Secure Healthcare Data Intake & Access

Data Access, Data Protection, and Secure Data Intake

Challenge

A large healthcare institution in Europe wanted to improve customer experience, reduce costs, and accelerate the data intake process for their donor program — all while achieving full compliance with GDPR and without compromising health data integrity. The donor program involved external, licensed physicians approving donors on the program. The incumbent process required that physicians have access to paper copies of application data, which diminished the speed of the overall approval process and proved to be an inconvenience for the physicians.

The client was looking for a solution that enabled authorized users to gain remote access to necessary targets with utmost security. This required a digital touchpoint for taking in and storing health-related information in a compliant and secure manner. Due to the sensitivity of the data, access and ability to download the information needed to be limited to those employees with “need-to-know” privileges.

Solution

The implementation included a secure digital touchpoint for collecting sensitive personal data from applicants in a structured manner over the internet, as well as facilitation of the encrypted storage and sharing of data. The solution also involved establishing stringent access management and user authentication systems that minimize the risk of human error and the mismanagement of personal health data.

How Does it Work?

1. Applicant completes secure, pre-formatted application form on company website.
2. Inputted data travels over a securely tunneled connection to the Deltagon Suite where it is encrypted and stored in a dedicated room. Access to the room is limited to authorized personnel only.
3. Authorized room personnel receive a secure email message notifying them of new applications.
4. To access the room, authorized persons are subject to two-factor authentication.
5. Application may then be processed and transferred to a licensed physician for final review.
6. Licensed physicians authenticate themselves with their medical practitioner's official authentication card by visiting a dedicated webpage and entering their username. This grants them access to the room, where they may provide final approval on applications.
7. Approved applications are moved to another system for permanent storage and the applicant is notified via secure email.
8. The notification email includes a link, which takes the applicant to a secure gateway holding the email content (informing the applicant of their application status) in encrypted format until opened by the applicant.
9. If the applicant has follow-up questions, they can reply securely to the email.
10. An audit trail is available for the purposes of tracking how secure data is being accessed and interacted with.

Results

External digital touchpoint, improved customer experience, improved automation with best available security, and the ability for privileged users to maintain file storage without compromising data security.

Let's get to know each other

Want to find out more about how we safeguard mission-critical data in transit, in use, and at rest for leading organizations around the world? We'd love to hear from you.

Request a Demo

SSH