Trustform Digital

Security & Compliance Overview

This document details how we protect your website, your practice, and the information your patients trust you with. It covers our approach to the **HIPAA Security Rule** and the **SOC 2 Trust Service Criteria**, the specific controls we build into every project, and how we work alongside your compliance program. In short: everything we do to keep your data safe.

1. Our approach: security by design

Security isn't a feature we add at the end. It's designed into every project from the first line of code. We follow a **defense-in-depth** model: multiple layers of protection so that no single failure exposes your data. Every website and application we build starts from a secure baseline, and for projects that handle sensitive information we extend that baseline to meet the specific controls your compliance needs require.

2. Credentials & expertise

Trustform Digital is led by a certified security professional with over a decade of experience building secure, scalable applications. We hold:

- **CISSP** — Certified Information Systems Security Professional, (ISC)²
- **AWS Certified Solutions Architect – Professional**
- **Google Cloud Professional Cloud Security Engineer**
- **CompTIA Security+** and **CompTIA Cloud+**

3. HIPAA compliance

HIPAA protects patients' health information (PHI) through three rules: the **Privacy Rule** (how PHI may be used and disclosed), the **Security Rule** (safeguards for electronic PHI), and the **Breach Notification Rule**. When your project handles PHI, we implement safeguards across all three of the Security Rule's categories.

Administrative safeguards

- Risk analysis and ongoing risk management
- Access management: role-based permissions and least-privilege
- Workforce authorization, security awareness, and training
- Security incident response procedures
- Contingency planning: data backup, disaster recovery, and testing
- Business Associate Agreements (BAA) with all parties that touch PHI

Physical safeguards

- Data-center facility access controls (via SOC 2-audited hosting providers)
- Workstation and device security policies
- Secure disposal and re-use controls for media and hardware

Technical safeguards

- Access control: unique user IDs, automatic logoff, emergency access
- Encryption and decryption of ePHI at rest and in transit
- Audit controls: logging of access to and activity on systems with PHI

- Integrity controls to prevent improper alteration or destruction of data
- Person/entity authentication, including multi-factor authentication
- Transmission security (TLS) for all data moving across networks

4. SOC 2 alignment

SOC 2 is an independent audit standard from the AICPA that evaluates an organization's controls against five **Trust Service Criteria**. A **Type I** report assesses control design at a point in time; a **Type II** report assesses how effectively controls operate over a period. For projects that require it, we build on SOC 2-ready infrastructure and align our controls to each criterion:

Security (Common Criteria)

- Logical access controls, MFA, and role-based access
- Encryption, network security, and web application firewalls
- Vulnerability and patch management
- Continuous monitoring, alerting, and change management

Availability

- Uptime and performance monitoring
- Automated backups and tested disaster recovery
- Redundancy and capacity planning

Processing Integrity

- Input and output validation
- Tested, reviewed releases and deployments
- Error and job monitoring

Confidentiality

- Data classification and least-privilege access
- Encryption at rest and in transit
- Confidentiality agreements and secure disposal

Privacy

- Clear privacy notice, consent, and data minimization
- Defined retention and disposal policies
- Support for patient right-of-access and data export

5. Security controls in every build

Regardless of package, every website and application ships with a security baseline:

Encryption

- TLS/HTTPS enforced sitewide with HSTS
- Encryption of data at rest on managed infrastructure

Access & authentication

- Least-privilege access and strong authentication
- Multi-factor authentication for administrative access

- Session timeouts and automatic sign-out

Application security

- Encrypted, validated forms
- Security headers (Content Security Policy, HSTS, anti-clickjacking)
- Dependency and security patch management
- Secure secrets handling (no credentials in code)

Network, monitoring & recovery

- Firewall / WAF and DDoS protection via the hosting layer
- Audit logging, uptime and error monitoring, and alerting
- Automated daily backups with tested restores and defined retention

Data handling

- Data minimization: we collect only what is needed
- Documented retention and secure disposal
- Support for patient right-of-access and data export

6. Infrastructure options

We deploy to the **cloud** or to your own **private, on-premise infrastructure**, depending on your needs. Cloud deployments run on SOC 2-audited providers (such as AWS and Google Cloud), inheriting their physical, network, and availability controls. For heightened compliance, we build on SOC 2-ready infrastructure and implement the additional controls your program requires.

7. Secure development & operations

- Secure software development practices and code review
- Dependency scanning and a defined patching cadence
- Least-privilege operational access and secrets management
- Documented incident response and breach notification procedures
- Vendor and subprocessor management, with BAAs where PHI is involved

8. A shared responsibility

Compliance is a partnership. We design and build to the appropriate security controls and give your practice a strong technical foundation. Full HIPAA compliance and SOC 2 certification are **organizational** efforts that also depend on your internal policies, training, and administrative safeguards. We support those efforts and coordinate with your compliance or legal advisor to make sure the whole picture holds together.

Ready to talk about your compliance needs? Visit trustformdigital.com to get started.