CSNP
CYBERSECURITY NON-PROFIT

Compliance Requirements Overview

A comprehensive guide to understanding and implementing major cybersecurity and privacy frameworks for your organization

INTRODUCTION

Navigating the Compliance Landscape

The cybersecurity compliance landscape has evolved dramatically in recent years. Organizations now face a complex web of federal, state, and industry-specific regulations designed to protect sensitive data and ensure privacy.

Understanding which frameworks apply to your organization is the first step toward building a robust compliance program. This overview will help you identify relevant requirements and create an actionable compliance roadmap.

GLOBAL

GDPR: General Data Protection Regulation

Scope & Applicability

Applies to any organization processing EU residents' data, regardless of location. Covers personal data collection, storage, and processing activities.

Key Requirements

- Lawful basis for processing data
- Data subject rights (access, deletion, portability)
- Privacy by design and default
- Breach notification within 72 hours

Penalties & Enforcement

Fines up to €20 million or 4% of global annual revenue, whichever is higher. Enforcement has been aggressive with major tech companies facing significant penalties.

UNITED STATES

CCPA/CPRA: California Privacy Laws

01

Consumer Rights

Right to know what personal information is collected, sold, or shared. Right to delete personal information and opt-out of sales.

02

Business Obligations

Provide clear privacy notices, honor consumer requests within 45 days, implement reasonable security measures, and maintain records.

03

CPRA Enhancements

Creates California Privacy Protection Agency, adds right to correct inaccurate data, and introduces stricter rules for sensitive personal information.

Does CCPA Apply to You?

You're covered if you do business in California and meet any threshold: $25M+ annual revenue, 100K+ consumers/households, or 50%+ revenue from selling consumer data.

PAYMENT SECURITY

PCI DSS: Payment Card Industry Data Security Standard

12 Core Requirements

- Install and maintain firewall configuration
- Encrypt transmission of cardholder data
- Restrict access to cardholder data
- Regularly test security systems

Compliance Levels

Level 1: 6M+ transactions annually

Level 2: 1-6M transactions

Level 3: 20K-1M transactions

Level 4: Under 20K transactions

Validation Methods

Requirements vary by level: annual on-site assessments for Level 1, self-assessment questionnaires for smaller merchants, and quarterly network scans for all levels.

HEALTHCARE

HIPAA: Health Insurance Portability and Accountability Act

Privacy Rule

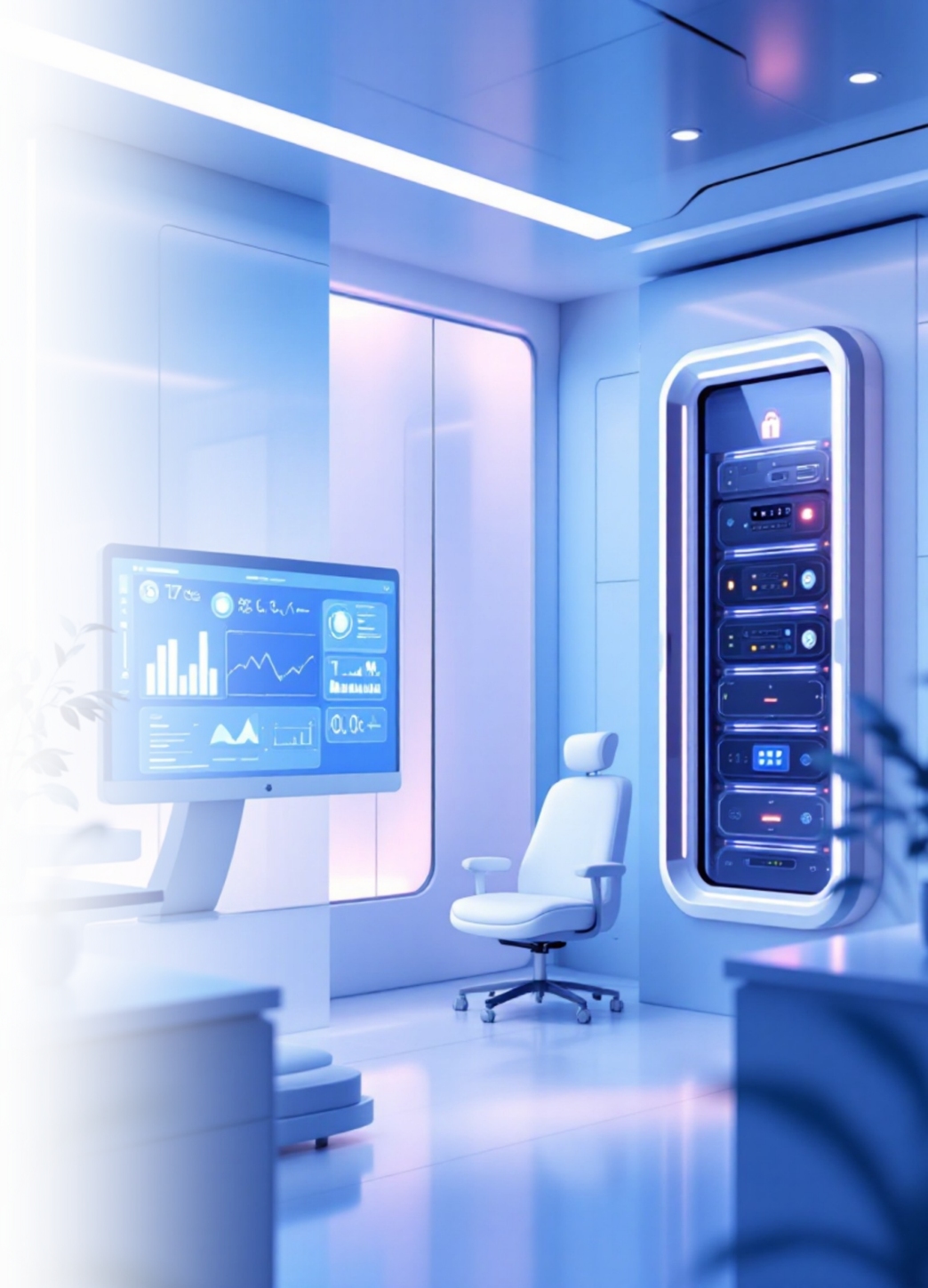
Establishes national standards for protecting medical records and personal health information. Gives patients rights over their health data.

Security Rule

Requires administrative, physical, and technical safeguards to ensure confidentiality, integrity, and availability of electronic PHI.

Breach Notification

Mandates notification to affected individuals, HHS, and potentially media when PHI breaches occur affecting 500+ individuals.



SOC 2: Service Organization Control

Trust Service Criteria

Security

Protection against unauthorized access

Availability

System accessible as agreed

Processing Integrity

Complete, valid, accurate processing

Confidentiality

Designated information protected

Privacy

Personal information collected and used properly

Type I vs Type II

Type I: Evaluates controls at a specific point in time. Faster and less expensive, suitable for early-stage companies.

Type II: Examines controls over a period (typically 6-12 months). More comprehensive and valuable to customers, demonstrates sustained compliance.

SOC 2 is especially important for SaaS providers, cloud service companies, and any organization handling customer data on behalf of others.

INDUSTRY-SPECIFIC

Specialized Compliance Requirements

Financial Services

GLBA: Gramm-Leach-Bliley Act requires financial institutions to explain information-sharing practices and safeguard sensitive data.

SEC/FINRA: Additional cybersecurity requirements for broker-dealers and investment advisors.

Education Sector

FERPA: Protects student education records and gives parents/students rights to review and correct records.

COPPA: Children's Online Privacy Protection Act for websites serving children under 13.

Government Contractors

NIST 800-171: Required for handling Controlled Unclassified Information (CUI) in federal contracts.

CMMC: Cybersecurity Maturity Model Certification for Department of Defense contractors.

State Privacy Laws: A Patchwork Landscape

Beyond California, numerous states have enacted or proposed comprehensive privacy legislation. Understanding this evolving landscape is crucial for multi-state operations.

State	Law	Effective Date	Key Feature
Virginia	VCDPA	January 2023	Consumer rights, data protection assessments
Colorado	CPA	July 2023	Universal opt-out mechanisms
Connecticut	CTDPA	July 2023	Data minimization requirements
Utah	UCPA	December 2023	Business-friendly approach
Texas	TDPSA	July 2024	Biometric data protections

Additional states including Montana, Oregon, Delaware, Iowa, Indiana, Tennessee, and Florida have enacted privacy laws with varying effective dates through 2026.

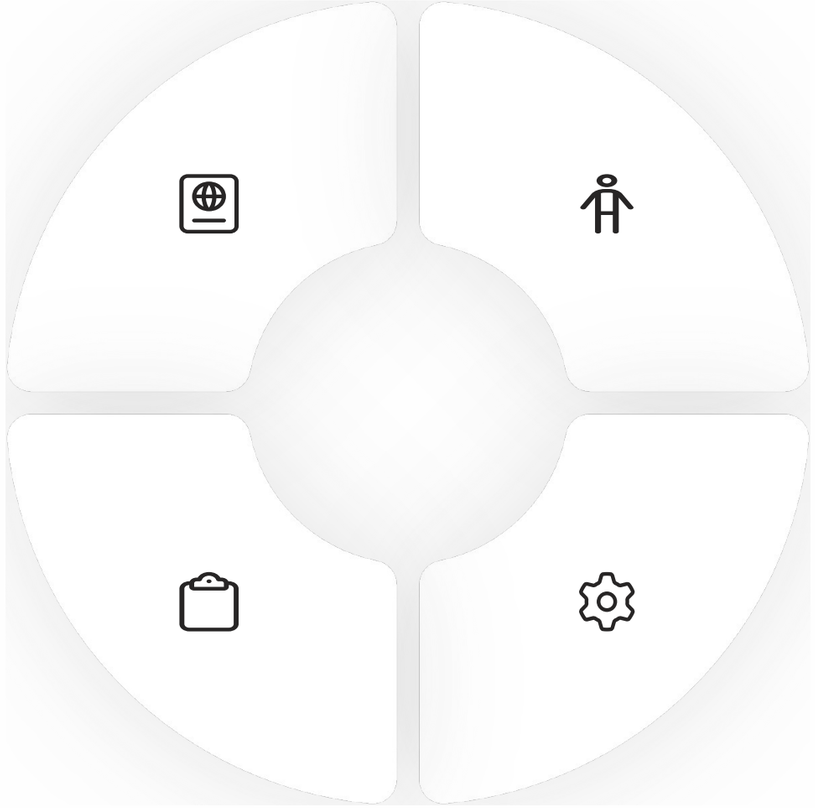
Compliance Framework Mapping

Common Controls

- Access management
- Encryption requirements
- Incident response plans
- Regular security assessments

Documentation

- Privacy policies and notices
- Data inventory and mapping
- Risk assessments
- Vendor management records



Personnel Security

- Background checks
- Security awareness training
- Clear roles and responsibilities
- Termination procedures

Technical Safeguards

- Multi-factor authentication
- Vulnerability management
- Audit logging and monitoring
- Network segmentation

DECISION GUIDE

Which Frameworks Apply to Your Organization?

1

Assess Your Data Types

Identify what data you collect: payment cards (PCI DSS), health information (HIPAA), EU resident data (GDPR), California consumer data (CCPA), or general customer data (state laws, SOC 2).

2

Determine Geographic Scope

Where are your customers located? Where do you operate? Multi-state or international operations trigger additional privacy law requirements.

3

Evaluate Industry Requirements

Check sector-specific mandates: financial services (GLBA), education (FERPA), government contracts (NIST 800-171/CMMC), healthcare (HIPAA).

4

Review Business Relationships

Do customers require SOC 2? Are you a service provider or vendor subject to contractual security requirements? B2B relationships often drive certification needs.

5

Prioritize and Plan

Start with legally required frameworks, then add voluntary certifications that provide competitive advantages. Create a phased implementation roadmap based on risk and resources.

Cybersecurity Non-Profit

> "Making cybersecurity knowledge accessible to everyone through education, community, and practical resources."

Our Programs

- Business & Non-Profit Security
- Family Cybersecurity
- Kids Safety Online
- Senior Digital Safety
- Women's Security Awareness
- Parents & Educators Resources

Everything we offer is completely free

Connect With Us

Visit our website: **csnp.org**

Access free resources: **csnp.org/resources**

CSNP is dedicated to making cybersecurity education accessible to everyone. Our comprehensive programs serve businesses, nonprofits, families, children, seniors, women, and educators with practical, actionable guidance.