HEALTH DATA COMPLIANCE CHECKLIST

When the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA 2018) went into effect in 2018, companies doing business with UK and European Union (EU) citizens scrambled to ensure they were in compliance, frantically trying to implement data protection changes to be in line with privacy requirements. Since then, several additional data protection legislations have been proposed and/or implemented: Data Governance Act, Data Act, Network and Information Systems Directive (NIS), and most recently, the European Health Data Space Regulation (EHDS).

So, how can you navigate this rapidly changing landscape of regulations and compliance efforts? You lean on known best practices and employ technologies that ensure health data processes comply with regulations and maintain data security—now and in the future.*

*Please keep in mind that nothing on these pages constitutes legal advice. We recommend you speak with an attorney specialised in data protection compliance who can apply the current and future data protection laws to your specific circumstances.

Meet Health Data Compliance Requirements and Save Time on Audits

With Rubrik, you can improve your data security readiness to meet health data regulations. Rubrik makes regulatory compliance simple and efficient with a single platform that delivers data management on premises and in the cloud. It enables users to automate data protection policies and expiration while providing full transparency regarding where the data resides and how policy compliance is met across the entire infrastructure.

Contact us to learn more about how Rubrik is preparing organisations and aligning with current and future data protection regulations in and outside the European Union on our continued mission to secure the world's data.

Scan here to learn more

7 STEPS TO HEALTH DATA COMPLIANCE

rubrik

1 Identify Roles and Responsibilities

Provide clearly written and defined roles and responsibilities explaining who is accountable for each step on the road to compliance. Examples include who will be responsible for identifying how sensitive health data is currently being collected and used, how current data policies and controls facilitate the use and distribution of personal data, and how patients can currently request access to and deletion of their health data.

2 Perform Gap Analysis

Review current data protection policies and the implementation of those policies to identify the purposes of health data processing, what kind of health data you process, who has access to it in your organisation, what third parties that have access (e.g., Epic, Cerner, McKesson, BigHealth) and from where, what you're doing to protect your health data, and for how long you plan to store it before auto-erasing it, if ever. Match your results up against the compliance requirements of current and future data protection regulations to identify areas in need of action.

3 Build Your Action Plan

Establish a timeline for priorities, steps, and actions needed to obtain and sustain compliance with current and future health data protection regulations keeping in mind the law, data security, accountability, governance, and privacy rights.

4 Get The Business Buy In

Raise awareness at the board level to ensure your organisation's leaders buy in to and support the necessary changes required to enact data protection compliance. It is critical that healthcare organisations take all the necessary steps to ensure that health data, intellectual property, and other business-critical data are secured accordingly to avoid facing significant financial penalties, not to mention reputational damage—and loss of life.

5 Educational Awareness

Raise awareness among staff—users, IT professionals, management, etc.—of the changes imposed by applicable data protection regulations and your staff's responsibility towards those regulations. Employee training on all aspects of data protection principles and internal policies regarding data management is a critical part of ensuring that healthcare organisations are meeting data protection regulations while safeguarding the sensitive data that individuals have entrusted to the organisation.

6 Reform Information Governance Frameworks

Ensure your information governance (IG) frameworks are compliant. Revise IG policies, such as data retention, access and deletion policies, data management, classification and storage procedures, disaster recovery, and security protocols for digital and paper-based sensitive records, including proactive monitoring to identify potential vulnerabilities, data breaches, over-privileged access, and unauthorised access attempts and procedures, to bring these in line with current (and future) requirements.

7 Audit, Audit, Audit

By establishing a regular schedule of audits, you can ensure that you are meeting regulations while safeguarding the sensitive data that individuals have entrusted to your organisation. To maintain regular audits and keep compliance simple and efficient, consider deploying a single platform that delivers data management on premises and in the cloud. It enables users to automate data protection policies and expiration while providing full transparency regarding where the data resides and how policy compliance is met across the entire infrastructure.