CalOptima Health

2025 HIPAA Privacy and Security Program

Protection of Member Health Information

(Revised September 2024)

TABLE OF CONTENTS

I. OBJECTIVES

This program description is a general introduction for all CalOptima Health employees to the privacy and security regulations dictated by the federal Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), other federal and California privacy laws, as well as CalOptima HIPAA security and privacy policies and procedures. This program description will be updated as needed and reviewed on an annual basis.

It is expected that all CalOptima Health employees understand that it is their legal and ethical responsibility to preserve and protect the privacy, confidentiality and security of all confidential information in accordance with these laws, policies, and procedures.

All employees are expected to access, use, and disclose confidential information only in the performance of their duties or when required or permitted by law. Additionally, all employees must disclose information only to persons who have the right to receive that information.

II. HIPAA PRIVACY AND CONFIDENTIALITY OVERVIEW

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law which, in part, protects the privacy of individually identifiable member information, provides for the electronic and physical security of health and member medical information, and simplifies billing and other electronic transactions through the use of standard transactions and code sets (billing codes). HIPAA applies to all "covered entities" such as hospitals, physicians and other providers, health plans, their employees and other members of the covered entities' workforce. HIPAA privacy and security standards were updated in 2009 by the Health Information Technology for Economic and Clinical Health (HITECH) Act and in 2013 by the HIPAA Final Omnibus Rule.

Privacy and security are addressed separately in HIPAA under two distinct rules, the Privacy Rule and the Security Rule. The Privacy Rule sets the standards for how all protected health information (PHI) should be controlled. Privacy standards define what information must be protected, who is authorized to access, use or disclose information, what processes must be in place to control the access, use, and disclosure of information, and member rights.

The Security Rule defines the standards for covered entities' basic security safeguards to protect electronic protected health information (ePHI). Security is the ability to control access to electronic information, and to protect it from accidental or intentional disclosure to unauthorized persons and from alteration, destruction, or loss. The standards include administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of ePHI.

III. DEFINITION OF PROTECTED HEALTH INFORMATION (PHI)

The HIPAA privacy regulations apply to "protected health information" (PHI). This term is used throughout this HIPAA Privacy and Security Program as well as in the policies and procedures.

Protected Health Information (PHI) has the meaning in 45 Code of Federal Regulations Section 160.103, including the following: individually identifiable health information transmitted by electronic media, maintained in electronic media (ePHI), or transmitted or maintained in any other form or medium. This information identifies the individual, or there is reasonable basis to believe the information can be used to identify the individual. The information was created or received by CalOptima Health or its Business Associate(s) and relates to:

1. The past, present, or future physical or mental health or condition of a member;
2. The provision of health care to a member; or
3. Past, present, or future payment for the provision of health care to a member.

PHI excludes:

1. Education records covered by the Family Educational Rights and Privacy Act;
2. Health records held by post-secondary educational institutions; and
3. Employment records held by a covered entity in its role as employer.

Electronic Protected Health Information (EPHI) is individually identifiable health information that is transmitted by electronic media or maintained in electronic media.

What is not considered PHI?

Health information is not PHI if it is de-identified. De-identified information may be used without restriction and without member authorization. The de-identification standard provides a method for which health information can be designated as de-identified. This method requires the removal of all 18 identifying data elements listed in the regulations. To ensure that PHI is de-identified, two methods can be used to satisfy the Privacy Rule's de-identification standard as specific in 45 CFR §164.514(b)(1) Expert Determination, and 45 CFR §164.514(b)(2) Safe Harbor.

The identifiers of an individual or of relatives, employers, or household members of the individual, which must be removed, are:

1. Names;
2. Geographic subdivisions smaller than a State (addresses);
3. Elements of dates (except year) for dates directly related to an individual (birthdates);
4. Telephone numbers;
5. Fax numbers;

6. Electronic mail addresses;
7. Social security numbers;
8. Medical records numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate or license numbers;
12. Vehicle identifiers and serial numbers (license plate numbers);
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers (finger, eye, and voice prints);
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code, except as permitted by paragraph c of 45 CFR §164.514(b)(2).

What member information must we protect?

We must protect all PHI including, but not limited to medical/clinical records, prescriptions, billing records, claim data, referral authorizations, member notifications such as explanation of benefits and other member materials including marketing materials that contain PHI.

We have implemented controls, as well as policies and procedures, for protecting member information pertaining to race, ethnicity, language, gender identity[1], and sexual orientation[2].

IV. THE PRIVACY RULE AND THE SECURITY RULE

Purpose of Privacy Rule

The purpose of the Privacy Rule is to protect and enhance the rights of members by providing them access to their health information and controlling the inappropriate use of that information.

Highlights of Privacy Rule

The Privacy Rule requires that access to PHI, including ePHI, by CalOptima Health employees is based on the general principles of "need to know" and "minimum

---

[1] **Gender identity** is defined as an individual's innermost concept of self and experience of gender (how individuals perceive themselves and what they call themselves). An individual's gender identity may be the same or different from the sex assigned at birth.

[2] **Sexual orientation**, which is separate from gender identity, is defined as an inherent or immutable and enduring emotional, romantic or sexual attraction or nonattraction to individuals of the same and/or other genders.

necessary," wherein access is limited only to the member information needed to perform a job function.

The Privacy Rule also affords certain rights to members, such as the right to request copies of their health records in paper or electronic format, or to request an amendment of information in their records.

Potential Consequences of Violating the Privacy Rule

The Privacy Rule imposes penalties for non-compliance and for breaches of privacy. These penalties range from $137 per violation to $2,067,813 per violation (with an annual penalty limit of $2,067,813), in addition to costs and attorneys' fees and costs, depending on the type of violation. In addition to civil monetary penalties, other consequences may include civil lawsuits, misdemeanor and felony charges, the reporting of individual violators to licensing boards for violations, and imprisonment.

Purpose of Security Rule

The Security Rule encompasses physical, administrative, and technical security, including computer systems and transmissions of ePHI. The rule's purpose is to:

- Ensure the confidentiality, integrity, and availability of all ePHI that is created, received, maintained, or transmitted by the covered entity.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI.
- Protect against unauthorized uses or disclosures of ePHI.
- Ensure compliance of the covered entity's workforce.

Definition of Security

"**Security**" is defined as having controls, countermeasures, and procedures in place to ensure the appropriate protection of information assets, and to control access to valued resources. The purpose of security is to minimize the vulnerability of assets and resources.

Requirements and Responsibility for Security

CalOptima Health's Information Cybersecurity Department is responsible for maintaining, monitoring, storing and securing transmission of ePHI data along with oversight of all policies and procedures regarding the security of CalOptima Health information assets.

CalOptima Health employees are responsible for protecting all of CalOptima Health's electronic information resources under their control by employing appropriate and applicable security controls.

Protection of CalOptima Health electronic information resources encompasses:

- Safeguarding ePHI from accidental or intentional disclosure to unauthorized persons.
- Safeguarding ePHI from accidental or intentional alteration, destruction, or loss.
- Safeguarding systems from viruses and malware.
- Taking precautions that will minimize the potential for theft, destruction, or any type of loss.
- Protecting workstations and mobile devices from unauthorized access and theft (e.g., via encryption, password authenticated access and physical lockdown) to ensure that ePHI is accessed, used, and/or disclosed only by authorized persons.
- Protecting other electronic assets and storage media (e.g., USB thumb drives, external hard drives, CD- ROM/DVD disks, floppy disks, magnetic tapes, videotapes, SD memory cards, etc.) from unauthorized access and theft, to ensure that ePHI contained within is accessed, used, and/or disclosed only by authorized persons.

V. WRITTEN POLICIES AND PROCEDURES FOR HIPAA PRIVACY PROGRAM

CalOptima Health's policies and procedures for the HIPAA Privacy and Security Program are located on CalOptima Health's intranet, InfoNet, which is accessible to all employees. Policies and procedures are available to CalOptima providers and health networks on CalOptima Health's website.

CalOptima Health maintains the written policies and procedures and other records related to implementation for ten years from the date created or the date last in effect, whichever is later.

VI. PRIVACY OFFICER, CHIEF INFORMATION SECURITY OFFICER AND COMPLIANCE COMMITTEE

The Privacy Officer and Chief Information Security Officer (CISO) shall work with the Compliance Committee to assist in the implementation of the HIPAA Privacy and Security Program. The Compliance Committee is chaired by the Chief Compliance Officer (CCO), and the members of the Compliance Committee are comprised of key stake holders in the HIPAA Privacy and Security Program, including the Privacy Officer, the CISO, Legal Counsel, Chief Executive Officer (CEO), and Chief Operations Officer (COO). This Committee is responsible for overseeing the following activities:

- Recommending and monitoring, in conjunction with the relevant business units or departments, the development of internal systems to carry out the privacy policies and procedures as part of daily operations;
- Determining the appropriate strategy/approach to promote compliance with the Privacy Program and Security Program and detection of any potential violations, such as through hotlines and other reporting mechanisms;

- Developing a system to solicit, evaluate and respond to referrals for privacy investigations, security incidents and breaches;
- Monitoring ongoing operations for the purpose of identifying potentially deficient areas and implementing corrective and preventive action;
- Reviewing and tracking of possible confidentiality breaches that may be identified through incident reports, security incident reports, referrals for privacy investigations, etc.;
- Analyzing and data collecting of business processes, systems and relationships to understand the cause of a reportable security incident/HIPAA breach;
- Developing policies to better prevent or address reportable security incidents/HIPAA breaches; and
- Developing resolutions which stem from reportable security incidents/HIPAA breaches.

When a potential problem is identified, the Privacy Officer and the CISO may convene a designated group of individuals to serve on an ad hoc task force to provide assistance in investigating an incident, such as an unauthorized disclosure, implementing mitigation measures and/or designing protocols to prevent a recurrence in the future.

VII. GENERAL PROVISIONS ON SAFEGUARDS AND MITIGATION PROCEDURES

Security Safeguards

CalOptima Health has in place appropriate administrative, technical and physical safeguards to protect the privacy of health information in all forms including electronic and hard copy. CalOptima Health employees are trained and educated on the HIPAA Security regulations to ensure that reasonable measures are taken to safeguard PHI from any use or disclosure that would violate the HIPAA regulations or CalOptima's privacy policies. CalOptima Health employees have limited access to PHI through job-based access and password protection. CalOptima Health also has security tools in place to protect information from those who do not need to access PHI to perform their job functions. CalOptima Health's established physical safeguards include electronic building access, restricted area access, limited access to mailroom processing, clean desk policy and controlled system access to PHI for employees and contracted personnel to perform their job function.

CalOptima Health has processes to limit employee access to member PHI based on the employee's role and job description. Employees have an obligation to limit the use of PHI to the minimum necessary for their business purposes. CalOptima Health prohibits the use of employee-owned equipment within CalOptima Health's network and employees may not transfer PHI to any portable devices for storage or otherwise without the express permission of CalOptima Health's ITS Department, which if granted, will be processed in

accordance with ITS policies and procedures. CalOptima Health data including member PHI may only be used in connection with business purposes.

E-mail Safeguards

E-mail communications between CalOptima Health and an external entity via the internet shall not contain member identifiable PHI unless the e-mail has been encrypted to safeguard the contents from being read by anyone other than the intended receiver. E-mail that is sent within CalOptima Health may contain member identifiable PHI but must be limited to the minimum necessary data required to complete the message.

Mass Disclosure Safeguards

Any large mailings that include PHI must be carefully reviewed to ensure that PHI is not inadvertently revealed to an unintended recipient. For example, this might include targeted mailings to members with specific health conditions or disease states (e.g., mailings to members with HIV). Electronic and non-electronic data must be appropriately safeguarded to ensure that PHI is protected, pursuant to CalOptima Health policies and procedures.

VIII. EDUCATION AND TRAINING PROGRAMS

CalOptima Health conducts regular training sessions on the HIPAA regulations, the CalOptima Health Privacy Program, the CalOptima Health ITS Cybersecurity awareness program, and the policies and procedures. All new employees are provided with training within a reasonable period at the New Employee Orientation. All CalOptima Health employees are also required to complete an annual mandatory online Compliance training, which includes a module on HIPAA privacy and security compliance. CalOptima Health shall maintain an annual log of training completion dates and assessment scores for all employees. Focused training will be provided as needed. Failure to complete the mandatory training within the specified timeframe may lead to disciplinary action up to and including termination of the employee.

CalOptima Health will periodically update the policies and procedures to reflect changes in operations or changes to applicable statutes and regulations. CalOptima Health will distribute the updates to affected employees and will provide additional training as necessary to ensure that employees and/or contracted personnel understand the revised policies and procedures.

IX. EFFECTIVE LINES OF COMMUNICATION

Member Complaint Procedure

CalOptima Health has procedures in place for handling complaints from its members regarding implementation of and compliance with the HIPAA privacy regulations as well as State and Federal privacy laws. CalOptima Health's Notice of Privacy Practices directs members with complaints to contact CalOptima Health, the DHCS Privacy Officer, the Secretary of the Health and Human Services or the Office for Civil Rights. Upon receipt of a complaint, the Customer Service Department will provide a copy of each complaint to CalOptima Health's Privacy Officer and forward the complaint to the Grievance and Appeals Resolution Services Department (GARS). GARS will follow the same procedure as when handling other complaints submitted by CalOptima Health members. All responses and other documentation relating to a privacy complaint are maintained in the member's file and by the Privacy Officer for ten years from the date of the last communication on the complaint.

Access to Privacy Officer

The Privacy Officer maintains an open door policy for all employees and accepts e-mails, telephone messages or written memoranda regarding any privacy matter. Any individual who has a question or wants to report a potential privacy incident may bring such issues directly to the Privacy Officer, CCO, or CISO. Reports of potential privacy incidents may be made on an anonymous or identifiable basis directly to the Privacy Officer or through the Compliance Hotline at 1-855-507-1805.

Responsibility to Report

CalOptima Health is committed to compliance with the HIPAA and state privacy laws and to correcting violations wherever they may occur in the organization. Every employee is responsible for reporting any activity they suspect violates applicable privacy and security laws, rules, regulations or the HIPAA Privacy and Security Program. CalOptima Health must notify the Department of Health Care Services (DHCS) of any suspected or actual security incident and breaches of unsecure (unencrypted) protected information or other unauthorized use or disclosure of our members' PHI and provide a written report of the investigation. On an as needed basis, CalOptima Health shall notify the Centers for Medicare & Medicaid Services (CMS), and/or the Department of Health and Human Services, Office of Civil Rights (OCR), and/or the California Attorney General of actual privacy and security breaches. The Office of Compliance will maintain documentation of incidents, including the nature of any investigation, mitigation and corrective action. In addition, employees and members have the right to report violations to the California DHCS Privacy Officer or the Secretary of the Department of Health and Human Services (DHHS). Contact information is below:

C/O: Office of HIPAA Compliance
Department of Health Care Services
P.O. Box 997413, MS 4722
Sacramento, CA 95899-7413
Email: privacyofficer@dhcs.ca.gov
Phone: 1-916-445-4646

Fax: 1-916-440-7680

OR

U.S. Department of Health and Human Services
Office for Civil Rights
Attention: Regional Manager
90 7th Street, Suite 4-100
San Francisco, CA 94103
(800) 368-1019 or FAX (415) 437-8329 or (800) 537-7697 TDD
Email: OCRComplaint@hhs.gov

In addition, employees who have observed a security incident or HIPAA breach (e.g., unsecured transmission of PHI, etc.) may contact the Compliance Hotline anonymously at: 1-855-507-1805, CalOptima Health's Privacy Officer at Privacy@caloptima.org, or CISO.

Confidentiality and No Retaliation

CalOptima Health will not threaten, intimidate, discriminate, or take other retaliatory action against any individual for filing HIPAA complaints, assisting in HIPAA investigations or compliance reviews, or raising concerns with any act or practice that they suspect is in violation of HIPAA and/or state privacy laws when the individual has a good faith belief that the act may be unlawful.

X. ENFORCING STANDARDS THROUGH DISCIPLINARY GUIDELINES

All violators of the HIPAA Privacy and Security Program or of the policies and procedures will be subject to disciplinary action. The precise discipline will depend on the nature and severity of the violation.

Disciplinary Guidelines

Any employee who fails to comply with CalOptima Health's HIPAA Privacy and Security Program or its policies and procedures is subject to focused and/or additional training or discipline. In coordination with Human Resource policy GA.8022 Progressive Discipline, such discipline may include: 1) a verbal warning; 2) written warning; 3) suspension; or 4) termination. The type of discipline rendered will depend on the degree of wrongdoing, whether there have been past violations and the individual's cooperation in promptly reporting the incident to the appropriate manager or to the Privacy Officer. Intentional or reckless non-compliance will not be tolerated and will subject the employee to discipline up to and including termination of employment.

CalOptima Health's Office of Compliance may require that an internal department or FDR develop a Corrective Action Plan based on the identified area(s) of non-compliance identified from the HIPAA and/or state privacy laws violation.

Consistent Enforcement of Policies

The range of disciplinary standards for improper conduct will be consistently applied and enforced. All personnel will be treated equally, and disciplinary action will be taken on a fair and equitable basis. CalOptima Health management must comply with and take action to ensure that their direct reports comply with the applicable policies and procedures.

Education on Disciplinary Guidelines

In the training sessions, all employees will be advised of the policy regarding disciplinary actions for non-compliance.

XI. RESPONSE TO DETECTED OFFENSES AND CORRECTIVE ACTION PLANS

Investigation and Corrective Action

If there is a report of non-compliance, or if the Privacy Officer, CISO, a member of the Compliance Committee, or a manager discovers credible evidence of a violation, an investigation will immediately ensue. When CalOptima Health substantiates a reported violation, it is the policy to institute corrective action.

Initiating Systemic Changes to Correct Problems

After a problem has been identified and corrected, the Privacy Officer, CISO, and the Compliance Committee will review the circumstances to determine: 1) whether similar problems have been uncovered elsewhere, and 2) whether modifications of the privacy policies and procedures are necessary to prevent and detect other inappropriate conduct or violations. The Privacy Officer and CISO will work with the Compliance Committee to initiate systemic changes throughout the company to avoid future problems of a similar nature.

Mitigation

If a suspected or actual use or disclosure occurs by CalOptima Health or a business associate that violates the HIPAA regulations and/or state privacy laws, CalOptima Health will take prompt corrective action to mitigate any damaging effects that the potential disclosure could have on the affected members as well as cure any system deficiencies to prevent future unauthorized uses or disclosures. CalOptima Health employees and FDRs are required to report any suspected or actual violation that they observe or learn about to his/her supervisor, or the Privacy Officer, CCO, or CISO immediately so that action to mitigate the damage can commence promptly.