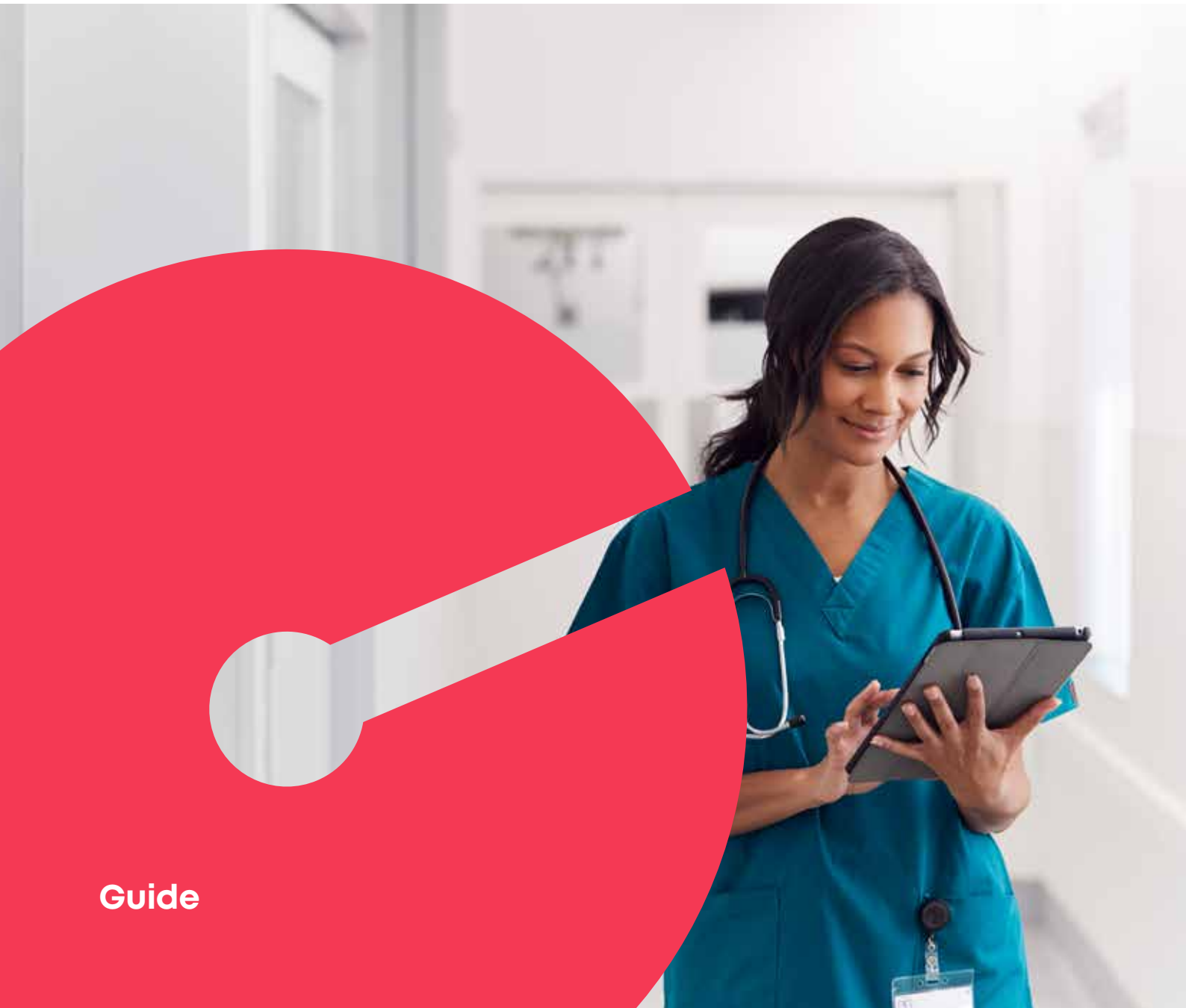
cassie

Mastering data privacy and consent in healthcare:

Your essential guide to the top 10 considerations

What is a Consent Management Platform and can it help healthcare providers tackle their data privacy challenges?



Guide

Why patient data protection is essential?

Patients give consent for healthcare organizations to use their personal data, including information about their health concerns, diet, and medications. Healthcare organizations are responsible for safeguarding this sensitive and valuable data, as data privacy has become more crucial in recent years, and patients are more aware of the need to protect their medical data.

To safeguard patients' information and to use it appropriately, healthcare providers must comply with rigorous standards established by governing bodies and only use it for suitable purposes. These standards include consent forms that patients must sign before medical procedures are carried out and protocols related to storing and sharing information with third parties. It is also essential that healthcare organizations invest in secure systems such as encryption technology and firewalls to protect patient records from unauthorized access.

In addition to securing patient data, healthcare providers have an ethical obligation to respect their patient's wishes regarding how their personal information is used. This includes ensuring consent is obtained before using personal details for research purposes or marketing campaigns. Patients must also be notified if their data has been compromised so they can take appropriate action if necessary.

As well as protecting information from external threats, healthcare organizations should focus on internal security measures such as employee training and regular structured audits of systems used for storing or accessing patient records.

Healthcare providers have a significant responsibility to protect the sensitive personal data entrusted to them by patients. While physical protection measures are important, gaining consent from those whose details are being stored should always remain at the forefront of any strategy designed to keep medical records safe and secure at all times.

The top 10 things healthcare providers should know when it comes to consent and data privacy

1. The importance of sensitive data

Sensitive data is any type of data that contains private or confidential information, such as healthcare records and financial details. This kind of data must be protected to ensure the privacy rights of individuals and organizations. The healthcare industry is responsible for safeguarding this data by using secure methods like encryption technology, authentication techniques, and access control measures.

Protecting sensitive healthcare data is critical since it can contain personal healthcare information that could otherwise be used for malicious purposes. Healthcare providers have an obligation to protect the confidential medical records of their patients, which may include detailed information about their diagnosis, prognosis, treatment history, medications, allergies, lifestyle habits, and more.

Giving healthcare providers consent to collect and store private healthcare data is essential because not only does it ensure that the patient's right to privacy is respected but it also provides them with peace of mind knowing that their sensitive healthcare information is being handled securely.

2. How to maintain patient trust

Patient trust is an important factor in healthcare. It is essential for healthcare providers to ensure their patients feel comfortable and confident that their data privacy is being respected.

This can be achieved by obtaining consent before collecting any medical data and maintaining the security of patient information according to health privacy regulations.

Healthcare providers should also strive to build trust with their patients by communicating openly and addressing data privacy concerns.

Healthcare providers must stay up-to-date on changes in healthcare laws and regulations to remain compliant regarding protecting patient data. By doing these things, healthcare providers can create a trusting relationship with their patients, leading to better healthcare outcomes.

3. How to ensure data protection

Data protection is paramount for healthcare providers, as healthcare data contains a wealth of sensitive information that must remain secure and private. Protecting healthcare data means not only protecting the data itself but also ensuring that healthcare providers have the consent of their patients when collecting and sharing data. Without proper consent, healthcare providers are violating their patients' privacy rights and risking legal action.

Data protection starts with understanding the regulations surrounding healthcare data and its management; healthcare providers need to be well-informed about which laws apply in their jurisdictions. For example, healthcare professionals in the European Union must adhere to the General Data Protection Regulation (GDPR), which sets out strict guidelines for storing and using personal data. In addition to this, organizations should also consider setting up other policies and procedures such as access control procedures and security audits.

Once healthcare organizations understand what regulations are applicable, they need to ensure that their systems are secure enough to protect stored healthcare data from potential breaches or misuse. (In October 2021, Broward Health, one of the ten largest public health systems in the U.S, suffered a data breach that exposed personal info of patients and employees.) This includes installing appropriate firewalls, implementing strong passwords and two-factor authentication protocols, encrypting databases, backing up server data regularly, monitoring user activities on a regular basis, etc. Healthcare practitioners should also take steps towards developing secure communication protocols for sending patient data electronically over public networks like email or messaging applications.

The last, but arguably most important step towards achieving effective data protection is obtaining explicit consent from patients before collecting or sharing any of their private information with third parties.

4. Why accurate patient records are a necessity

Accurate patient records are essential for healthcare providers as they enable healthcare workers to make informed decisions about patient care and treatment.

Accurate records provide healthcare organizations with a comprehensive overview of a patient's health status, including relevant medical information and medication history. By ensuring that healthcare organizations have access to accurate and up-to-date healthcare records, healthcare workers can provide the best care possible.

Having accurate personal records also helps healthcare providers to ensure that they have obtained the necessary consent from their patients before providing them with treatment. When healthcare providers obtain a patient's consent for medical procedures, they are able to confirm that they have received the patient's agreement and that they are providing care in accordance with the patient's wishes.

5. What data regulations affects healthcare

Data privacy regulations are of utmost importance in the healthcare industry. HIPAA and GDPR are two of the most widely adopted frameworks worldwide when it comes to patient data privacy and security.

HIPAA (Health Insurance Portability and Accountability Act) is a US-based legislation that mandates strict security requirements for healthcare providers that store or process personal health information. HIPAA requires healthcare providers to protect the privacy and security of patient data, as well as provides individuals with specific rights regarding their medical records. It also outlines mandatory breach notification requirements for healthcare providers upon discovery of a data breach.

The GDPR (General Data Protection Regulation) is an European-based regulation that gives individuals control of their personal data and sets out rules on how it can be processed by organizations.

Healthcare providers are also subject to GDPR, as it provides an additional layer of protection for patient information and data privacy. It requires healthcare providers to inform patients about their rights in collecting, storing, and using their data.

6. Why staff must be trained to handle sensitive information safely

Accurate patient records are essential for healthcare providers as they enable healthcare workers to make informed decisions about patient care and treatment.

Accurate records provide healthcare organizations with a comprehensive overview of a patient's health status, including relevant medical information and medication history. By ensuring that healthcare organizations have access to accurate and up-to-date healthcare records, healthcare workers can provide the best care possible.

Having accurate personal records also helps healthcare providers to ensure that they have obtained the necessary consent from their patients before providing them with treatment. When healthcare providers obtain a patient's consent for medical procedures, they are able to confirm that they have received the patient's agreement and that they are providing care in accordance with the patient's wishes.

7. The challenges the healthcare sector faces around data privacy

Healthcare data privacy, for all its importance, does face several major challenges.

Modern digital attacks like malware, ransomware, and trojan attacks pose significant threats to digitally interconnected hospital systems. All it takes is one employee opening a suspicious email for a malware virus to enter a medical facility's network. Then it can potentially breach other security barriers and access patient data for the purposes of selling it, stealing it, or corrupting it.

Furthermore, patients who requested their data to be sent to them may not be counted on to keep their data safe. Due to the rise of telehealth software and technology, this risk is likely to increase in the future, especially as people talk openly about their health or transmit unencrypted information over email.

In addition, healthcare data privacy measures and technology must keep up with evolving viruses and hacker strategies. As time goes on, malware viruses, for example, continue to evolve in complexity. Digital security solutions must also grow and become stronger.

8. The consequences of non-compliance

Organizations and legislation like HIPAA and the GDPR impose heavy fines and penalties on healthcare organizations that fail to protect patient medical information properly.

Several organizations have already seen the consequences of running afoul of HIPAA in particular:

- Advocate Health Care Network had to pay a penalty of $5.5 million when 4 million healthcare records were stolen
- CardioNet had to pay a $2.5 million fine when they misunderstood HIPAA requirements, which resulted in them breaching the law
- The Feinstein Institute paid $3.9 million when they stole protected health information from 13,000 research participants

9. The current and upcoming trends regarding data privacy

In healthcare, data privacy is becoming more important. Companies and healthcare providers are taking steps to make sure that private information stays safe.

They are also finding new ways to use this data in helpful ways. This means that healthcare providers can use data to improve their services, create more personalized treatments, and develop better healthcare solutions.

Additionally, healthcare providers are investing in technology that helps protect patient data from unauthorized access or misuse. This includes encryption of sensitive data, as well as ensuring that only authorized personnel have access to it. Healthcare providers also need to have strict policies in place to ensure that healthcare data is kept private and secure. This includes putting in measures such as requiring passwords, two-factor authentication, and regular backups of healthcare data.

By taking these steps, healthcare providers can ensure that they are keeping with the advancements in patient consent and data privacy.

10. Why SaaS platforms are used to store and protect health records

SaaS platforms are increasingly being used to store and protect health records due to the security measures they offer.

These platforms provide an added layer of security, allowing only authorized users to access sensitive information. Most SaaS providers use cloud computing technology, which means that data is stored in a secure, off-site location and can be accessed from any device with an internet connection.

This makes it easy for treatment departments to manage patient records, through user level access across multiple locations in a secure environment.

Can Consent Management Platforms help healthcare providers achieve these goals?

Consent Management Platforms (CMP) safeguard patient data. They exercise control over information access and ensure data is always managed, stored and used compliantly in the right way. Ideally suited when real-time data matters and when managing complex and high-volume data.

A CMP will record and make sure that health information remains up-to-date, allowing for quick access when needed. This helps medical staff quickly access patient records in order to provide better care. With the help of these platforms, healthcare organizations can ensure that all users are aware of their responsibilities and remain compliant with regulations.

Furthermore, these platforms provide a secure way to store patient data so that it is not vulnerable to cyber-attacks or misuse. This ensures that patient data remains safe and confidential while still allowing medical staff access when needed.

What is Cassie and is it the right CMP for you?

Cassie is the Consent and Preference Management platform for organizations processing complex and high volumes of data, they rely on Cassie to build stronger customer relationships through the respect of individual choices.

We believe that customers should be in control of their data. We build stronger customer relationships by respecting individual choices and driving deeper insights through enhanced preference management.

Our advanced preference management system allows for the auditable capture of brand, pricing, channel, relationships and other important customer choices. We apply customers' preferences across your communications channels in micro-seconds.

We go beyond compliance. If granular detail matters: Cassie delivers.

Cassie helps healthcare providers go beyond compliance

Cassie gives healthcare providers the opportunity to focus on building patient trust and achieve the following goals:

- **Ensure full HIPAA and GDPR compliance (and any other regulation that affects them)**
- **Ensure that patients' personal data is securely stored**
- **Provide a complete audit trail of all access permissions and changes**
- **Provide a convenient way to track, manage, and share sensitive data securely**
- **Better understand how patient data is being used and ensure that it is used appropriately**

Don't just take our word for it...

> **Cassie has solved a lot of issues that we had in previous tools. It's been instrumental in helping us centralize all our patient information. Cassie enables us to have confidence in our data whilst achieving HIPAA compliance.**
>
> Senior Data Protection Officer, Pharmaceutical Company

Get closer to every patient with unlimited metadata

If you would like to learn more about how Cassie helps healthcare providers manage consent while surpassing their compliance goals read our expert blog:

Implement Cassie on your terms

At Cassie, our team partners with you to understand your data flow and help you integrate your systems as your business expands. With Cassie, you have complete control and customization options, as well as the assurance of sustainable, long-term solutions.

Book a Cassie demo to see that you can manage compliance according to your business rules.

Be on the right side of the future

If you'd like to learn more about how we can help you on your healthcare compliance journey, our team of dedicated consent and preference management experts will be able to guide you every step of the way.

UK Office

0800 368 7842
+44 20 4551 9501

US Office

+1 844 585 6264

Australia Office

+61 2 5119 5048

info@trustcassie.com

trustcassie.com/contact

cassie