mobidev

8 steps to ensure healthcare software HIPAA compliance

MobiDev has been developing healthcare software since 2009. We have experience in GDPR and HIPAA compliance to help our clients increase patient trust. Each project is unique and it is impossible to describe a single technical solution for everyone. However, here is a list of the most common practices for ensuring HIPAA compliance.

Alex Vasilchenko
Solution Architect

01 Hosting

- [ ] Server hosting must be HIPAA compliant. A hosting provider must sign a Business Associate Agreement (BAA) with the product owner.

02 Sensitive Data Protection

- [ ] Determine which data that you use in your project is highly sensitive and which is less sensitive. In the case of medical projects, highly sensitive data is classified as Protected Health Information (PHI) and must be encrypted in a database.
- [ ] Only encrypted records should be transferred. The typical solution is to use SSL encryption for HTTPS protocol.
- [ ] Every case of access to sensitive records must be logged (including modification and deletion). It should be possible to find out who had access to sensitive records and when.

02 Sensitive Data Protection

- [ ] If your project involves integration with third-party AI services and APIs (such as OpenAI), be aware that they are typically not HIPAA compliant by default. If you send PHI to such third parties, you may need additional security strategies specific to each use case. This may include anonymizing data before it is used in AI models and only working with AI providers willing to sign a BAA.

03 Backups

- [ ] There must be a disaster recovery strategy in place. Data must be able to be restored from a backup. Ideally, backups should be duplicated in different locations and must also be encrypted.

- [ ] There must be a way to fully dispose of data for certain users. This often means replacing sensitive fields with fake data if complete deletion isn't possible. Alternatively, removing data entirely and setting backups to expire can work.

04 Development Security

- [ ] The development environment must be completely separate from production. For example, if developers need sample data to test the system, they must have no way to load production database records to their machines. If it's important to copy production data to the development environment to reproduce some specific issue and fix it, developers should use data anonymization techniques.

05 Access Control

- [ ] Typically secured systems would also have role-based access control (RBAC) implemented. It would allow users to be grouped by roles with limited permissions.

06 Secure Authentication

The authentication process must be secured. There is no unified way to achieve this, but there are a lot of good practices to use:

- [ ] Login with a strong password
- [ ] Password is hashed in DB
- [ ] Two-factor authentication must be used
- [ ] Allowlisting IPs can be used (e.g. disallowing access outside of a certain network for most critical operations)
- [ ] Automatic logoff. The session must expire if the user leaves their computer/device for a certain time.

07 Image Protection

- [ ] Sometimes images or PDFs are classified as or contain sensitive data. For example, MRI scans. This type of data must be prevented from being cached in the browser.

08 HIPAA Requirements for Mobile Application

- [ ] Local data must be encrypted.
- [ ] Users must be authorized before getting any data (important in case their phone is stolen).
- [ ] Data transmission must be encrypted.

Feel free to contact us!

if you need assistance in ensuring HIPAA compliance for your software product

Healthcare app development services

Calendly

+1 916 243 0946

(USA/Canada Sales Department)

10 a.m. - 7 p.m.