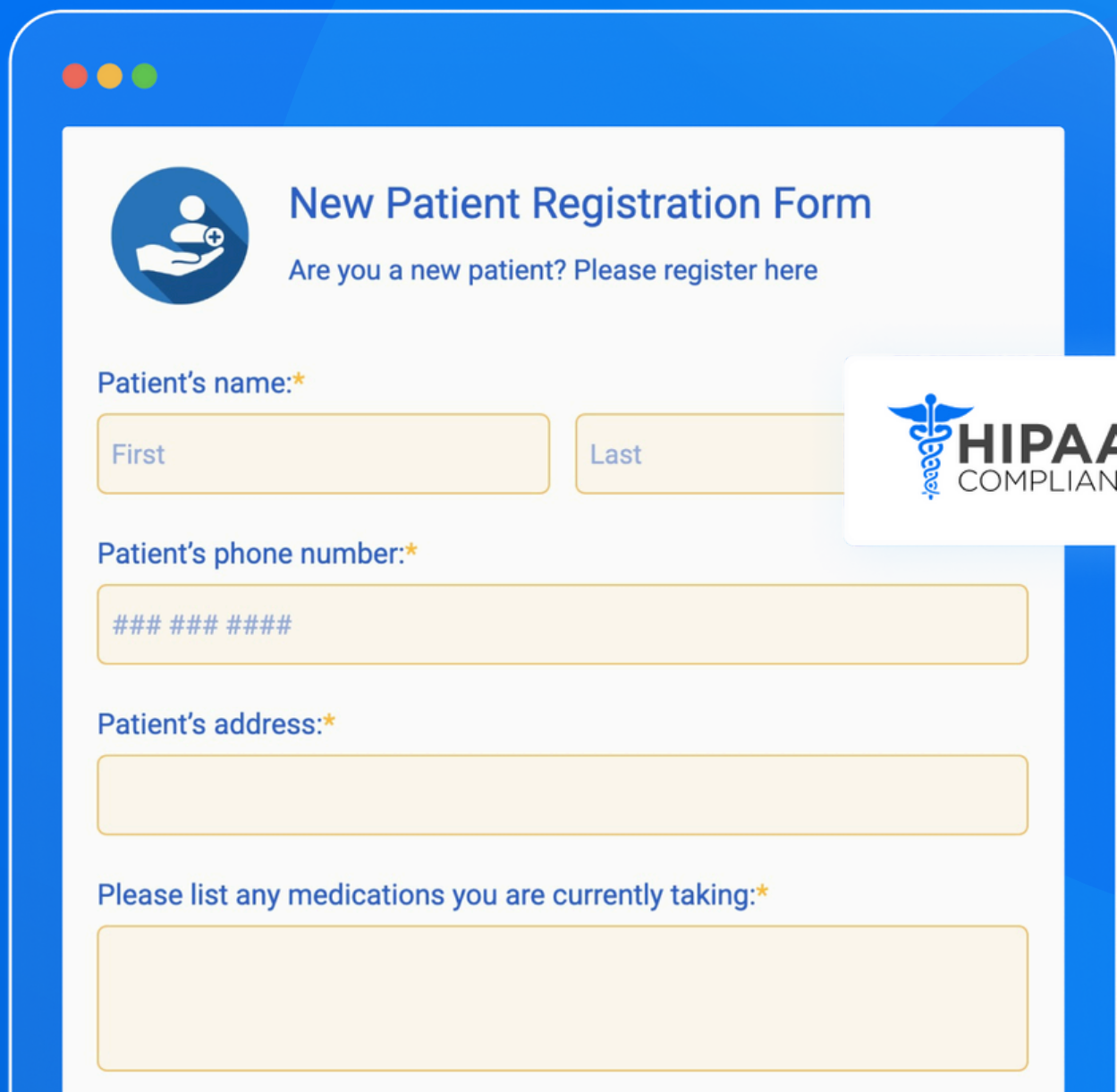


Securely Gathering Patient Data

THE HIPAA COMPLIANCE GUIDE



The image shows a digital form titled "New Patient Registration Form" with a medical icon. It includes fields for patient name (first and last), phone number, address, and a list of medications. A "HIPAA COMPLIANT" badge is visible on the right side of the form.

 **New Patient Registration Form**
Are you a new patient? Please register here

Patient's name:*

First Last

Patient's phone number:*

Patient's address:*

Please list any medications you are currently taking:*



Table of Contents

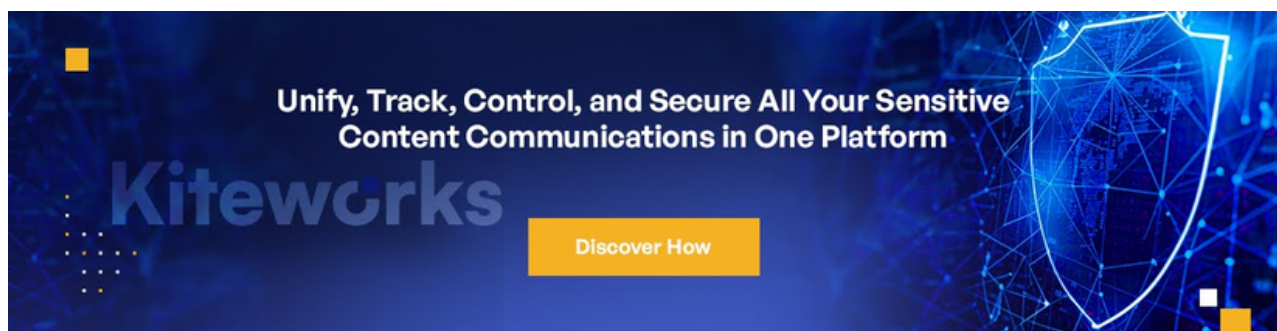
Context	02
A brief history of HIPAA	03
Are you affected by the HIPAA regulations?	03
Securely gathering and storing data	04
Business Associates vs Covered Entities in HIPAA compliance	05
How to Stay HIPAA-Compliant in Your Everyday Operations	06
Is Your Data Collection HIPAA-Compliant?	07
HIPAA Compliance Checklist	08
Achieving HIPAA Compliance with 123FormBuilder	11
Indemnification, Insurance and Liability	14
Customer Success Stories	15
Final thoughts	17



Context

Healthcare providers, including hospitals and small practices, face the growing challenge of securely managing vast amounts of patient data. With the rise of mobile technology and businesses moving online, protecting sensitive information has become critical, especially in healthcare.

Each patient interaction requires accurate data collection for the best outcomes, but with more information online, data security is now a top priority. The global data security market, which was valued at \$75 billion in 2015, has more than doubled, surpassing \$160 billion in 2023, reflecting the growing importance of cybersecurity. This trend is driven not just by software and hardware providers, but also by increasing government regulations aimed at safeguarding sensitive information.



A brief history of HIPAA

In the healthcare industry, sharing personal and sensitive information is essential for patient care. To address privacy and security concerns, the Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996. Its Title II, the Administrative Simplification provisions, established national standards for electronic healthcare transactions and identifiers for providers, insurers, and employers.

The January 2013 Final Omnibus Rule updated HIPAA, strengthening privacy protections under the HITECH Act. It expanded compliance to include business associates and revised breach notification requirements. Now, an impermissible disclosure of Protected Health Information (PHI) is presumed a breach unless a four-factor risk analysis shows a low probability of data compromise. This stricter standard aims to improve data breach accountability and reporting.

Additionally, HIPAA provisions address marketing, requiring entities to obtain explicit consent for certain uses of PHI, especially if financial motivations exist. These measures ensure a balance between operational efficiency and the safeguarding of sensitive data

Are you affected by the HIPAA regulations?

If you request sensitive information, even social security numbers or any type of information (date of birth, telephone number, email address) that may lead to the identification of a real person, then you may be subject to potential civil or criminal penalties if you are not HIPAA compliant.

Securely gathering and storing data

With the rise of online tools and software, businesses have increasingly turned to digital forms for tasks like event registrations, orders, and employee tracking. In the medical field, practices have shifted from paper forms to more secure online alternatives to store sensitive patient data.

Patient information, or Protected Health Information (PHI**), must be strictly safeguarded, with access limited to authorized personnel only. HIPAA regulations ensure that PHI is used properly and only with patient consent. Examples of sensitive data shared through online forms include:



Names



Date of birth



Telephone numbers



Email addresses



Social Security numbers



Medical record numbers



Health plan beneficiary numbers

*Health Information Technology for Economic and Clinical Health

**PHI stands for Protected Health Information and refers to any information that can be used to identify a patient, including: telephone or fax numbers, web URLs or photos, name of relatives, any number or code that may lead to identifying a patient's identity and much more.

Business Associates vs Covered Entities in HIPAA compliance

In HIPAA compliance, "Covered Entities" and "Business Associates" have distinct roles and responsibilities. Both must adhere to HIPAA regulations, with Business Associates required to sign a Business Associate Agreement (BAA) ensuring they safeguard PHI.



Covered Entities

A Covered Entity refers to any healthcare provider, health plan, or healthcare clearinghouse that creates, maintains, or transmits Protected Health Information (PHI). Hospitals, healthcare providers, and insurance companies are typically considered Covered Entities, responsible for implementing and enforcing HIPAA policies to protect PHI.

- **Examples:** Hospitals, doctors, health insurance plans, and healthcare clearinghouses.
- **Responsibilities:** Covered Entities are responsible for managing and safeguarding PHI in compliance with HIPAA regulations.



Hybrid Entities

Not all employers who maintain PHI about employees are Covered Entities. For instance, employers offering self-insured health plans or Employee Assistance Programs may qualify as Hybrid Entities, which are partially governed by HIPAA rules. These entities still must ensure PHI protection and could be liable for any unauthorized disclosures.



Business Associates

A Business Associate is any third-party entity that provides services to a Covered Entity and requires access to PHI to carry out those services. These entities are responsible for safeguarding the PHI they handle, as dictated by HIPAA regulations.

- **Examples:** Lawyers, IT contractors, billing services, data storage providers, and email encryption services.
- **Responsibilities:** Business Associates must sign a Business Associate Agreement (BAA) with the Covered Entity, outlining how PHI is accessed, used, and protected. They are also liable for HIPAA compliance and must safeguard PHI during and after their service.

Both Covered Entities and Business Associates must adhere to HIPAA regulations to protect PHI and avoid legal consequences from data breaches. A signed BAA is essential to ensure both parties understand their responsibilities regarding PHI access and protection.

How to Stay HIPAA-Compliant in Your Everyday Operations

Staying HIPAA-compliant can be challenging, but it's easier with a few simple steps:

- **Understand Key Terms:** HIPAA language can be confusing. Take time to learn the definitions and ask questions when needed.
- **Identify PHI:** Make sure you know all the Protected Health Information (PHI) your organization handles, including PHI shared with vendors and partners.
- **Evaluate Security Measures:** Review the security protocols in place to protect PHI and assess any potential threats—both intentional and accidental.
- **Assess Risks:** Consider the impact of a potential breach on your organization and rank the likelihood and severity of each risk.
- **Document Findings:** Keep detailed records of your risk assessment and policies to ensure compliance. Retain these documents for at least six years.

- **Back Up Data:** Always back up patient records and store backups securely offsite.
- **Sign Business Associate Agreements:** Ensure contracts with data providers or service partners specify their responsibilities regarding PHI.
- **Ensure Compliance with Providers:** Verify that any third-party services involved in data collection or processing are also HIPAA-compliant.
- **Regular Staff Training:** Regularly train employees to stay updated on HIPAA best practices.

By following these tips, you'll reduce the risk of violations and ensure HIPAA compliance.

Is Your Data Collection HIPAA-Compliant?

To be HIPAA-compliant, your data collection processes must meet a set of safeguards to ensure the security of Protected Health Information (PHI), whether collected online or on paper. However, relying on paper forms could lead to potential compliance issues, exposing you to civil and criminal penalties. Here's why:

Key HIPAA Safeguards

HIPAA compliance is based on three types of safeguards:



Technical Safeguards



Physical Safeguards



Administrative Safeguards

While paper forms may meet some of these safeguards, they are still prone to vulnerabilities. Let's break it down:

Why Paper Forms Are a Liability:

- **Confidentiality:** Paper records can be easily accessed if someone breaks into the physical storage area.
- **Integrity:** Paper forms are susceptible to damage, like spills or physical wear and tear, which can compromise data accuracy.
- **Availability:** Paper forms can be difficult to organize, making it hard to quickly retrieve data when needed.

Why Digital Forms Are a Better Option:

Digital forms, when managed properly, help ensure compliance with HIPAA safeguards:

- **Improved Confidentiality:** Online systems can securely encrypt data, minimizing unauthorized access.
- **Better Integrity:** Data stored electronically can be backed up and protected from physical damage, ensuring its accuracy.
- **Enhanced Availability:** Digital records are easier to organize and access, improving the speed and efficiency of retrieving PHI when needed.

While paper forms can partially meet HIPAA requirements, digital forms are a much safer, more efficient, and HIPAA-compliant solution. Online forms make it easier to ensure continuous compliance with all necessary safeguards, keeping your data secure and accessible when needed.

HIPAA Compliance Checklist

As mentioned before, there are three main categories of safeguards that enable an entity to stay compliant with HIPAA regulations: technical, physical, and administrative. Below you will find a checklist table you can use to make sure you are HIPAA-compliant. For extensive explanations, take a look at this [glossary of HIPAA terms](#).

Technical Safeguards

Safeguard	Paper Forms	Online Forms
Implement access control	Can be locked, but if the key is lost, access is easy, and intruders are hard to identify.	Unique user IDs ensure traceable and secure access to PHI.
Ensure ePHI authentication	PHI on paper forms requires manual transfer to digital format, limiting authentication options.	Emergency access procedures enable rapid ePHI authentication.
Use encryption and decryption tools	Encryption/decryption isn't applicable unless converted to digital.	All ePHI is encrypted and decrypted for secure access.
Implement activity logs and audit controls	Logs must be manual; human error can compromise accuracy.	Automated logs and controls ensure easy access and reliability.
Enable automatic log-offs on devices	Not applicable unless forms are digitized.	Automatic log-offs secure idle devices accessing ePHI.

Physical Safeguards

Safeguard	Paper Forms	Online Forms
Facility access controls	Achieved through electronic access controls.	Implemented through electronic controls.

Workstation policies	May not impact if data remains on paper.	Easily implemented for all ePHI users
Mobile device policies	Limited impact if data remains on paper.	Easily enforced for ePHI users.
Hardware inventory	Limited impact if data remains on paper.	Easily maintained for ePHI systems.

Administrative Safeguards

Safeguard	Paper Forms	Online Forms
Conducting risk assessments	Difficult without digital safety measures.	Conducted through risk analysis to assess ePHI risks.
Introducing a risk management policy	Some risk measures can be applied.	Full measures to minimize risk.
Training employees to be secure	Can be implemented.	Can be implemented.
Developing a contingency plan	Lost data is often irrecoverable.	Implemented with backups and restoration procedures.
Testing of contingency plan	Not possible for irreparably damaged paper data.	Regular testing and adaptation of plans.
Restricting third-party access	Hard to track with limited traceability.	Managed via passwords and access log reviews.

Reporting security incidents

Relies on human reports.

Supported by digital security tools for detection.

While paper form PHI collection can be somewhat HIPAA-compliant, online forms offer better traceability and security, making your Protected Health Information more secure and improving your overall HIPAA compliance.

Achieving HIPAA Compliance with 123FormBuilder

123FormBuilder is a HIPAA-compliant online form creation platform designed to streamline internal operations securely. The cloud-based solution ensures data backup, access control, and seamless digitization of processes for medical organizations.

With over 15 years of expertise, the 123FormBuilder team collaborates closely with medical professionals to provide scalable, efficient, and secure tools tailored for the healthcare industry. Our solutions cater to various practice sizes:



**Hospitals &
Large Practices**



**Small and
Medium Practices**



**Single
Practices**

Technical Safeguards

123FormBuilder meets the **5 key HIPAA technical safeguard** standards:

1. **Access Control**

- **Unique User Identification:** Each user is assigned a unique username or ID.
- **Multi-Factor Authentication:** Secure login processes ensure only authorized users gain access.

- **Emergency Access Procedures:** Provide alternative methods to access data during emergencies.
- **Automatic Logoff:** Sessions are automatically logged out after inactivity to maintain data integrity.

2. **Audit Controls**

- **Activity Monitoring:** All platform activity is tracked through advanced hardware and software tools.
- **User Access Logs:** Strict logging ensures users access only the data necessary for their roles.

3. **Integrity**

- **Robust Systems:** Collaboration with reliable data storage providers like Amazon ensures that data is protected from corruption or tampering.

4. **Authentication**

- **Verification Protocols:** Rigorous procedures confirm that only authorized users can access Protected Health Information (PHI).

5. **Transmission Security**

- **Encrypted Data:** Information transmitted via forms is secured with SSL protocols and sent exclusively to designated recipients.
- **Reliable Infrastructure:** Secure internal data transmission enhances protection.

123FormBuilder prioritizes compliance and user security while simplifying data collection for healthcare professionals. This commitment ensures that organizations meet HIPAA requirements effortlessly and securely.

Physical Safeguards

The Physical Safeguards section has **4 major standards**, which are:

- Facility Access Controls
- Workstation Use
- Workstation Security
- 123FormBuilder, certified by TÜV Austria, holds ISO 27001:2013, ISO 27017:2015, and ISO 27018:2019 certifications.

These certifications ensure our Information Management and Security System meets stringent ISO 27001 standards and HIPAA physical safeguard requirements. Specifically, we have implemented:

- Acquisition, development, and maintenance procedures for all the systems
- Equipment security procedures

- Device and media control usage procedures in conformity with the information classification scheme

At 123FormBuilder, all equipment is operated under strict security measures to prevent unauthorized access. Facility access is tightly controlled, with entry to specific areas restricted to employees and authorized visitors only.

Administrative Safeguards

There are **9 important aspects** of Administrative Safeguards:

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident
- Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts

Same as in the case of Technical Safeguards, 123FormBuilder's ISO 27001 certification enables us to comply with all the Administrative Safeguards imposed by our HIPAA certification as well. To be more specific, we have implemented:

- A risk management manual
- A risk control identification procedure
- An employee training procedure (regarding all of our security measures)
- A business continuity plan with an emergency procedure and periodic testing
- A third-party restricted access procedure
- Network access control procedures
- System acquisition, development, and maintenance procedures
- Monitoring procedures
- Incident management procedures

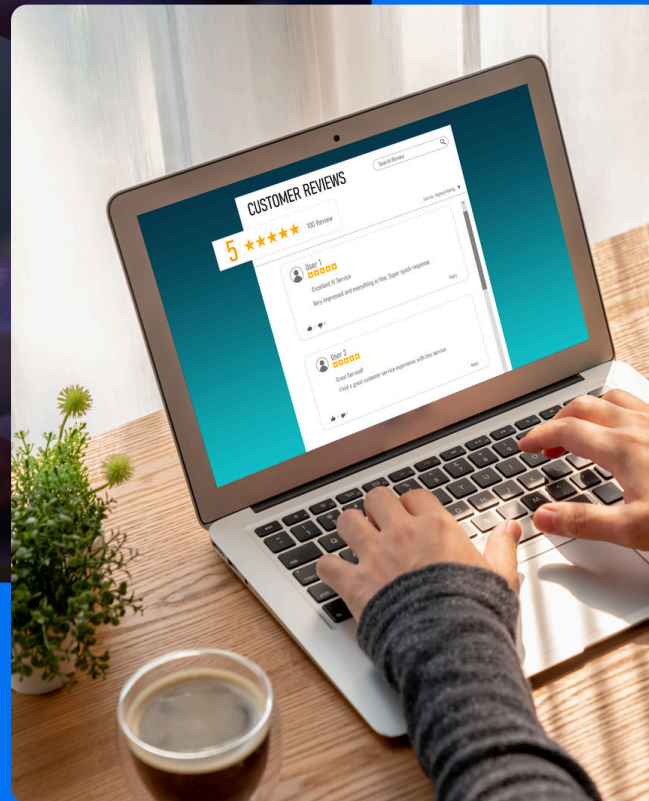
123FormBuilder ensures user peace of mind with advanced security measures, including software, protocols, and contingency plans. Compliant with HIPAA, the platform implements industry-leading security standards. Employees adhere to strict obligations, supported by Bitdefender Endpoint Security for robust workstation protection.

Indemnification, Insurance and Liability

Taking in consideration all security measures that 123FormBuilder implements, being safe also requires the collaboration of our users. That's why 123FormBuilder acts as a Business Associate when performing functions or providing services involving the use or disclosure of PHI. The Business Associate Agreement (called a BAA) is one of the most important requirements of the HIPAA regulations. All covered entities should have this agreement with their service providers.

The level of indemnification and the accepted liabilities are always subject to negotiations. If there is a data breach, or in other words, something goes bad, the Covered Entity should make sure that they can hold the service provider accountable. 123FormBuilder has signed a 5M USD insurance policy to make sure that we can satisfy any indemnification clause.





Customer Success Stories



ENHANCING PATIENT CARE AND COMPLIANCE WITH 123FORMBUILDER

Perfect Patients, a leader in digital marketing for chiropractors, has been a 123FormBuilder client since 2018, serving over 2,500 clients across North America, Australia, and the UK. They specialize in boosting patient acquisition and retention through online solutions.

Perfect Patients needed a secure, HIPAA-compliant solution for handling patient data and streamlining appointment bookings across multiple healthcare systems.

123FormBuilder allowed Perfect Patients to create customizable, HIPAA-compliant forms for patient appointments, including secure payment integrations. This solution ensured seamless, secure data management and patient engagement.

With over 817 forms created and an average of 3.6K submissions per month, Perfect Patients enhanced patient booking processes, improved patient satisfaction, and increased operational efficiency for their chiropractic clients.



We've had a completely positive experience with 123FormBuilder. We highly recommend it — a full 5-star rating!

FINAL THOUGHTS

Managing patient information is a critical healthcare task. HIPAA compliance ensures data security, while partnering with 123FormBuilder provides the tools and expertise to protect patient information and streamline operations.



Contact Information 25%

Patient Intake Form

Name

First Last

Age Gender

Male Female

Address

Street Address

City Region

Postal / Zip Code Country

Email



Contact us for further inquiries

Try 123FormBuilder
for FREE

Ask for a Dedicated
Demo



marketing@123formbuilder.com



www.123formbuilder.com