## 2.2.17 Administrative Requirements for Privacy and Security Officials

**(a) Policy**

California Correctional Health Care Services (CCHCS) shall develop and maintain an entity-wide information security, privacy, and risk management strategy and program to support health information privacy and security compliance as required by federal and state privacy and security laws.

**(b) Purpose**

To define specific workforce roles related to privacy and security and outline those roles in duty statements to ensure privacy and security policies and procedures are developed, implemented, monitored, and maintained.

**(c) Responsibility**

The CCHCS Chief Privacy Officer (CPO) and Chief Information Security Officer (CISO) are responsible for the implementation, monitoring, and maintenance of this policy.

**(d) CCHCS Workforce Staffing Roles**

**(1) CCHCS Chief Privacy Officer**

(A) The CPO shall ensure compliance with CCHCS's policies and procedures relating to privacy. Responsibilities include, but are not limited to:

1. Assisting in the development and implementation of privacy policies and procedures.
2. Monitoring compliance with privacy policies and procedures pursuant to applicable federal and state privacy laws, standards, and industry best practices.
3. Performing ongoing compliance monitoring activities including initial and periodic information privacy risk assessments or analyses and implementing mitigation and remediation efforts.
4. Working with legal counsel and management to ensure forms, authorizations, and notices are current.
5. Assisting with, coordinating, and supporting departmental tracking of workforce member access to health information as needed for Privacy Office operations.
6. Developing, revising, and monitoring compliance with Privacy Awareness Training and ensuring that all users who have access to CCHCS data complete training before being provisioned and annually thereafter.
7. Monitoring patients' rights to access, amend, and restrict access to their health information.
8. Ensuring a process for addressing complaints on privacy policies and procedures, including complaints on denial of access to health information and responding to privacy questions and issues.
9. Coordinating control activities with the CISO.
10. Conducting fact-finding for reported information security incidents, making breach determinations, and issuing notifications required by the Health Insurance Portability and Accountability Act (HIPAA) and applicable state law and policy.
11. Coordinating with the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), Center for Data Insights and Innovation (CDII), state regulators, and other oversight entities in compliance reviews and investigations.
12. Coordinating with the CISO to recommend sanctions for privacy violations.
13. Coordinating with the CISO and contracting units in the development, implementation, and ongoing compliance monitoring of business associates (BA) and business associate agreements (BAA) to ensure privacy concerns, requirements, and responsibilities are addressed.
14. Identifying a point of contact by name, title, or office and telephone number in any notice describing how a patient's health information may be used and disclosed, and how the patient may access their information, including the designated contact person or office that is responsible for receiving privacy-related complaints and providing additional information about the content of the privacy notice.

**(2) CCHCS Chief Information Security Officer**

(A) The CCHCS CISO shall ensure compliance with CCHCS' policies and procedures relating to information security. Responsibilities include, but are not limited to:

1. Building a strategic and comprehensive information security program that defines, develops, maintains, and implements policies and processes that enable consistent, effective information security practices which minimize risk and ensure the integrity, confidentiality, and availability of information that is owned, controlled, or processed within the organization.
2. Ensuring information security policies, standards, and procedures are up-to-date with applicable federal and state information security laws, licensing and certification requirements and accreditation standards.

3. Initiating, facilitating, and promoting activities to foster information security awareness within the organization.
4. Creating a culture of cyber security with information technology to drive behavioral change within the organization.
5. Evaluating security trends, evolving threats, risks, and vulnerabilities and applying tools to mitigate risk as necessary.
6. Managing security incidents and events involving electronic health information.
7. Ensuring that the technology recovery, business continuity, risk management, and access control needs of the organization are addressed.
8. Ensuring the organization complies with the administrative, technical, and physical safeguards.
9. Working closely with the CPO to ensure alignment between security and privacy compliance programs, including policies, practices, and investigations, and assisting with reporting to oversight agencies.
10. Performing and analyzing initial and periodic information security risk assessments and implementing mitigation and remediation.
11. Developing and implementing information security risk management plans.
12. Ensuring the organization has audit controls to monitor activity on electronic systems that contain or use electronic protected health information.
13. Overseeing periodic monitoring and reviewing of audit records to ensure the appropriateness of system activity, including, but not limited to, logons and logoffs, file accesses, updates, edits, and printing.
14. Ensuring the organization has and maintains an appropriate system use and disclosure and confidentiality statement.
15. Overseeing, developing, and delivering initial and ongoing security training to the workforce.
16. Participating in the development, implementation, and ongoing compliance monitoring of BAs and BAAs, to ensure security concerns, requirements, and responsibilities are addressed.
17. Assisting the CPO as needed with breach determination and notification processes under HIPAA and applicable state breach rules and requirements.
18. Establishing and administering a process for investigating and acting on security incidents which may result in a privacy breach.
19. Partnering with the CPO to recommend sanctions for information security violations.
20. Cooperating with the HHS OCR, CDII, state regulators, and other legal entities, organizations, or officers in any compliance reviews or investigations.

**References**

- Code of Federal Regulations, Title 45, Subtitle A, Subchapter C, Part 164, Subpart C, Section 164.308 - Administrative Safeguards
- Code of Federal Regulations, Title 45, Subtitle A, Subchapter C, Part 164, Subpart E, Section 164.520 - Notice of Privacy Practices for Protected Health Information
- Code of Federal Regulations, Title 45, Subtitle A, Subchapter C, Part 164, Subpart E, Section 164.530 - Administrative Requirements
- State Administrative Manual 5305.3, Information Security Roles and Responsibilities
- State Administrative Manual 5305.5, Information Asset Management
- State Administrative Manual 5310, Privacy
- Statewide Health Information Policy Manual, Chapter 5.3.1, Notice of Privacy Practices
- Statewide Health Information Policy Manual, Chapter 4.1.4, Staffing: Privacy Official, Security Official

**Revision History**

Effective: 10/23/2023