TeloChain

Information Security & Privacy Whitepaper

v1.0

Table of Contents

Commitment to Privacy & Security

At TeloChain, we are team of professionals around the world with deep expertise in business strategy, statistical analysis, healthcare, and technology working to improve outcomes through smart solutions to complex problems. At the heart of what we do is the desire to help improve healthcare efficiencies in order to positively influence patient outcomes. This may be through retrospective analyses of healthcare claims, workforce multiplying software deployments, or patient enrollment acceleration for clinical studies; no matter how we might help you or your organization, we understand that we have to earn and maintain your trust. That's why the TeloChain team works tirelessly to ensure the safety of our clients' and patients' protected health information ("PHI") with stringent security policies and practices.

Data security is built into everything we do. In order to ensure data security and uptime for our clients, our platforms are built within only the most secure and tested Technologies. End-to end encryption, access controls, physical security, and employee training are foundational to our culture of compliance. Additionally we have a dedicated team that works to constantly evolve the security commitments of our company through the best partners in the information security industry, ensuring that you can keep your patients' trust, now and in the future.

How TeloChain Protects your data

Almost every week we hear about major breaches in data security. People all over the world seek to exploit weaknesses in cybersecurity practices to steal sensitive information. That's why we have built our business on practical security measures that ensure our data are protected using the highest security specifications to prevent access, and, also, enforcing protections to ensure that in the unlikely event of an intrusion, all sensitive data are encrypted at rest, making the PHI unusable.

Encryption

Encryption is the number one way we can protect data. Encryption at rest ensures that, in the event someone could breach our network or computers, there would be nothing to see. At TeloChain, we encrypt all data exceeding all NIST 800-111 standards.

Additionally, we realize that PHI data must be transmitted, sometimes multiple times depending on the needs of the client. As it travels from the patient's web browser to our secure servers and/or on to our clients' data centers, PHI is potentially vulnerable to eavesdropping, tampering, and forgery. Encryption in transit (encrypted with at least 256 bits of key in a TLS or 2048 Bit

SSH, exceeding NIST 800-52 standards.) ensures authentication, confidentiality, and data integrity as the data travels between applications.

Access Controls

Most breaches occur because of human error. In order to best protect the systems and data entrusted to us, we limit access through tight controls and the due diligence of our team.

- Due diligence through background checks, ensures that everyone that works on our team has been vetted before being given access to our back-end platform or any of your data.
- Multi-factor authentication protects your data from the possibility of theft through password fraud
- Access is logged and monitored with alerts for any unusual activity to ensure that we would recognize and respond quickly to a breach if someone managed to get through our secure defenses.
- Role based access control ensures only the minimum necessary access - limiting the probability of a breach.
- Privileges are revoked when they are no longer necessary so that we always keep access to a minimum to protect our clients' & patients' privacy and security

Redundancy & Backups

- Storage in multiple highly secured geographical locations ensures that you have access to your data or software solution even in the event of a natural disaster or other emergency.
- Source codes are kept separate with backups of each code change, protecting you from long down times in the event of a issue with a new update. It should be noted, that TeloChain also has extensive testing protocols before releasing software updates and that we work with all clients to schedule any updates based on their needs.
- As extra assurance for data integrity, document authentication can be provided through our immutable, distributed digital ledger.
- Data storage flexibility allows you to choose whether data will be stored in servers under your control or using TeloChain's secure storage options and when the data will be securely destroyed according to NIST 800-88 standards.

Training

Understanding cyber security is a complex process. That is why we train every person working for us in TeloChain's compliance expectations and the reasons why they are important. Additionally, we update our policies and training as newer technologies become available and monitor compliance through our mobile device management program. Keeping our team knowledgeable around security and compliance is just the way we do business. Monitoring how we implement our policies is how we keep your sensitive information protected.

Security Management

Having controls in place is only the first part of ensuring privacy and security. That's why at TeloChain, we don't assume everything is working as intended. Constant vigilance, partnered with comprehensive emergency plans, ensure that your business services and patient data are safe in our hands.

Continuous Monitoring

If someone is attempting to intrude into our system, we should know about it and address the threat before there is a breach. We work with partners to provide continuous monitoring, alerts for any unusual activity or non-compliant devices, and regular comprehensive testing for all of our services. In this way we can address the issue quickly providing uptime and safety for our clients.

Business Continuity & Disaster Recovery

Sometimes the threat isn't another person, it is a man-made or natural disaster. At TeloChain we mitigate these threats by having all data replicated in servers in different geographical locations across the US. Additionally, we have built out and tested comprehensive emergency preparedness strategies to get all of our business services back up and running as quickly as possible in the event of a disaster. The processes we have established specify a course of action, individual responsibilities, a secondary support network, and comprehensive documentation strategies that help us build stronger processes in the future. Events that directly impact our clients are always given the highest priority.

Policies

TeloChain has adopted policies to ensure the safety of your data. These include the following:

- Privacy Policy: Sets guidelines on the ways we protect the privacy of all data we collect, including applying minimum necessary access and de-identification principles for all PHI.
- Security Policy: Lays out a structure for risk assessments and principles that ensure information security.
- Breach Notification Policy: Instructs our team on what to look for and how to respond in the event of a suspicion of breach.
- Social Policy: Sets guidelines for data security and confidentiality in the context of social media outlets.
- Cloud Policy:Lays out minimum requirements to guide our company in decisions about cloud based partnerships

- Mobile Device Policy: Instructs our team on acceptable uses, settings, and care of mobile devices including limitations on when and where any company data can be accessed, setting the stage for our mobile device management platform.
- Contingency Framework: Includes our Data Backup Policy & Plan, Disaster Recovery Policy & Plan, Emergency Mode Operations Policy & Plan, and our Testing and Revision Procedures.

If you would like to learn more about our commitment to compliance and the policies that establish our roadmap for information security, please reach out.

Commitment to Compliance

HIPAA, HITECH/ARRA, ACA, Omnibus Rule

Having a robust compliance framework including policies, procedures, monitoring, and regular assessments, ensures that we are meeting all compliance rules for these comprehensive healthcare security standards. We have partnered with Expresso Risk Assessments to build policies and a risk assessment framework to offer you the highest level of security and privacy for your company and your patients.

As an additional layer of protection, we have adopted the Microsoft Azure HITRUST certified Health Analytics Blueprint for all of our service and storage offerings. (View the HITRUST certification here.) Our BAA with Microsoft Azure ensures that MS Azure is as dedicated to privacy and security as we are.

SOC2

The AICPA compliance standards for storing customer data on the cloud incorporates 5 “trust service principles” - Security, Privacy, Confidentiality, Processing Integrity, and Availability. TeloChain also works to meet all standards of the SOC2 guidelines, providing the framework, monitoring, and incident handling to exceed all of our clients expectations for patient trust.

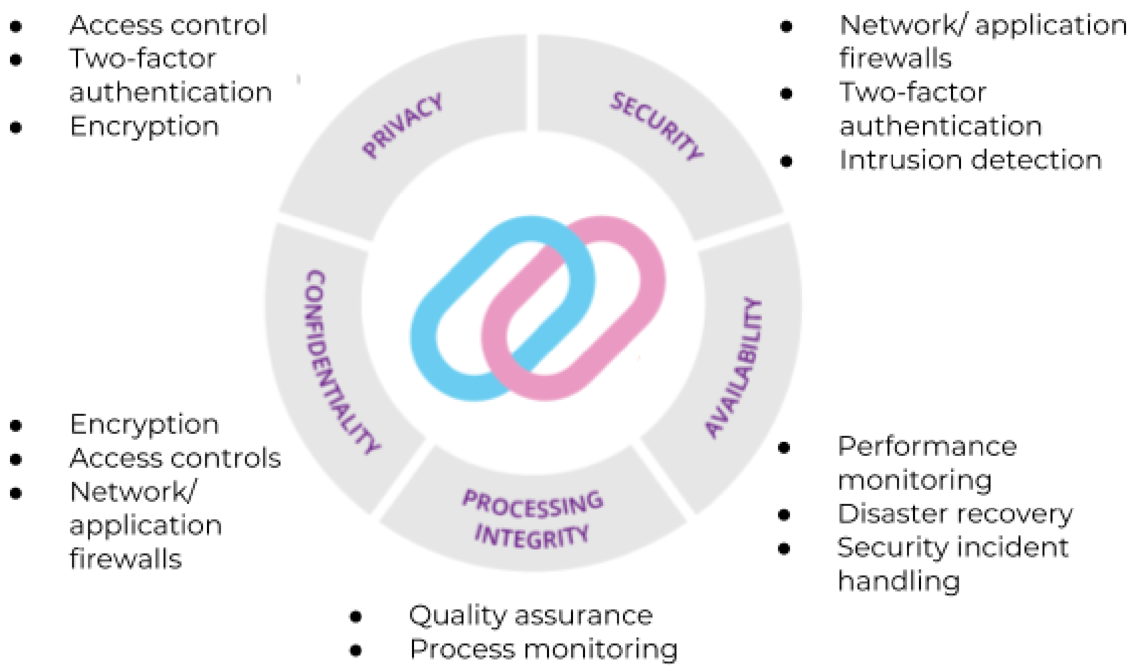

Image licensed under a Creative Commons Attribution 4.0 International Licence and adapted from Incapsula

21 CFR Part 11 for Signatures

With any eConsent solution, in addition to security and privacy, our clients are concerned about verifying that the signer is who they say they are. That's why TeloChain offers eConsent solutions that can be built in compliance with 21 CFR part 11 standards. The biggest hurdle in executing compliance with this standard is the necessity for two distinct identification components that would require collaboration of multiple people to execute fraud. We are able to customize the solution to the needs of your study to execute any number of possible patient authentications to achieve compliance. From tokenized ids, passwords, ID scans, and in person verification at a doctor or CRO office, we have a customizable solution for you, built within our secure framework of offerings.

Summary

At TeloChain everything we do is built on a foundation of security and privacy with a mentality of continuous improvement. We are passionate about helping you utilize technology securely to solve problems within the systems you already use. Want to know more? Contact us.