

GDPR Compliance Challenges for Healthcare Providers: How to Avoid Them

The GDPR has brought into play a multifaceted regulatory regime for healthcare providers to work their way through, balancing the compliance imperative with the need to safeguard highly sensitive patient information. Here are ten common challenges healthcare organizations face regarding GDPR compliance and their detailed elaboration, followed by strategies to avoid such pitfalls.



Photo by Hush Naidoo Jade Photography on Unsplash

1. Obtaining Explicit Consent

One of the major challenges under the GDPR is consent from the subjects themselves-the patients-before any processing takes

place. This consent has to be clear, informed, and unambiguous, something quite hard to achieve in an often- hectic health environment. Sometimes, what patients sign for in consent forms is not exactly what they had in mind, partly because the information may be conveyed through difficult legal terms. Additionally, healthcare providers often depend on presumed consent given the nature of their practice, which falls short of the standards expected under GDPR.

Robust consent management systems would help healthcare providers avoid this pitfall. These can organize the process of consent solicitation and documentation in such a way that their validity would meet GDPR standards. Regular training about the importance of consent and how to obtain it helps staff enhance compliance.

2. Data Minimization

The principle of [data protection in healthcare](#) requires the collection and processing of only the minimum amount of data for certain purposes, but this is a principle that by far and large many healthcare providers are failing at. This counterproductively exposes data to an increased risk of being breached, among many other difficulties in attaining compliance.

For example, the avoidance of over-collection requires organizations to run periodic audits of their data collection practices with the help of an [outsourced data protection officer](#), so that the said processes can be refined to meet the principle of data minimization. This will reduce the chances of being considered non-compliant.

3. Data Transfers

It becomes quite problematic to transfer personal data outside the EEA due to strict regulations under GDPR. Many healthcare

providers remain in a dilemma regarding the compliance with these requirements if they have to share health information with any international partner or use cloud services hosted outside the EEA. Penalties for such non-compliance are very severe.

The barrier can be bridged by first familiarizing the organizations with the legal frameworks regulating international transfers of data. It may be by using SCCs or possibly the regime of ensuring that the third-country recipients maintain an adequate level of data protection.

4. Lack of Staff Training

A difference in IT knowledge among healthcare staff leads to a non-uniform understanding of GDPR requirements, raising the likelihood of data breaches. In the absence of any formal training, employees might inadvertently leak personal data or not recognize various risk factors to personal information.

Healthcare providers should invest in holistic training programs focused on compliance with the GDPR and data protection best practices. Workshops and regular updates will keep all staff abreast of their responsibilities regarding patient data security.

5. Data Breach Notification Requirements

In the case of breach of GDPR, the affected individuals and authorities should receive a notification within 72 hours. Numerous healthcare organizations face challenges in making timely breach notifications because of unclear procedures or unpreparedness for the incidents. Delays in notifications lead to considerable fines and damaged reputations.

The risk here should be minimized through the development of a

clear incident response plan that tells an organization what to do in case a breach occurs. Such procedures have to be regularly drilled with the staff so that timely actions can be taken if needed.

6. Data Protection Officer

The other challenge is the appointment of a Data Protection Officer, responsible for overseeing the compliance effort and serving as a contact point for patients and regulators alike. Finding competent personnel is a challenge most healthcare providers face due to the shortage of qualified professionals who have experience in both health care and data protection law.

This is often an effective option, particularly for organizations that may not have all the relevant expertise in-house. An outsourced data protection officer can bring that knowledge and experience without any conflicts of interest, and thereby effective compliance.

7. Conducting Data Protection Impact Assessments (DPIAs)

DPIAs are crucial in establishing risks likely to occur from the processing of personal information, especially when there is an introduction of new technologies or processes that may affect patient privacy. Many healthcare providers fail to do this because they either lack awareness or means to operate this.

In order to enhance data protection in healthcare industry, organizations should incorporate DPIAs into planning for projects. This means they can perform any necessary assessments before launching new initiatives, and subsequently apply measures to reduce any impending risks proactively.

8. Assurance of Data Security Measures

The healthcare organizations in developing countries usually do not provide an adequate security system that can protect sensitive patient information from unauthorized access. Increasing cyberattacks have enhanced awareness for security protocols in healthcare systems.

It is for this reason that a variety of cybersecurity solutions, including encryption and DLP tools, need to be invested in. Periodic security testing and patching will keep the guard up and maintain compliance with the GDPR against dynamic threats.

9. Patient Rights Requests

Patients have several rights under GDPR, including access to their data and the right to erasure (the right to be forgotten). Healthcare providers may struggle to manage these requests efficiently due to inadequate systems or lack of understanding about how to respond appropriately within required timeframes.

Having a centralized system for tracking and responding to patient rights requests can manage the process much easier. Having clear policies and procedures regarding staff dealing with such requests will ensure timely responses that also help build trust among patients.

10. Record Keeping for Compliance

The GDPR requires recordkeeping of the data processing activities of a company in great detail. It is often cumbersome for healthcare providers to manage the kind of documentation burden coming out of data handled every day.

This, on one hand, calls for a proper documentation strategy from the organization, comprising regular updates on the processes of data processing and compliance. It is advisable to make use of digital tools regarding recordkeeping and thereby further the process with ease and accuracy to avoid [breach of GDPR](#).

Key Takeaways

In summary, while GDPR therefore challenges healthcare providers at many points in the protection of health data, proactive measures may significantly reduce risks. Focusing on consent management, staff training, robust security measures, and effective documentation, healthcare organizations can successfully navigate the complexities of compliance with GDPR while protecting sensitive patient information from breaches and other risks related to non-compliance.