

Using Highly Sensitive Data in HubSpot for Healthcare



+



www.bridgerev.com

Your Hosts



Ashley Quintana

CEO, BridgeRev

Jerome Simmons

Sr. Product Marketing
Manager, HubSpot



Agenda



- What is Sensitive Data?
- Overview of Sensitive Data in Healthcare
- HubSpot's Sensitive Data Tools for HIPAA Compliance
- HubSpot in Action: Practical Applications for Healthcare
- Tips and Tricks
- Q&A Session

Why Does Sensitive Data Even Matter?

Because we're not just saving lives,
we're protecting people's lives.

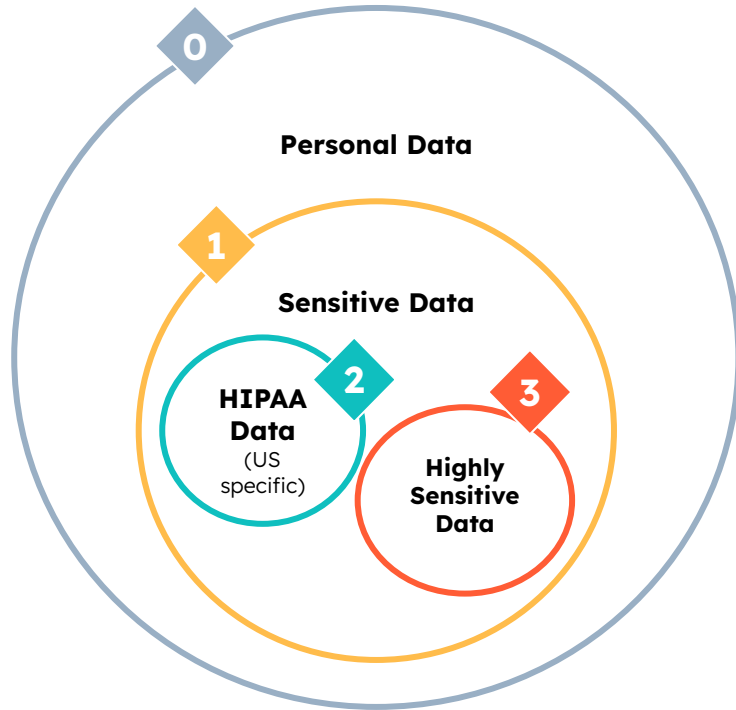
What Is Sensitive Data?

**How We Think About
Sensitive Healthcare Data
In HubSpot?**

What is Sensitive Data?

Sensitive data is **confidential information** that must be **kept safe and out of reach from all outsiders** unless they have permission to access it.

What is Sensitive Data to HubSpot?



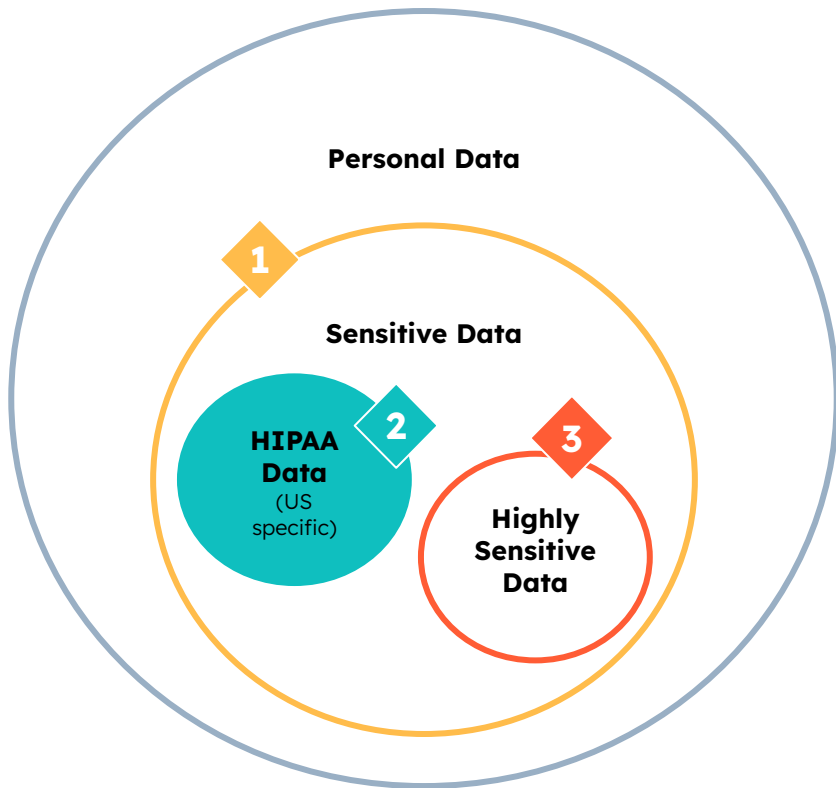
Not all Personal Data is considered sensitive (e.g. first name, email).

HubSpot categorizes Sensitive Data into three buckets based on risk & customer need:

1. Sensitive Data
2. HIPAA Data
3. Highly Sensitive Data

The level of protection needed increases with each category, and requires different legal obligations and product experiences.

HubSpot has also aligned these categories with their product rollouts.



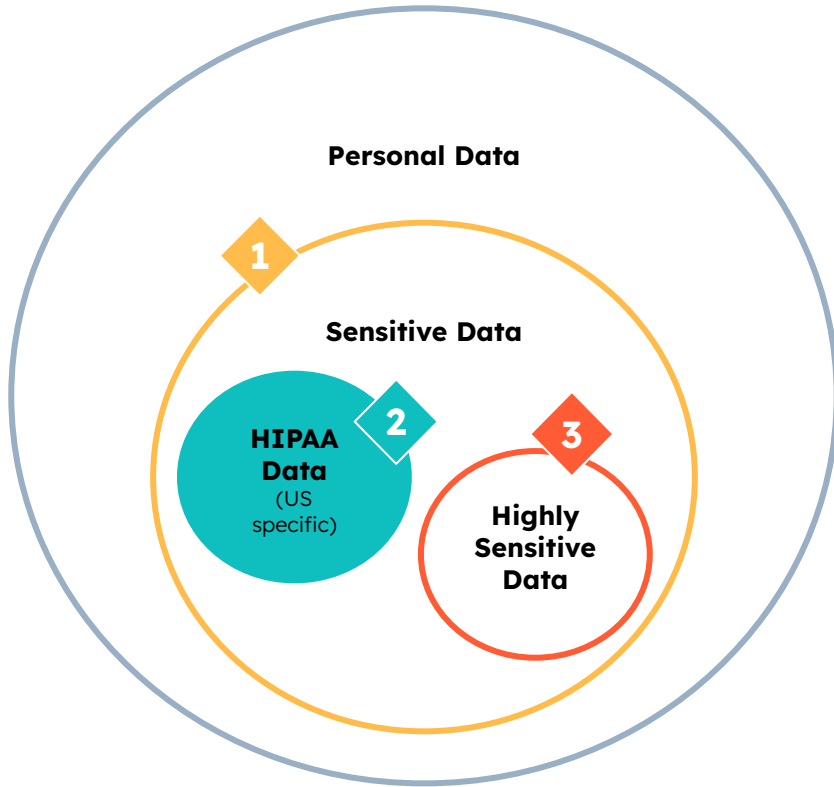
Examples:

- Patient medical records
- Health insurance information
- Billing and payment records
- Laboratory results
- prescriptions
- Health condition information

HIPAA (Health Insurance Portability and Accountability Act) is **a US law** designed to provide strict data privacy and security provisions for **safeguarding medical information**.

HIPAA sets **standards & rules** for the protection and sharing of sensitive patient health information, known as **Protected Health Information (PHI)**

2 HIPAA Data (continued)



- HIPAA applies to **Covered Entities** and their **Business Associates**
 - **Covered entities** are healthcare providers, health plans, and healthcare clearinghouses that handle protected health information (PHI)
 - **A Business Associate** is a person or organization that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involves the use or disclosure of protected health information (PHI)
 - Your customers who are Business Associates will need to sign a **Business Associate Agreement (BAA)** with HubSpot

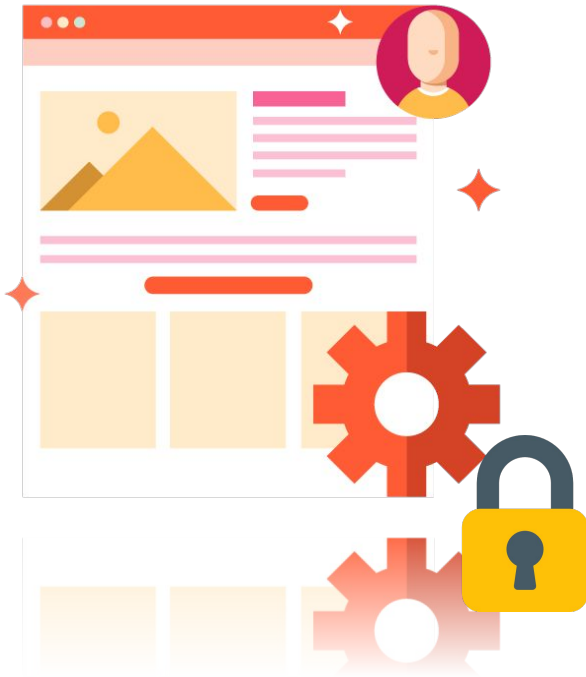
How to use Sensitive Data?

By storing sensitive data in HubSpot Smart CRM, HubSpot offers **an effective way to easily and safely:**

- Fuel your go-to-market engine,
- Manage regulatory compliance,
- and prevent business disruptions.



Fuel your go-to-market engine



- Collect sensitive data manually, via import, forms, APIs, & integrations
- Store sensitive data in properties, attachments, and activities
- Personalize customer experiences through workflows and lists

Manage compliance and prevent disruptions

This Enterprise HubSpot feature provides privacy and security protections enabling customers to store sensitive data in HubSpot and comply with HIPAA regulations.

- Comprehensive audit logging
- Account security recommendations
- Platform layer encryption
- Advanced authentication features
- And more...

Please refer to the [Trust Center](#) for resources on storing sensitive data—including how to ensure that you use our products and services in a way that supports your HIPAA obligations.

Overview of Sensitive Data in Healthcare

How HubSpot Supports *HIPAA Compliance*

- **Encryption:** TLS for in-transit data and storage encryption.
- **Role-Based Permissions:** Access can be restricted to ensure only authorized individuals interact with PHI.

Sensitive Data settings

Protect sensitive data in your account such as personal identification, health information, financial information (excluding account information used for payment processing). [View the full list of permitted data](#) ↗

How sensitive is this data?

This setting affects tool access, settings access, and visibility. [Learn more](#) ↗



Not sensitive

This data doesn't need additional protection



Sensitive Data

This data needs protection, but can be used in most tools and doesn't need to be masked.

Will this property store HIPAA Protected Health Information (PHI)?

Categorizing this property helps HubSpot protect your data. [Learn more](#) ↗



Yes, this data contains Protected Health Information (PHI)

Need to change who can view and edit this property?

View and edit access can be changed in the "Manage access" section.







[Manage access for this property](#)

How HubSpot Supports *HIPAA Compliance*

- **Compliance Support:** In-app BAA and HIPAA support.
- **Audit Logs and Data Retention:** Support HIPAA's record-keeping requirements.

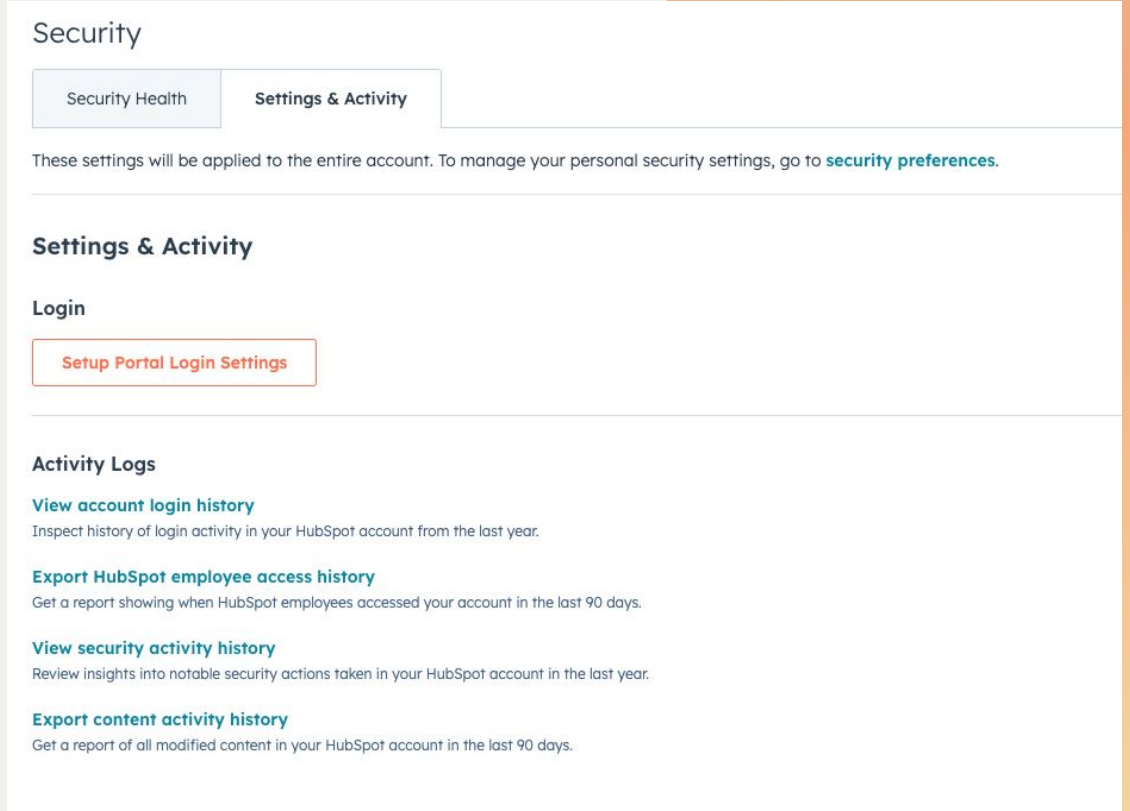
Audit Log

View user actions taken in your HubSpot account over the last 365 days.

CATEGORY	SUBCATEGOR...	ACTI...	MODIFIED BY	DATE OF CHANGE	SOURCE
Login	Login Succe...	Perf...	 Ashley Quintana ashley@brid...	Nov 19, 2024 1:5...	170.89.122.44
Content	Template	Upd...	 Kevin Cornett kevin.cornett...	Nov 18, 2024 1:1...	Partner Home ...
Content	Template	Upd...	 Kevin Cornett kevin.cornett...	Nov 18, 2024 1:1...	Partner Home ...
Content	Template	Upd...	 Kevin Cornett kevin.cornett...	Nov 18, 2024 1:1...	Partner Home ...
Content	Template	Upd...	 Kevin Cornett kevin.cornett...	Nov 18, 2024 11:...	Partner Home ...
Content	Template	Upd...	 Kevin Cornett kevin.cornett...	Nov 18, 2024 11:...	Partner Home ...

How HubSpot Supports *HIPAA Compliance*

- **Compliance**
Workflows: Automate compliance checks and incident reporting.
- **Data Protection:** Data export restrictions, Single Sign-On (SSO), and private CRM records to prevent unauthorized data access.



The screenshot shows the HubSpot Security settings interface. At the top, there are two tabs: "Security Health" and "Settings & Activity". Below the tabs, a message states: "These settings will be applied to the entire account. To manage your personal security settings, go to [security preferences](#)." The main section is titled "Settings & Activity" and contains a "Login" subsection with a button labeled "Setup Portal Login Settings". Below this is an "Activity Logs" section with three links: "View account login history" (with a sub-description: "Inspect history of login activity in your HubSpot account from the last year."), "Export HubSpot employee access history" (with a sub-description: "Get a report showing when HubSpot employees accessed your account in the last 90 days."), and "View security activity history" (with a sub-description: "Review insights into notable security actions taken in your HubSpot account in the last year."). A final link, "Export content activity history" (with a sub-description: "Get a report of all modified content in your HubSpot account in the last 90 days."), is also present.

Security

Security Health Settings & Activity

These settings will be applied to the entire account. To manage your personal security settings, go to [security preferences](#).

Settings & Activity

Login

[Setup Portal Login Settings](#)

Activity Logs

[View account login history](#)
Inspect history of login activity in your HubSpot account from the last year.

[Export HubSpot employee access history](#)
Get a report showing when HubSpot employees accessed your account in the last 90 days.

[View security activity history](#)
Review insights into notable security actions taken in your HubSpot account in the last year.

[Export content activity history](#)
Get a report of all modified content in your HubSpot account in the last 90 days.

HubSpot in Action: Practical Applications for Healthcare

Tips and Tricks

Sensitive Data **Best Practices**



- **Encrypt Your Data**
 - **At Rest:** Ensure all stored data, including backups, is encrypted.
 - **In Transit:** Use TLS to secure data moving between systems.
- **Train Your Team**
 - Educate employees on how to protect sensitive data and recognize phishing attempts.
- **Conduct Regular Audits**
 - Perform routine checks to ensure compliance and identify potential vulnerabilities.
 - Use automated tools to monitor CRM activity for suspicious behavior.
- **Prepare a Data Breach Response Plan**
 - Have a clear plan for immediate actions, notifications, and remediation.
- **Consolidate Your Tech Stack**
 - Having less tools in your tech stack, decreases your exposure to data breaches.

Sensitive Data **Best Practices** (Cont.)



Key HIPAA Requirements for CRMs

- **Privacy Rule:**
 - Ensures that PHI is properly protected while still allowing necessary information flow for quality healthcare.
- **Security Rule:**
 - Requires robust administrative, physical, and technical safeguards to protect electronic PHI.
- **Breach Notification Rule:**
 - Mandates timely notification to affected individuals and authorities in the event of a PHI breach.

Sensitive Data **Best Practices** (Cont.)



Implications of Mishandling Sensitive Data

- **Legal Risks**
 - Fines and penalties for non-compliance with regulations like HIPAA and GDPR.
- **Financial Risks**
 - Data breaches can result in expensive lawsuits and loss of business.
- **Reputational Damage**
 - Loss of customer trust can have long-lasting effects on your brand.

Q&A

Helpful Resources and Events

Interested in a live demo from the HubSpot team - [Schedule some time here!](#)

[HubSpot Sensitive Data Terms](#) - please make sure to review this page before you get started

Start your security review with the HubSpot [Trust Center](#)

Get up to speed with the sensitive data [knowledge base](#)

Get In Touch

Contact BridgeRev

ashley@bridgrev.com

[linkedin.com/in/ashleyegarcia](https://www.linkedin.com/in/ashleyegarcia)

www.bridgrev.com
