

How did we helped telehealth firm decoded **HIPAA** requirements for mobile app?



Theorfrare

How We Assisted a Development Firm to Fill 47 Security Gaps to Develop a HIPAA Compliant Healthcare App?

A healthcare app or any other digital healthcare product stores and shares many crucial PHI of patients and their family members. To ensure the security of ePHI, federal and state governments have imposed many laws and regulations which should be adhered to. These regulations require expertise for implementation.

The Project

A Canada-based app development firm which has been developing a healthcare collaboration platform to streamline communication between different healthcare entities, owned by a group of physicians approached SyS Creations to decode the complex PHIPA and HIPAA compliance rules & regulations, carry out gap analysis and implement the ways to ensure the ePHI security to be compliance-ready. We discussed requirements broadly. The app development firm and healthcare startup owners had many common concerns related to healthcare compliance.



 Industry	: Healthcare
 Location	: Ontario, Canada
 Employee	: 10-20
 Year	: 2020
 Service	: Compliance Consulting

Objectives & Problem Statements



01 Decode HIPPA & PHIPA Regulations

Carry out security standard audit, asset & device audit, and security risk assessment and discover the app security gaps which leave ePHI open for unauthorized users.

02 App Security Gaps Discovery

Find out the easiest and workable solutions to fill those security gaps and Identify the high-risk security gaps followed by advanced security solutions to eliminate them.

03 Security Audits

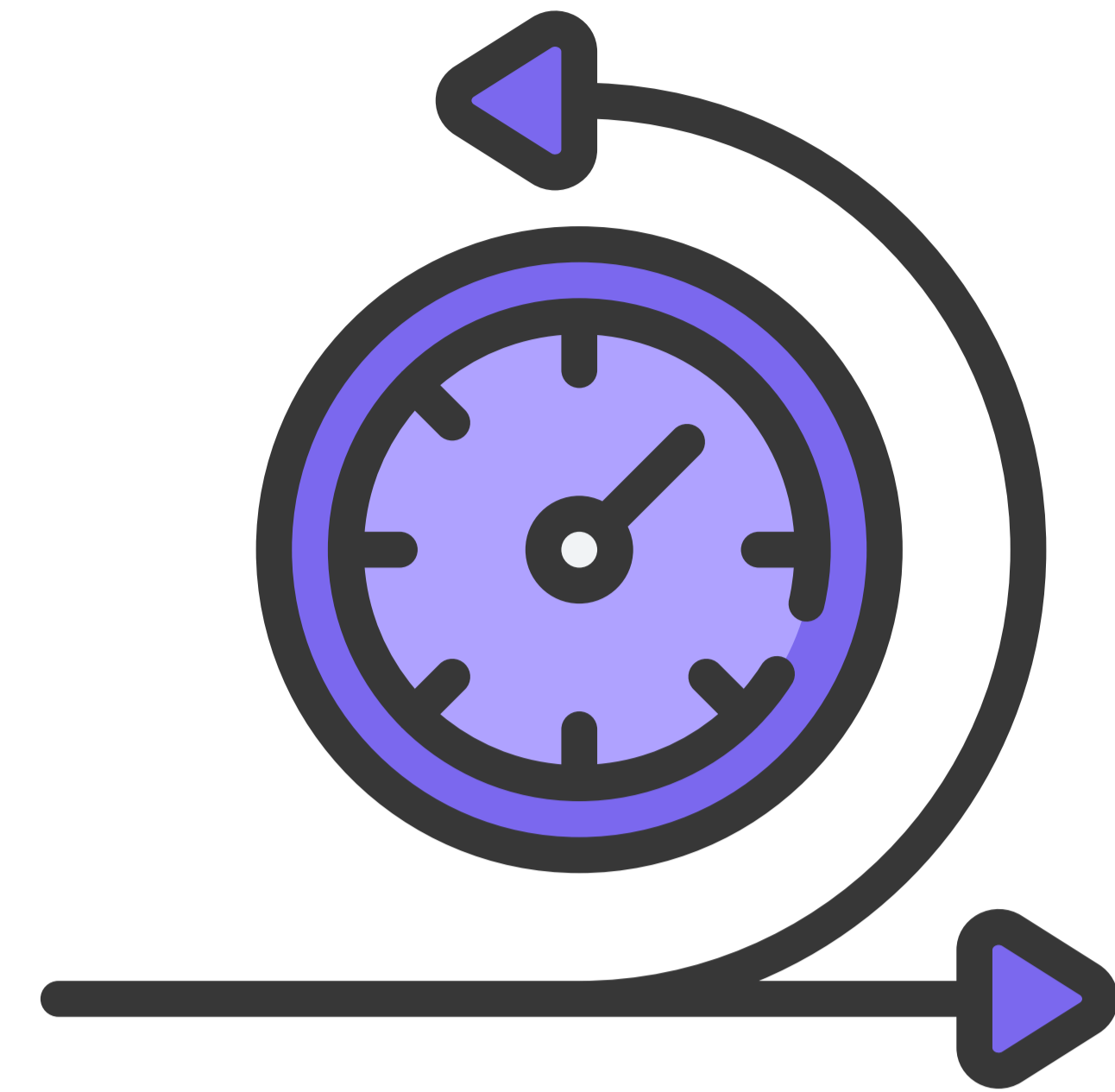
Gain an ability to track the data breach and define a post-breach process.

04 Security Risk Assessment

The app should also meet secure healthcare app requirements suggested by individual regulatory bodies such as the College of Nurses of Ontario and Royal College of Physicians and Surgeons of Canada.



The Action Plan



01 Requirement Gathering

Our healthcare compliance team understood the workflow and architecture of the admin app as well as the patient app with deep-dive analysis of the application.

02 Deep-Dive Analysis of Application

The team carried out a security standard audit, asset & device audit, security risk assessment and gap analysis to find out app security gaps.

03 Networking Hardware Configuration

Healthcare compliance experts planned the HIPAA/PHIPA compliance strategy and prepared a straightforward gap analysis document.

04 Post-Breach Strategy Documentation

The document contained the current state of the app, detailed information, required state of the app, HIPAA/PHIPA standards, and necessity to achieve required state. The following is one such example.

05 Compliance Strategy Planning

With the help of our cloud and the network security team, the healthcare compliance team defined a personalized way to discover the data breach and documented a post-breach process or strategy.

The Outcome



01 Security Gaps

The client has filled 47 security gaps in the healthcare collaboration platform.

02 ePHI Security Standards

The platform is meeting the ePHI security standards imposed by individual regulatory bodies.

03 Data Breach Acknowledgment

The client gained the ability to discover the data breach.

04 Post-Breach Strategy

With a defined post-breach strategy, the client can act professionally and legally in the case of a data breach.

05 HIPAA/PHIPA Compliant App

The ultimate outcome was a HIPAA/PHIPA compliant healthcare platform.