1touch.io

Discover Why Healthcare Organizations Require Complete Data Visibility

Introduction

The healthcare sector is one of the most highly-regulated industries in existence. The high value of a patient's medical record to cybercriminals and the sensitive and personal data it stores, makes it imperative that the organizations to whom this data is entrusted correctly protect and secure it against unauthorized access.

To this end, the **Health Insurance Portability and Accessibility Act (HIPAA)** and other regulations have been put in place to outline the minimum security controls that organizations must put in place to secure patient data and their rights regarding their data adequately. As the regulatory landscape grows more complex and requirements become more stringent, maintaining data visibility and regulatory compliance manually will quickly become unsustainable and ineffective.

HIPAA Regulation and Requirements

In the healthcare industry, ***HIPAA*** is the most well-known regulation for protecting the personal data of patients. The law protects many different types of patient data, such as:

- **Names**
- **Birth dates, death dates, treatment dates, admission dates and discharge dates**
- **Telephone numbers and other contact information**
- **Addresses**
- **Social Security numbers**
- **Medical record numbers**
- **Photographs**
- **Finger and voiceprints**
- **Any other identifying numbers**

For these types of protected healthcare data, healthcare providers and their business associates (payment processors and other organizations that may be provided access to a patient's data by the healthcare provider) must implement protections against data breaches and unauthorized exposure. The ***HIPAA Security Rule*** outlines the security controls that an organization must have in place to achieve ***HIPAA*** compliance.

However, an organization's duties under ***HIPAA*** are not limited to protecting healthcare data entrusted to them by its patients or partners. ***HIPAA*** also provides patients with a number of different rights regarding their data collected by a healthcare provider, such as:

Right to Access

The right to request a full copy of their protected health information collected by a healthcare provider.

Right to Correction

The right to request that their stored data be modified to correct errors or add additional information.

Right to Disclosure

The right to request a full list of the organizations to which a healthcare provider has disclosed their data.

Right to Confidential Communication

The right to request confidential communication between themselves and their healthcare provider.

Right to Complain

The right to register an official complaint regarding how their protected data is being collected, used, secured, etc.

Right to a Privacy Policy

The right to be informed of the privacy practices of a healthcare provider, plan or clearinghouse.

Patients can exercise their rights under ***HIPAA*** at any time, and an organization must be prepared to access and/or modify data as needed. This requires full visibility into how data is being stored and processed within an organization.

Healthcare Data Security Beyond HIPAA

While ***HIPAA*** is the most widely known and applicable data protection law for the healthcare sector, it is far from the only one. Healthcare providers and their business associates also may be required to achieve, maintain, and demonstrate compliance with a number of other regulations, including:

HITECH

(Health Information Technology for Economic and Clinical Health Act)

HITECH was designed to encourage healthcare to adopt electronic medical records. It also imposes security requirements beyond those outlined in HIPAA.

PCI DSS

(Payment Card Industry Data Security Standard)

PCI DSS protects the security of payment card information. Healthcare providers and their business associates must comply with the requirements of PCI DSS when storing and processing patients' payment data.

GDPR

(General Data Protection Regulation)

The EU's GDPR is designed to protect a wide range of personal data for EU citizens. If a healthcare provider or business associate is processing the personal data of EU citizens, then GDPR requirements may apply.

CCPA

(California Consumer Privacy Act)

The CCPA is one of many state-level data protection laws designed to give their constituents similar protections to those outlined in the GDPR. Patient data that falls under the purview of these state-level privacy laws must be protected according to their requirements.

Organizations working within the healthcare industry need to have the knowledge and resources necessary to achieve and maintain compliance with all applicable regulations. A key component of this is achieving and maintaining complete visibility into the protected data within an organization's keeping.

The Need to Know Where Your Data Is

It is impossible to protect something that you don't know exists. As corporate networks become more complex and business operations are increasingly "data-driven", protected patient data can be stored and used in a variety of different places.

A failure to maintain complete visibility into this data carries a number of different risks. Two of the biggest risks are regulatory non-compliance and a breach of sensitive data.

Regulatory Compliance

Data protection regulations like ***HIPAA*** and the ***GDPR*** do not have a limited scope. Any information that falls into the "protected" category is covered by these regulations, regardless of where it is stored and used on an organization's networks or those of its partners.

A key component of meeting the requirements of these regulations is the ability to access any piece of data rapidly. Most data protection regulations allow six weeks or less for a response to a subject rights request, and the ***Office for Civil Rights (OCR)***, the regulatory body responsible for enforcing ***HIPAA*** only gives a health care provider ten days to respond once the ***OCR*** has initiated an audit.

These tight response deadlines - and the large volume of data that may need to be collected during them - makes data tracking a must for regulatory compliance. An organization without complete visibility into their data and reliant on manual data discovery processes risks regulatory non-compliance and legal action due to a failure to respond by the deadline or providing incomplete information in response to a legitimate request.

The cost to the organization of such a mistake can far outweigh the expense of implementing proper data tracking within the organization. ***HIPAA*** fines are capped at $1.5 million per violation, but ***GDPR*** fines can reach the greater of 40 million Euros or 4% of an organization's global turnover.

Data Breach Avoidance

A data breach can have a major impact on an organization's ability to sustain operations. The average cost of a data breach in the healthcare industry is $7.13 million, and this does not include the reputational damage that an organization incurs when they are the victim of a breach determined to be caused or enabled by their own negligence.

The healthcare sector has one of the highest rates of data breaches within a particular industry. In 2019, 70% of healthcare organizations reported having experienced a data breach at some point, and a third reported suffering one within the previous year.

In many cases, a major enabler of data breaches is the fact that the targeted organization lacks visibility into their data or does not even know that the breached data existed. Effective breach detection - and mitigation - only requires complete visibility into an organization's sensitive data and the use of access monitoring to track use - and attempted exfiltration - of this data. The fact that many organizations lack one or both of these is the reason that it takes an average of 207 days for an organization to detect a data breach after it has occurred.

Achieving Regulatory Compliance and Data Security with 1touch.io

The ability to track data throughout and beyond an organization's network is essential to ensuring regulatory compliance and protecting against data breaches. Tight regulatory response deadlines and effective incident response both require an organization to know where to look for their data in response to a subject rights request or potential security incident.

1touch.io's Inventa™ provides a usable and scalable solution to an organization's data tracking needs. The advantages that Inventa provides include:

Automated Identification

Sensitive data within an organization's network is automatically identified by matching data to patterns of common types of sensitive or protected data (phone numbers, email addresses, social security numbers, etc.).

Data Flow Tracking

Agents deployed throughout the organization's network track access and movement of sensitive data, providing full visibility into where it is stored and used within the network. This includes identification of flows leaving the network and the partners with access to each piece of sensitive data.

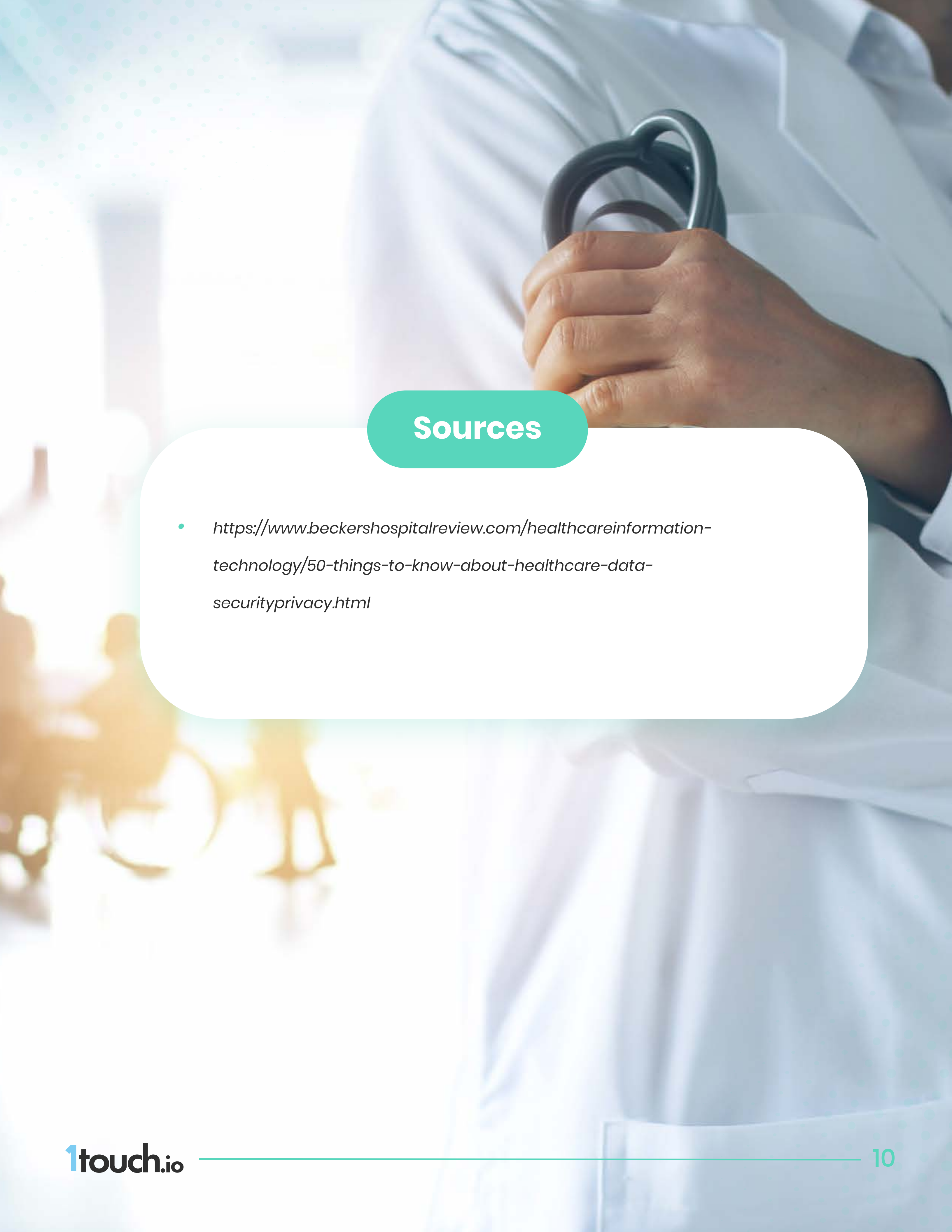
Centralized Data Visibility

The Master Record identifies the full history of data within the network, making it easy to determine where it is being stored and used.

Automated Collection and Reporting

Inventa integrates with web portals for subject rights requests, automatically collecting the requested data and enabling "one-click" responses.

The cyber threat landscape is evolving rapidly, and organizations' regulatory compliance responsibilities continue to expand. ***1touch.io's Inventa™*** provides an organization with the tools required to effectively and sustainably manage their data security and regulatory compliance.



Sources

- *https://www.beckershospitalreview.com/healthcareinformation-technology/50-things-to-know-about-healthcare-data-securityprivacy.html*