CUSTOMER NAME | Main office ADDRESS | CITY, STATE AND ZIP CODE

HIPAA Policies and Procedures Manual

Telehealth | Telemedicine Edition 2021

Customer Template

**A Covered entity**

Table of Contents

[Policy and Procedure Approval Log 5](#_Toc74010016)

[IN-100 HIPAA and Telehealth Policies and Procedure Approval Log 5](#_Toc74010017)

[IN-101 Introduction 7](#_Toc74010018)

[Section I - General Guidelines 3](#_Toc74010019)

[G-100 Overview of Federal HIPAA Regulations 3](#_Toc74010020)

[G-101 Disclosure of Substance Abuse Disorder 7](#_Toc74010021)

[G-102 Telehealth 11](#_Toc74010022)

[G-103 California Medical and Privacy Laws 15](#_Toc74010023)

[G-104 Florida Information Protection Act of 2014 (FIPA) 18](#_Toc74010024)

[G-105 Texas HB 300 23](#_Toc74010025)

[G-106 Workforce Members 25](#_Toc74010026)

[G-107 Emergency Contact Information 27](#_Toc74010027)

[G-108 Roles and Responsibilities 30](#_Toc74010028)

[G-109 Breach and Notification Guidelines 33](#_Toc74010029)

[G-110 Minimum Necessary Access 41](#_Toc74010030)

[G-111 Training Requirements 43](#_Toc74010031)

[Section II – Privacy and Disclosure Rights 44](#_Toc74010032)

[P-100 Privacy and Notification Rule 44](#_Toc74010033)

[P-101 Permitted Disclosures 48](#_Toc74010034)

[P-102 Mandatory Disclosures 50](#_Toc74010035)

[P-103 Disclosure to Personal Representative 54](#_Toc74010036)

[Section III – Business Associates 57](#_Toc74010037)

[B-100 Business Associates Overview 57](#_Toc74010038)

[Section IV – Security Rule 60](#_Toc74010039)

[S-100 HIPAA Security Rule Basics 60](#_Toc74010040)

[S-101 Administrative Safeguards 65](#_Toc74010041)

[S-102 Physical Safeguards 67](#_Toc74010042)

[S-103 Technical Safeguards 71](#_Toc74010043)

[S-104 Storage, Transportation, Transfer, and Transmission of PHI 75](#_Toc74010044)

[Section V – Disposal and Destruction of PHI 76](#_Toc74010045)

[D-100 Disposal of Printed PHI 76](#_Toc74010046)

[D-101 Disposal of Electronic PHI 80](#_Toc74010047)

[D-102 Disposal of Electronic Devices and Media 84](#_Toc74010048)

[Section VI – Disaster Preparedness and Response 88](#_Toc74010049)

[DI-100 Disaster Preparedness and the Community 88](#_Toc74010050)

[Quick Information Guide 1.0: Civil and Criminal Penalties 91](#_Toc74010051)

[Quick Information Guide 2.0: HIPAA State Security Laws 93](#_Toc74010052)

[Quick Information Guide 3.0: HIPAA Definitions 98](#_Toc74010053)

[Quick Information Guide 4.0: Privacy Disclosure Guideline Examples 103](#_Toc74010054)

[HIPAA Forms (Fillable PDFs) 106](#_Toc74010055)

# Policy and Procedure Approval Log

## IN-100 HIPAA and Telehealth Policies and Procedure Approval Log

THE BOARD OF DIRECTORS has met and has agreed to assume full responsibility for the implementation and ongoing oversight of the approved policies and procedures contained herein. This page will serve as the acknowledgement that the policies and procedure have been reviewed and approved as noted.

|  |  |  |
| --- | --- | --- |
| **Action** | **Approval** | **Date** |
| Policy and Procedures Approval |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Add additional pages as needed.

## IN-101 Introduction

### Mission

### Values

### Locations

# Section I - General Guidelines

## G-100 Overview of Federal HIPAA Regulations

### Introduction

The Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) covers both individuals and organizations. Those who must comply with HIPAA are called “***covered entities***” or “***business associates.***” is a covered entity, which is involved in transactions that involve receiving, storing, and transmitting Protected Health Information (PHI)? Employees and contracted providers have a duty to protect PHI in all forms, including instances when verbal PHI is being used or overheard in the workplace.

### Scope

CSM Team considers patient privacy and the security of Protected Health Information (PHI) a fundamental responsibility of its operations and the practices of its providers and employees. The term “Patient and CSM Team for the purpose of this policy is the “individual” for which the HIPAA and PHI rules apply. The CSM Team leadership, and workforce members must be committed to respecting patients’ privacy and safeguarding their individually identifiable health information (also known as “protected health information” or “**PHI**”). This includes, but is not limited to:

1. Responding to patients’ requests for access to, or amendment of, their PHI, restrictions on its disclosure, or an accounting of disclosures.

1. Ensuring the confidentiality, integrity, security, and availability of all PHI created, received, maintained, or transmitted by or on behalf of the Medical Office.

### Policy Framework

**The United States Department of Health and Human Services (HHS)** has established regulatory requirements for the protection of PHI through the following rules:

***The Privacy Rule***, which sets national standards for when protected health information (PHI) may be used and disclosed.

***The Security Rule***, which specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of electronically protected health information.

***The Breach Notification Rule***, which requires covered entities to notify affected individuals, U.S. Department of Health & Human Services (HHS), and in some cases, notification of the media of a breach of unsecured PHI, which also requires notifications to affected individuals and the Secretary of the Department of Health and Human Services.

### Policy Statement

In furtherance of its commitment, CSM Team has adopted the following Policies and Procedures (collectively, this “**Policy**”) as an integral part of its operations and requires all employees, volunteers, trainees, and agents under CSM Team, control to comply with this Policy, as well as any owner or director who administers or delivers CSM Team services (collectively, “**Workforce Members**”).

This Policy is intended to comply with the standards, requirements, and implementation specifications of the Health Insurance CSM Team Portability and Accountability Act of 1996, and the regulations set forth at 45 CFR Part 160 and Part 164, as amended by the Health Information Technology for Economic and Clinical Health Act (collectively, “**HIPAA**”). HIPAA preempts contrary provisions of State law unless such provisions are more stringent than the HIPAA privacy standard.

The CSM Team leadership, workforce members, and business associates (as defined by HIPAA) have an individual and collective responsibility to protect patients’ Protected Health Information (PHI) as a “covered entity” defined by the U.S. Department of Health and Human Services (HHS). PHI includes recognizable patient information in printed, electronic, and spoken formats, photos, and any combination of PHI, which can be used to identify a person or entity that is protected by HIPAA rules. The policies contained within this manual are subject to change and are not intended to be all-inclusive of the HIPAA laws and possible interpretations. Contact the Compliance Officer or designee at any time there is a question regarding a policy or HIPAA incident that may need further clarification.

### Compliance Officer

The Compliance Officer shall have responsibility for all privacy and security matters and for monitoring compliance with this Policy. In addition, the Compliance Officer shall be responsible for modifying existing or developing and implementing new procedures to ensure CSM Team ongoing compliance with HIPAA and ensuring that all Workforce Members are trained in accordance with this Policy and certifications of such training and attendance are kept by CSM Team human resources department. All questions, complaints, or reports of violations or other matters are to be directed to the Compliance Officer. The Compliance Officer and the role is further described in Policy G-102 “Roles and Responsibilities.”

### Other Protected Patient and Patient Information

### It is important to understand that sensitive personal, financial, and other data that is used or could be used to identify a person or entity may also be protected by other U.S. regulatory agencies. Therefore, it is vitally important that all Workforce Members and business associates treat all patient and patient information and data as private and take the necessary steps to maintain appropriate levels of security in accordance with the law.

* 1. The ***Genetic Information Discrimination Act of 2008 (GINA)*** prohibits genetic information discrimination in employment. Under Title II of GINA, it is illegal to discriminate against employees or applicants because of genetic information.
  2. The ***Gramm-Leach-Bliley (GLB) Act requires financial institutions to send consumer’s annual privacy notices and allow them to opt-out of sharing their information with unaffiliated third parties***. It requires financial institutions to implement reasonable security policies and procedures.
  3. The ***COPPA Rule requires websites and apps to get parental consent before collecting personal information from kids under 13.*** The Rule was revised in 2013 to strengthen kids’ privacy protections and gives parents greater control over the personal information that websites and online services may collect from children under the age of thirteen.
  4. The ***Disposal Rule under the Fair and Accurate Credit Transactions Act of 2003 (“FACTA”***), which amended the FCRA, requires that companies dispose of credit reports and information derived from them in a safe and secure manner.
  5. The ***Red Flags Rule*** requires financial institutions and certain creditors to have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.
  6. The ***Telemarking Sales Rule*** requires telemarketers to make specific disclosures of material information; prohibits misrepresentations; limits the hours that telemarketers may call consumers; and sets payment restrictions for the sale of certain goods and services.

### References

The ***Health Insurance Portability and Accountability Act of 1996 (HIPAA)*,** Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy, and security of health information. Collectively these are known as the *Administrative Simplification* provisions.

The ***Standards for Privacy of Individually Identifiable Health Information*** (“Privacy Rule”) establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services (“HHS”) issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). The Privacy Rule standards address the use and disclosure of individuals’ health information—called “protected health information” by organizations subject to the Privacy Rule — called “covered entities,” as well as standards for individuals' privacy rights to understand and control how their health information is used. Within HHS, the Office for Civil Rights (“OCR”) has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

The ***Security Rule***, like all of the Administrative Simplification rules, applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA (the “covered entities”).

The ***Genetic Information Nondiscrimination Act (GINA)*** was signed into law on May 21, 2008. GINA protects individuals against discrimination based on their genetic information in health coverage and employment. GINA is divided into two sections or Titles. Title I of GINA prohibits discrimination based on genetic information in health coverage. Title II of GINA prohibits discrimination based on genetic information in employment.

The ***Health Information Technology for Economic and Clinical Health (HITECH) Act*** through notice and comment rulemaking, as required by the Administrative Procedure Act. These provisions include business associate liability; new limitations on the sale of protected health information, marketing, and fundraising communications; and stronger individual rights to access electronic medical records and restrict the disclosure of certain information. OCR has issued a Notice of Proposed Rulemaking (NPRM) regarding these provisions. Although the effective date (February 17, 2010) for many of these HITECH Act provisions have passed, the NPRM and the final rule that will follow, provide specific information regarding the expected date of compliance and enforcement of these new requirements.

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights issued a final rule that implemented a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, also known as ***the Final Omnibus Rule***, to strengthen the privacy and security protections for health information established under the ***Health Insurance Portability and Accountability Act of 1996 (HIPAA)***.

## G-101 Disclosure of Substance Abuse Disorder

### The Substance Abuse and Mental Health Services Administration (SAMHSA) July 2020 Update

The Substance Abuse and Mental Health Services Administration (SAMHSA), part of the U.S. Department of Health and Human Services (HHS or Department), announces the adoption of the revised Confidentiality of Substance Use Disorder Patient Records regulation, 42 CFR Part 2. The adoption of this revised rule represents a historic step in expanding care coordination and quality through the Deputy Secretary’s Regulatory Sprint to Coordinated Care.

In general, Part 2 Programs are prohibited from disclosing any information that would identify a person as having or having had a Substance Abuse Disorder (SUD) unless that person provides written consent. Part 2 specifies a set of requirements for consent forms, including but not limited to the name of the patient, the names of individuals/entities that are permitted to disclose or receive patient identifying information, the amount and kind of the information being disclosed, and the purpose of the disclosure (see §2.31).

In addition to Part 2, other privacy laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) have been enacted. HIPAA generally permits the disclosure of protected health information for certain purposes without patient authorization, including treatment, payment, or health care operations.

### The Department of Health and Human Services Response to SAMHSA Substance Abuse Disorder privacy requirements under HIPAA Laws

A health provider that provides treatment for substance use disorders, including opioid abuse, needs to determine whether it is subject to 42 CFR Part 2 (i.e., a “Part 2 program”) and whether it is a covered entity under HIPAA. Generally, the Part 2 rules provide more stringent privacy protections than HIPAA, including in emergency situations. If an entity is subject to both Part 2 and HIPAA, it is responsible for complying with the more protective Part 2 rules, as well as with HIPAA. HIPAA is intended to be a set of minimum federal privacy standards, so it generally is possible to comply with HIPAA and other laws, such as 42 CFR Part 2, that are more protective of individuals’ privacy.

For example, HIPAA permits disclosure of protected health information (PHI) for treatment purposes (including in emergencies) without patient authorization and allows PHI to be used or disclosed to lessen a threat of serious and imminent harm to the health or safety of the patient or others (which may occur as part of a health emergency) without patient authorization or permission. Because HIPAA permits, but does not require, disclosures for treatment or to prevent harm, if Part 2 restricts certain disclosures during an emergency, an entity subject to both sets of requirements could comply with Part 2’s restrictions without violating HIPAA.

### Fact Sheet: SAMHSA 42 CFR Part 2 Revised Rule

The 42 CFR Part 2 regulations (Part 2) serve to protect patient records created by federally assisted programs for the treatment of substance use disorders (SUD). Part 2 has been revised to further facilitate better coordination of care in response to the opioid epidemic while maintaining its confidentiality protections against unauthorized disclosure and use.

What Has Not Changed Under the New Part 2 Rule: The revised rule does not alter the basic framework for confidentiality protection of substance use disorder (SUD) patient records created by federally assisted SUD treatment programs. Part 2 continues to prohibit law enforcement’s use of SUD patient records in criminal prosecutions against patients, absent a court order.

Part 2 also continues to restrict the disclosure of SUD treatment records without patient consent, other than as statutorily authorized in the context of a bona fide medical emergency; or for the purpose of scientific research, audit, or program evaluation; or based on an appropriate court order.

### **What Has Changed Under the New Part 2 Rule?**

The revised rule modifies several major sections of Part 2, as follows:

|  |  |  |
| --- | --- | --- |
| **Provision** | **What Changed?** | **Why Was This Changed?** |
| **Applicability and Re-Disclosure** | Treatment records created by non-Part 2 providers based on their own patient encounter(s) are explicitly not covered by Part 2, unless any SUD records previously received from a Part 2 program are incorporated into such records. Segmentation or holding a part of any Part 2 patient record previously received can be used to ensure that new records created by non-Part 2 providers will not become subject to Part 2. | To facilitate coordination of care activities by non-part-2 providers. |
| **Disposition of Records** | When an SUD patient sends an incidental message to the personal device of an employee of a Part 2 program, the employee will be able to fulfill the Part 2 requirement for “sanitizing” the device by deleting that message. | To ensure that the personal devices of employees will not need to be confiscated or destroyed, in order to sanitize in compliance with Part 2. |
| **Consent Requirements** | An SUD patient may consent to disclosure of the patient’s Part 2 treatment records to an entity (e.g., the Social Security Administration), without naming a specific person as the recipient for the disclosure. | To allow patients to apply for benefits and resources more easily, for example, when using online applications that do not identify a specific person as the recipient for a disclosure of Part 2 records. |
| **Disclosures Permitted w/ Written Consent** | Disclosures for the purpose of “payment and health care operations” are permitted with written consent, in connection with an illustrative list of 18 activities that constitute payment and health care operations now specified under the regulatory provision. | In order to resolve lingering confusion under Part 2 about what activities count as “payment and health care operations,” the list of examples has been moved into the regulation text from the preamble and expanded to include care coordination and case management activities. |

|  |  |  |
| --- | --- | --- |
| **Provision** | **What Changed?** | **Why Was This Changed?** |
| **Medical Emergencies** | Declared emergencies resulting from natural disasters (e.g., hurricanes) that disrupt treatment facilities and services are considered a “bona fide medical emergency,” for the purpose of disclosing SUD records without patient consent under Part 2. | To ensure clinically appropriate communications and access to SUD care, in the context of declared emergencies resulting from natural disasters. |
| **Research** | Disclosures for research under Part 2 are permitted by a HIPAA-covered entity or business associate to individuals and organizations who are neither HIPAA covered entities, nor subject to the Common Rule (re: Research on Human Subjects). | To facilitate appropriate disclosures for research, by streamlining overlapping requirements under Part 2, the HIPAA Privacy Rule and the Common Rule. |
| **Audit and Evaluation** | Clarifies specific situations that fall within the scope of permissible disclosures for audits and/or program evaluation purposes. | To resolve current ambiguity under Part 2 about what activities are covered by the audit and evaluation provision. |
| **Undercover Agents and Informants** | Court-ordered placement of an undercover agent or informant within a Part 2 program is extended to a period of 12 months, and courts are authorized to further extend the period of placement through a new court order. | To address law enforcement concerns that the current policy is overly restrictive to some ongoing investigations of Part 2 programs. |
| **Updated July 13, 2020** | | |

### References and Examples

Healthcare Information Exchange: <https://www.samhsa.gov/sites/default/files/how-do-i-exchange-part2.pdf>

Disclosure of Patient Records: <https://www.samhsa.gov/sites/default/files/does-part2-apply.pdf>

Federal Register: <https://www.govinfo.gov/content/pkg/FR-2017-01-18/pdf/2017-00719.pdf>

### Policy Statement

CSM Team shall inform the compliance officer whenever there is a request for patient records that includes information regarding the patient’s substance abuse disorder. All requests for medical records that contain SUD related information that is attributable to a patient, must be requested in writing and must be approved by the Compliance Officer and Medical Director.

### Procedures

1. All Workforce Members will follow appropriate policies and procedures for verifying the identity and authority of Individuals requesting PHI.
2. The policies for permitted and mandatory disclosures shall be followed in accordance with this policy to ensure that disclosures are appropriate and follow all of the pertinent rules and regulations.
3. The Compliance Officer will document the request and delivery of the PHI and assure that the proper chain of custody is followed.
4. In the event that the identity and legal authority of an Individual or entity requesting PHI cannot be verified, the PHI will not be released until such verification can be made.
5. Once it is determined that a Use or Disclosure is appropriate, the Compliance Officer and Medical Director shall jointly approve the request.
6. The designated staff with appropriate authorization to the EHR will access the Individual's PHI using proper access and authorization procedures.
7. The requested PHI will be delivered in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
8. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

Please refer to the appropriate policies and procedures that correspond with the request for Substance Abuse Disorder patient records:

P-100 Privacy and Notification Rule

P-101 Permitted Disclosures

P-102 Mandatory Disclosures

P-103 Disclosures to Personal Representatives

## G-102 Telehealth

### Overview

The purpose of this policy is to provide information regarding the Centers for Medicare and Medicaid expansion of telehealth services and related HIPAA interim guidelines. This policy is to be used as reference only and if telehealth services are offered, additional policies and procedures must be added to provide clear instructions to avoid federal and state violations regarding Protected Health Information (PHI) and telehealth services.

### Centers for Medicare and Medicaid Services Expansion of Telehealth

Telehealth, telemedicine, and related terms generally refer to the exchange of medical information from one site to another through electronic communication to improve a patient’s health. Innovative uses of this kind of technology in the provision of healthcare is increasing. And with the emergence of the virus causing the disease COVID-19, there is an urgency to expand the use of technology to help people who need routine care and keep vulnerable beneficiaries and beneficiaries with mild symptoms in their homes while maintaining access to the care they need. Limiting community spread of the virus, as well as limiting the exposure to other patients and staff members will slow viral spread.

### Expansion of Telehealth with 1135 Waiver

Under this new waiver, Medicare can pay for office, hospital, and other visits furnished via telehealth across the country and including in patient’s places of residence starting March 6, 2020. A range of providers, such as doctors, nurse practitioners, clinical psychologists, and licensed clinical social workers, will be able to offer telehealth to their patients. Additionally, the HHS Office of Inspector General (OIG) is providing flexibility for healthcare providers to reduce or waive cost-sharing for telehealth visits paid by federal healthcare programs.

Prior to this waiver, Medicare could only pay for telehealth on a limited basis: when the person receiving the service is in a designated rural area and when they leave their home and go to a clinic, hospital, or certain other types of medical facilities for the service. Even before the availability of this waiver authority, CMS made several related changes to improve access to virtual care. In 2019, Medicare started making payment for brief communications or Virtual Check-Ins, which are short patient-initiated communications with a healthcare practitioner.

Medicare Part B separately pays clinicians for E-visits, which are nonface-to-face patient-initiated communications through an online patient portal. Medicare beneficiaries will be able to receive a specific set of services through telehealth including evaluation and management visits (common office visits), mental health counseling and preventive health screenings. This will help ensure Medicare beneficiaries, who are at a higher risk for COVID-19, are able to visit with their doctor from their home, without having to go to a doctor’s office or hospital, which puts themselves and others at risk. There are three main types of virtual services physicians and other professionals can provide to Medicare beneficiaries summarized in this fact sheet: Medicare telehealth visits, virtual check-ins, and e-visits.

### Medicare Telehealth Visits

Currently, Medicare patients may use telecommunication technology for office, hospital visits and other services that generally occur in-person. The provider must use interactive audio and video telecommunications system that permits real-time communication between the distant site and the patient at home. Distant site practitioners who can furnish and get payment for covered telehealth services (subject to state law) can include physicians, nurse practitioners, physician assistants, nurse midwives, certified nurse anesthetists, clinical psychologists, clinical social workers, registered dietitians, and nutrition professionals.

It is imperative during this public health emergency that patients avoid travel, when possible, to physicians’ offices, clinics, hospitals, or other health care facilities where they could risk their own or others’ exposure to further illness. Accordingly, the Department of Health and Human Services (HHS) is announcing a policy of enforcement discretion for Medicare telehealth services furnished pursuant to the waiver under section 1135(b)(8) of the Act. To the extent the waiver (section 1135(g)(3)) requires that the patient have a prior established relationship with a particular practitioner, HHS will not conduct audits to ensure that such a prior relationship existed for claims submitted during this public health emergency.

### Virtual Check-In’s

In all areas (not just rural), established Medicare patients in their home may have a brief communication service with practitioners via a number of communication technology modalities including synchronous discussion over a telephone or exchange of information through video or image. We expect that these virtual services will be initiated by the patient; however, practitioners may need to educate beneficiaries on the availability of the service prior to patient initiation. Medicare pays for these “virtual check-ins” (or Brief communication technology-based service) for patients to communicate with their doctors and avoid unnecessary trips to the doctor’s office. These virtual check-ins are for patients with an established (or existing) relationship with a physician or certain practitioners where the communication is not related to a medical visit within the previous 7 days and does not lead to a medical visit within the next 24 hours (or soonest appointment available).

The patient must verbally consent to receive virtual check-in services. The Medicare coinsurance and deductible would generally apply to these services. Doctors and certain practitioners may bill for these virtual check-in services furnished through several communication technology modalities, such as telephone (HCPCS code G2012). The practitioner may respond to the patient’s concern by telephone, audio/video, secure text messaging, email, or use of a patient portal. Standard Part B cost-sharing applies to both.

### E-Visits

In all types of locations including the patient’s home and, in all areas, (not just rural), established Medicare patients may have non-face-to-face patient-initiated communications with their doctors without going to the doctor’s office by using online patient portals. These services can only be reported when the billing practice has an established relationship with the patient. For these E-Visits, the patient must generate the initial inquiry and communications can occur over a 7-day period.

The patient must verbally consent to receive virtual check-in services. The Medicare coinsurance and deductible would apply to these services. Medicare Part B also pays for E-visits or patient-initiated online evaluation and management conducted via a patient portal.

### State Regulations

Telehealth policy changes occurring within the COVID-19 environment have been rapidly developing on almost a daily basis. The Center for Connected Health Policy (CCHP) is committed to providing updates regarding federal and state regulations. There are no two states that have identical telehealth regulations, so it is imperative to understand federal and state regulations, as well as the policies of the insurance payors.

For more information go to: <https://www.cchpca.org/telehealth-policy/current-state-laws-and-reimbursement-policies>

### Health Insurance Portability and Accountability Act (HIPAA)

Effective immediately, the HHS Office for Civil Rights (OCR) will exercise enforcement discretion and waive penalties for HIPAA violations against health care providers that serve patients in good faith through everyday communications technologies, such as FaceTime or Skype, during the COVID-19 nationwide public health emergency. The following are topics and resources provided by the Department of Health and Human Services (HHS).

Source : <https://telehealth.hhs.gov/providers/legal-considerations>

### Cybersecurity

Electronic health records are often targeted by malware and hackers. These resources can help you ensure that you are taking the necessary steps to protect patients’ health information:

[Cybersecurity 101: What You Need to Know](https://www.ama-assn.org/system/files/2020-06/ama-telehealth-quick-guide-appendix-d3-cybersecurity-101.pdf)[[exit disclaimer icon](https://www.hhs.gov/disclaimer.html)](https://www.hhs.gov/disclaimer.html)(PDF) — from the American Medical Association

[Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients](https://healthsectorcouncil.org/wp-content/uploads/2018/12/HICP-Main-508.pdf)[[exit disclaimer icon](https://www.hhs.gov/disclaimer.html)](https://www.hhs.gov/disclaimer.html)(PDF) — from the Health Sector Coordinating Council

[Cyber Security Guidance Material](https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html) — from the U.S. Department of Health and Human Services HIPAA compliance

The [Health Insurance Portability and Accountability Act of 1996](https://www.hhs.gov/hipaa/for-professionals/index.html) (HIPAA) ensures that health care providers protect patients’ personal health information. When we are not in the COVID-19 Public Health Emergency, all of the telehealth services you provide need to follow HIPAA rules.

### HIPAA flexibility during the COVID-19 Public Health Emergency

The U.S. Department of Health and Human Services Office for Civil Rights issued a [Notification of Enforcement Discretion](https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html) to empower covered health care providers to use widely available communications applications without the risk of penalties imposed by the U.S. Department of Health and Human Services Office for Civil Rights for violations of HIPAA rules for the good faith provision of telehealth services. For more information, read [FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency](https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf) (PDF) or visit [HIPAA and COVID-19](https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html).

While the U.S. Department of Health and Human Services Office for Civil Rights has issued a notice of enforcement discretion to waive HIPAA penalties, the State Attorney Generals have not issued the same notices. Under Sec. 13410(e) of the HITECH Act, State Attorney Generals are permitted to obtain civil money penalties on behalf of state residents for HIPAA violations. You should check with any applicable states to see if they have also waived these penalties.

### Obtaining Informed Consent

While specific, informed consent laws vary by state, these commonsense actions are always a good idea:

1. When you meet with a patient, explain what they can expect from the telehealth visit and what their rights are.
2. Check-in with the patient about their responsibilities during a telehealth visit — for example, they need to be aware of privacy on their end.
3. If there is anyone observing the visit, tell the patient, and get their consent at the start.

### Resources for Telemedicine and Informed Consent

1. Agency for Healthcare Research and Quality: [Easy-to-Understand Telehealth Consent Form](https://www.ahrq.gov/health-literacy/informed-consent-telehealth.html)
2. Southwest Telehealth Resource Center: [Telemedicine & Informed Consent: How Informed Are You?](https://southwesttrc.org/blog/2017/telemedicine-informed-consent-how-informed-are-you)

### CMS Telehealth Resources:

CMS MLN:

<https://www.cms.gov/outreach-and-education/medicare-learning-network-mln/mlnproducts/downloads/telehealthsrvcsfctsht.pdf>

## G-103 California Medical and Privacy Laws

The California Consumer Privacy Act (CCPA) was enacted in 2018 and takes effect on January 1, 2020. This landmark piece of legislation secures new privacy rights for California consumers. On October 10, 2019, Attorney General Xavier Becerra released draft regulations under the CCPA for public comment.

### California Consumer Privacy Act (CCPA)

**The CCPA grants new rights to California consumers:**

* 1. The right to know what personal information is collected, used, shared, or sold, both as to the categories and specific pieces of personal information.
  2. The right to delete personal information held by businesses and by extension, a business’s service provider.
  3. The right to opt-out of sale of personal information. Consumers are able to direct a business that sells personal information to stop selling that information. Children under the age of 16 must provide opt-in consent, with a parent or guardian consenting for children under 13.
  4. The right to non-discrimination in terms of price or service when a consumer exercises a privacy right under CCPA.

### The CCPA applies to certain businesses.

**Businesses are subject to the CCPA if one or more of the following are true:**

* 1. Has gross annual revenues in excess of $25 million.
  2. Buys, receives, or sells the personal information of 50,000 or more consumers, households, or devices.
  3. Derives 50 percent or more of annual revenues from selling consumers’ personal information.
  4. As proposed by the draft regulations, businesses that handle the personal information of more than 4 million consumers will have additional obligations.

### The CCPA imposes new business obligations.

**Businesses subject to the CCPA must provide notice to consumers at or before data collection:**

* 1. Businesses must create procedures to respond to requests from consumers to opt-out, know, and delete.
  2. For requests to opt-out, businesses must provide a “Do Not Sell My Info” link on their website or mobile app.
  3. Businesses must respond to requests from consumers to know, delete, and opt-out within specific timeframes. As proposed by the draft regulations, businesses must treat user-enabled privacy settings that signal a consumer’s choice to opt-out as a validly submitted opt-out request.
  4. Businesses must verify the identity of consumers who make requests to know and to delete, whether or not the consumer maintains a password-protected account with the business.
  5. As proposed by the draft regulations, if a business is unable to verify a request, it may deny the request, but must comply to the greatest extent it can. For example, it must treat a request to delete as a request to opt-out.
  6. As proposed by the draft regulations, businesses must disclose financial incentives offered in exchange for the retention or sale of a consumer’s personal information and explain how they calculate the value of the personal information. Businesses must also explain how the incentive is permitted under the CCPA.
  7. As proposed by the draft regulations, businesses must maintain records of requests and how they responded for 24 months in order to demonstrate their compliance.
  8. In addition, businesses that collect, buy, or sell the personal information of more than 4 million consumers have additional record-keeping and training obligations.

### Cost Estimates for CCPA compliance

* 1. According to estimates in the Standardized Regulatory Impact Assessment for the CCPA regulations, the CCPA will protect over $12 billion worth of personal information that is used for advertising in California each year.
  2. Preliminary estimates suggest a total of $467 million to $16,454 million in costs to comply with the draft regulation, if finalized, during the period 2020-2030.2 CCPA and GDPR the California Consumer Privacy Act (CCPA) and the European Union’s General Data Protection Regulation (GDPR) are separate legal frameworks with different scopes, definitions, and requirements.
  3. A business that complies with GDPR and is subject to CCPA may have additional obligations under CCPA.
  4. For example, under GDPR, companies must undertake a data inventory, and mapping of data flows in furtherance of creating records to demonstrate compliance. Additional data mapping may be important to reflect the different requirements under CCPA.
  5. Under GDPR, companies must develop processes and/or systems to respond to individual requests for access to personal information and for erasure of personal information. These processes and/or systems may be applied to handling CCPA consumer requests, although businesses may need to review and reconcile the different definitions of personal information and applicable rules on verification of consumer requests.
  6. Under GDPR, companies must disclose data privacy practices in a privacy policy. CCPA also requires companies to disclose specific business practices in a comprehensive privacy policy.
  7. Many California companies that operate commercial websites and online services must post a privacy policy under the California Online Privacy Protection Policy (CalOPPA) and will need to update this policy for CCPA.
  8. Under GDPR, companies must draft and execute written contracts with their service providers (“processors”). Companies may need to review these contracts to reflect requirements under CCPA.

### Next steps in the regulatory process

* 1. The Attorney General is required to promulgate regulations to clarify and operationalize the CCPA.
  2. After holding seven statewide public forums and reviewing over 300 written comments during the preliminary rulemaking stage, the Attorney General released draft regulations on October 10, 2019.
  3. The Attorney General will consider all comments and may revise the regulations in response.
  4. Any revision to the proposed regulations will be subject to an additional 15-day public comment period.
  5. Following the comment period, the Attorney General will submit the final text of the regulations, the final Statement of Reasons responding to every comment submitted, and an updated informative digest to the Office of Administrative Law.
  6. OAL has 30 working days to review the regulations, and if approved, the rules will go into effect.

Visit the State of California Department of Justice Website for more details and updates.

<https://www.oag.ca.gov/privacy/ccpa>

## G-104 Florida Information Protection Act of 2014 (FIPA)

The Florida Information Protection Act of 2014 (FIPA) is effective July 1, 2014. Under FIPA, a covered entity is defined as a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. This also can include a government entity. Importantly, FIPA is a Florida state law with broad enforcement and includes companies doing business in Florida. Those with clients/patients in Florida are responsible for complying with FIPA requirements.

### FIPA Protections for Consumer’s Personal Information

* 1. An individual’s first name or first initial and last name in combination with any one or more of the following data elements for that individual:
     1. Social Security number and/or A driver’s license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity.
     2. A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual’s financial account.
     3. Any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
     4. An individual’s health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
     5. Patient Records include any material, regardless of physical form, on which personal information is recorded or reserved – including written or spoken words, graphics, or print.
     6. A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

### FIPA Exclusions

### Data elements do not include information about an individual that has been made publicly available by a federal, state, or local governmental entity.

### Data does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

### 3. Requirements for Data Security

### Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information.

### 

### Notice to the Department of the Security Breach

### A covered entity shall provide notice to the department of any breach of security affecting 500 or more individuals in his/her state.

### Such notice must be provided to the department as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred.

### A covered entity may receive 15 additional days to provide notice as required in subsection (4) if good cause for delay is provided in writing to the department within 30 days after the determination of the breach or reason to believe a breach occurred.

### The written notice to the department must include A synopsis of the events surrounding the breach at the time notice is provided.

### The number of individuals in this state who were or potentially have been affected by the breach.

### Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions as to how to use such services. A copy of the notice required under subsection (4), or an explanation of the other actions taken pursuant to subsection (4).

### The name, address, telephone number, and e-mail address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.

### The covered entity must provide the following information to the department upon its request.

### A police report, incident report, or computer forensics report.

### A copy of the policies in place regarding breaches.

### Steps that have been taken to rectify the breach.

### Notice to Individuals

* 1. A covered entity shall give notice to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach. Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay authorized under paragraph (b) or waiver under paragraph (c).
  2. If a federal, state, or local law enforcement agency determines that notice to individuals required under this subsection would interfere with a criminal investigation, the notice shall be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary.
  3. A law enforcement agency may, by a subsequent written request, revoke such delay as of a specified date or extend the period set forth in the original request made under this paragraph to a specified date if further delay is necessary.
  4. Notwithstanding paragraph (a), notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed.
  5. Such a determination must be documented in writing and maintained for at least 5 years.
  6. The covered entity shall provide the written determination to the department within 30 days after the determination.
  7. The notice to an affected individual shall be by one of the following methods: Written notice sent to the mailing address of the individual in the records of the covered entity, or an e-mail notice sent to the e-mail address of the individual in the records of the covered entity.

### Minimum Requirements for a Breach of Security Involving an Individual

* 1. The date, estimated date, or estimated date range of the breach of security.
  2. A description of the personal information that was accessed or reasonably believed to have been accessed as a part of the breach of security.
  3. Information that the individual can use to contact the covered entity to inquire about the breach of security and the personal information that the covered entity maintained about the individual.
  4. A covered entity required to provide notice to an individual may provide substitute notice in lieu of direct notice if such direct notice is not feasible because the cost of providing notice would exceed $250,000, because the affected individuals exceed 500,000 persons, or because the covered entity does not have an e-mail address or mailing address for the affected individuals. Such substitute notice shall include the following:
  5. A conspicuous notice on the Internet website of the covered entity if the covered entity maintains a website, and,
     1. Notice in print and to broadcast media, including major media in urban and rural areas where the affected individuals reside.
  6. Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity’s primary or functional federal regulator is deemed to be in compliance with the notice requirement in this subsection if the covered entity notifies affected individuals in accordance with the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security.

* 1. Under this paragraph, a covered entity that timely provides a copy of such notice to the department is deemed to be following the notice requirement in subsection (3).

### Notice to Credit Reporting Agencies

* 1. If a covered entity discovers circumstances requiring notice pursuant to this section of more than 1,000 individuals at a single time, the covered entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices.

### Requirements for Disposal of Patient Records

* 1. Each covered entity or third-party agent shall take all reasonable measures to dispose of or arrange for the disposal of patient records containing personal information within its custody or control when the records are no longer to be retained. Such disposal shall involve shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

### Enforcement

* 1. A violation of this section shall be treated as an unfair or deceptive trade practice in any action brought by the department under s. 501.207 against a covered entity or third-party agent.
  2. In addition to the remedies provided for in paragraph (a), a covered entity that violates subsection (3) or subsection (4) shall be liable for a civil penalty not to exceed $500,000, as follows:
  3. In the amount of $1,000 for each day up to the first 30 days following any violation of subsection (3) or subsection (4) and, thereafter, $50,000 for each subsequent 30-day period or portion thereof for up to 180 days.
  4. If the violation continues for more than 180 days, in an amount not to exceed $500,000.
  5. The civil penalties for failure to notify provided in this paragraph apply per breach and not per individual affected by the breach.

### No Private Cause of Action

* 1. This section does not establish a private cause of action.

### Public Records Exemption

* 1. All information received by the department pursuant to a notification required by this section, or received by the department pursuant to an investigation by the department or a law enforcement agency, is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution until such time as the investigation is completed or ceases to be active.
  2. This exemption shall be construed in conformity with s. 119.071(2)(c).
  3. During an active investigation, information made confidentially and exempt pursuant to paragraph (a) may be disclosed by the department:
     1. In the furtherance of its official duties and responsibilities.
     2. For print, publication, or broadcast if the department determines that such release would assist in notifying the public or locating or identifying a person that the department believes to be a victim of a data breach or improper disposal of patient records, except that information made confidential and exempt by paragraph (c) may not be released pursuant to this subparagraph; or
     3. To another governmental entity in the furtherance of its official duties and responsibilities.
  4. Upon completion of an investigation or once an investigation ceases to be active, the following information received by the department shall remain confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution:
     1. All information to which another public records exemption applies.
     2. Personal information.
     3. A computer forensic report.
     4. Information that would otherwise reveal weaknesses in a covered entity’s data security.
     5. Information that would disclose a covered entity’s proprietary information.
     6. For purposes of this subsection, the term “proprietary information” means information that:
     7. It is owned or controlled by the covered entity.
     8. It is intended to be private and is treated by the covered entity as private because disclosure would harm the covered entity or its business operations.
     9. Has not been disclosed except as required by law or a private agreement that provides that the information will not be released to the public.
     10. It is not publicly available or otherwise readily ascertainable through proper means from another source in the same configuration as received by the department, which includes:
     11. Trade secrets as defined in s. 688.002.
     12. Competitive interests, the disclosure of which would impair the competitive business of the covered entity who is the subject of the information.
     13. This subsection is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed on October 2, 2019, unless reviewed and saved from repeal through reenactment by the Legislature. As of November 30, 2019, there are no known public notices regarding the review or the enactment of this subsection.

## G-105 Texas HB 300

### Introduction

Compliance with Texas HB 300 is mandatory for all covered entities that are based in Texas or do business with Texas residents. Covered entities under Texas HB 300 differ from covered entities as defined in HIPAA. Texas HB 300 expanded the HIPAA definition of a covered entity (healthcare providers, health plans, and healthcare clearinghouses) to include any entity or individual that possesses, obtains, assembles, collects, analyzes, evaluates, stores, or transmits protected health information in any form.

Texas HB 300, therefore, applies to all healthcare organizations, including those that are not covered by HIPAA, and also lawyers, schools, universities, researchers, accountants, Internet service providers, IT service providers, government agencies, and individuals who maintain a website that collects, stores, or interacts with PHI.

### Texas HB 300 Exemptions

* 1. Not-for-profit agencies that pay for healthcare services or prescription drugs for indigent persons if the primary business of the agency is not the provision of healthcare services or reimbursement for healthcare services.
  2. Workers’ compensation insurance and any entity or individual who acts in connection with the provision, support, administration, or coordination of benefits under a self-insured workers’ compensation program.
  3. Employee benefit plans and entities or individuals that act in connection with those plans.
  4. Entities or individuals that provide, administer, support, or coordinate benefits associated with compensation for victims of crime.
  5. Processing of certain payment transactions by financial institutions and education records covered by the Family Educational Rights and Privacy Act of 1974.

### Texas HB 300 Training for Employees

* 1. All employees who are required to handle PHI or sensitive personal information (SPI), or are likely to encounter PHI, are required to undergo formal privacy training within 60 days of commencing employment.
  2. Texas HB 300 requires additional privacy training to be provided at least every two years.
  3. Training sessions need to be tailored to the role and responsibilities of the employee.
  4. All training must be documented, and employees are required to sign to confirm that they have received the training.
  5. CSM Team shall ensure that new staff receives privacy training upon hire and every 2 years from the date they received the training.
  6. Existing employees must be assigned privacy training every two-years.
  7. Training is assigned in the MedTrainer LMS and completed by the Workforce Member at <https://lms.medtrainer.com> (username and password required).
  8. The complete report is available for review by the manager on demand.

### Texas HB 300 Penalties for Noncompliance:

* 1. The Texas attorney general can issue civil monetary penalties to entities and individuals that fail to comply with the legislation.
  2. State licenses can also be revoked in cases where an entity or individual has demonstrated continued noncompliance.
  3. The penalties for noncompliance with Texas HB 300 are broken down into tiers:
     1. **Tier 1:** Up to $5,000 per violation, per year, for violations due to negligence
     2. **Tier 2:** Up to $25,000 per violation, per year, for a knowing or intentional violation
     3. **Tier 3:** Up to $250,000 per violation, per year, for an intentional violation for financial gain
     4. The maximum financial penalty is $1.5 million per year in cases with a pattern of noncompliance.

## G-106 Workforce Members

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), covers both individuals and organizations. Employees, who may also be referred to as “Workforce Members,” may have access to Protected Health Information (PHI), which includes, but is not limited to, medical records, verbal discussion or orders for patients, documentation notes, and all other instances of handling, transmitting, storing, submitting claims, or managing PHI. It is important that Workforce Members understand their role in maintaining PHI security and promptly report any incidents which may have created a breach.

### Workforce Member Responsibilities

* 1. Workforce Members may directly or indirectly gain access to Protected Health Information (PHI) as defined under the federal Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder (HIPAA) during their course of employment.
  2. Workforce Members acknowledge that the PHI is protected from unlawful disclosure by Federal HIPAA regulations and applicable state laws; and may be held accountable for civil and monetary penalties.
  3. Employment is contingent on maintaining the confidentiality of all PHI as set forth in this condition of employment policy and agree to the following:
  4. Term of the Agreement. This agreement shall commence on the date set forth in the first paragraph above. The obligations herein shall continue in effect so long as Employee uses, discloses, creates, or otherwise possesses any PHI created or received during their employment with the employer and until all PHI created or received during their employment with Employer has been returned to Employer.
  5. Use of PHI by Employee. The employee may only use and disclose PHI created or received by them during the term of their employment, on behalf of Employer or any of Employer's clients, for the purposes of carrying out the provisions of the Health Care Provider Contracts.
  6. Maintenance of Security and Privacy of PHI. Employee hereby agrees to maintain the security and privacy of all PHI in a manner consistent with state and federal laws and regulations, including HIPAA, and all other applicable law. Employee further agrees not the use or disclose PHI except as expressly permitted by this Agreement, applicable law, or the Health Care Provider Contracts. Employee further agrees to use appropriate safeguards to prevent use or disclosure of PHI not permitted by this Agreement, applicable law, or the Health Care Provider Contracts.
  7. Prohibition Against Possession and/or Use of Photographic Equipment by Employee During the term of their employment with Employer, Employee agrees they will not use or possess any photographic equipment at any time while performing services on behalf of Employer, while present at Employer's offices or other trade premises, or while present at the trade premises, facility, hospital, or office of any client of Employer.
  8. For the purposes of this Agreement, photographic equipment shall mean any device capable of creating, capturing, or recording still or video graphic digital or analog images including, but not limited to, digital or analog (film) cameras, camera phones or cellular telephones with cameras, and portable digital assistants (PDA's) capable of recording digital images. Employees have the right to take pictures in the workplace; however, it is limited to the National Labor Relations Act when employees are engaged in Section 7 activity, as long as "employees are acting in concert for their mutual aid and protection, and no overriding employer interest."
  9. In regard to HIPAA, patient privacy, workplace safety, and the privacy of co-workers, the employer has a right to prohibit the use of photographic equipment.
  10. Reporting Unauthorized Disclosure of PHI Employee agrees to immediately report to Employer any unauthorized or inadvertent use or disclosure of PHI by Employee, Employer's other employees, Employer's subcontractors, employees of Employer's clients, or any other person or persons which occur while Employee is performing services within the scope of their employment with Employer.
  11. Termination of Employment upon Breach of Agreement Employer may immediately terminate Employee's employment if the Employer determines that Employee has breached a material term of this Agreement. Employer's remedies for breach of this Agreement are cumulative, and termination of Employee's employment shall not preclude Employer from exercising any other remedy, whether at law, equity, or otherwise.
  12. Return of PHI upon Termination of Employment Upon termination of Employee's employment, Employee shall return all PHI, regardless of the form in which it is being stored, acquired, created, or received by Employee on account of Employer or while Employee was performing services within the scope of their employment with Employer. Employee further agrees that they shall retain no copies of any such PHI. The duties of Employee hereunder to maintain the security and privacy of PHI shall survive the termination of Employee's employment with Employer.
  13. Indemnification. Employee shall, to the fullest extent permitted by law, protect, defend, indemnify, and hold harmless Employer and Employer's employees, directors, officers, agents, clients, and the directors, officers, and employees of Employer's clients, (each an Indemnitee) from and against any and all losses, costs, claims, penalties, fines, demands, liabilities, legal actions, judgments, and expenses of every kind (including reasonable attorney’s fees at trial and on appeal) asserted or imposed against any Indemnitee arising out of the acts or omissions of Employee related to the performance or nonperformance of this Agreement.

## G-107 Emergency Contact Information

Introduction

This Policy and Procedure manual is organized into functional sections that are designed for ease-of-use and practical application guides that are designed to demonstrate the intent of the policies and procedures, according to Federal, State, and Local regulations. The government reserves the right to change public policy and laws that supersede or preempt current policies, which may not be immediately available to the covered entity, management staff, and personnel.

This policy manual may not cover all potential privacy rights and security within the regulations, guidelines, civil and criminal penalties, or possible exclusions that may apply to the covered entity environment. If any topic covered in this manual does not clearly define the expected actions and behaviors of CSM Team management, and workforce members, please contact the appropriate Compliance Officer or Government Agency noted in this policy.

Scope

This Policy and Procedures apply to CSM Team and its business associates. In the event that the federal, state, or local regulations are more restrictive than the Policies and Procedures in this manual, the guidelines that are most restrictive shall apply.

Emergency Contact Numbers

The person utilizing these policies and procedures in emergency situations shall consider the chain-of-command when reporting emergencies, which begins with the immediate supervisor, followed by the covered entity Manager. In all emergency situations, the person making contact shall have as much information available as possible regarding the nature of the emergency, the types and the possible number of records involved, and if possible, the steps taken to mitigate the breach of Protected Health Information.

### Local Contact Information

**Facility Lead Administrator / Compliance Officer:**

**Director of Human Resources:**

**Emergency Contact:**

**Health and Human Services (HHS) Contact Information**

For direct media inquiries to the HHS: Press Office at (202) 690-6343

For questions related to Health Information Privacy or Patient Safety, e-mail [OCRPrivacy@hhs.gov.](mailto:OCRPrivacy@hhs.gov.)

For non-privacy related inquiries, including comments or questions about OCR's web site, e-mail [OCRMail@hhs.gov](mailto:OCRMail@hhs.gov) or write to:

**Office for Civil Rights**

U.S. Department of Health and Human Services

200 Independence Avenue, SW Room 509F, HHH Building Washington, D.C. 20201 Toll-free: (800) 368-1019: TDD toll-free: (800) 537-7697

**Southeast Region - Atlanta**

**(Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, Tennessee)**

Office for Civil Rights U.S. Department of Health and Human Services

Sam Nunn Atlanta Federal Center, Suite 16T70 61 Forsyth Street, S.W. Atlanta, GA 30303-8909

Patient Response Center : (800) 368-1019 Fax : (202) 619-3818 TDD :(800) 537-7697 e-mail : [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**Florida Health**

General Information: 850-488-2323

Email Address: health@flhealth.gov.

**New England Region - (Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont)**

Office for Civil Rights U.S. Department of Health and Human Services Government Center

J.F. Kennedy Federal Building - Room 1875 Boston, MA 02203

Patient Response Center : (800) 368-1019 Fax : (202) 619-3818 TDD : (800) 537-7697 e-mail : [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**Eastern and Caribbean Region - (New Jersey, New York, Puerto Rico, Virgin Islands)**

Office for Civil Rights U.S. Department of Health and Human Services

Jacob Javits Federal Building 26 Federal Plaza - Suite 3312 New York, NY 10278

Patient Response Center : (800) 368-1019 Fax : (202) 619-3818 TDD : (800) 537-7697 e-mail : [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**Mid-Atlantic Region - (Delaware, District of Columbia, Maryland, Pennsylvania, Virginia, West Virginia)**

Office for Civil Rights U.S. Department of Health and Human Services

150 S. Independence Mall West, Suite 372, Public Ledger Building Philadelphia, PA 19106-9111

Patient Response Center : (800) 368-1019 Fax : (202) 619-3818 TDD : (800) 537-7697 e-mail : [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**Midwest Region - (Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, Ohio, Wisconsin)**

Office for Civil Rights U.S. Department of Health and Human Services 233 N. Michigan Ave., Suite 240 Chicago, IL 60601

Patient Response Center : (800) 368-1019 ; Fax : (202) 619-3818 ; TDD : (800) 537-7697 e-mail : [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**Kansas City**

Office for Civil Rights - U.S. Department of Health and Human Services 601 East 12th Street - Room 353 Kansas City, MO 64106

Patient Response Center : (800) 368-1019 ; Fax : (202) 619-3818 ; TDD : (800) 537-7697 e-mail : [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**Southwest Region - (Arkansas, Louisiana, New Mexico, Oklahoma, Texas)**

Office for Civil Rights - U.S. Department of Health and Human Services 1301 Young Street, Suite 1169 Dallas, TX 75202

Patient Response Center : (800) 368-1019 ; Fax : (202) 619-3818 ; TDD : (800) 537 7697 e-mails : [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**Rocky Mountain Region - (Colorado, Montana, North Dakota, South Dakota, Utah, Wyoming)**

HHS/Office for Civil Rights

1961 Stout Street Room 08-148 Denver, CO 80294

Patient Response Center : (800) 368-1019 ; Fax : (202) 619-3818 ; TDD : (800) 537-7697 e-mail : [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**Pacific Region - (Alaska, American Samoa, Arizona, California, Commonwealth of the Northern Mariana Islands, Federated States of Micronesia, Guam, Hawaii, Idaho, Marshall Islands, Nevada, Oregon, Republic of Palau, Washington)**

Office for Civil Rights U.S. Department of Health and Human Services 90 7th Street, Suite 4-100 San Francisco, CA 94103

Patient Response Center : (800) 368-1019 ; Fax : (202) 619-3818 ; TDD : (800) 537-7697 e-mail : [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

## G-108 Roles and Responsibilities

Purpose

The role of leadership for HIPAA Compliance at CSM Team is defined by the Governing Body of the organization, which may be delegated to a location by onsite or offsite representatives, which for the purpose of this policy shall be defined as the Compliance Officer.

The purpose of the HIPAA Policy Manual is to provide the structure, policies, and procedures for the security of confidential and protected information throughout the organization. This policy applies to all board members, employees, volunteers, agents, interns, contractors, and agents, regardless of whether or not the individual in question works directly with such information. Individuals who have access to confidential information must ensure that such information, in whatever form it exists, is handled in strict accordance with this policy and applicable legal, accreditation and regulatory requirements regarding safeguarding confidential information.

It is the intent of CSM Team that the responsibility for maintaining HIPAA compliance is not totally dependent on leadership, rather that leadership can depend on a fully trained and aware workforce, to identify and close gaps in HIPAA privacy and security that they encounter in their daily responsibilities. It is imperative that ALL members of the CSM Team, including employees, interns, students, volunteers, and any member that has access or control of PHI to ***SPEAK UP*** to their supervisor or leadership if a potential vulnerability exists that is not being immediately addressed.

### The Role of the Compliance Officer

* 1. The Compliance Officer ensures continued compliance with all national, state, and local regulations related to medications and their management.
  2. The Compliance Officer will coordinate additional resources as needed to include legal advice and intervention, outside specialist, and internal resources to address the issues of the breach and make recommendations and additional policies as needed.
  3. The Compliance Officer shall maintain the overall responsibility for the ongoing maintenance, security, access, and updates for all CSM Team information systems.
  4. This includes assigning access, data back-up, authentications, and digital signatures guidelines and assignments.
  5. The Compliance Officer shall conduct or oversee internal and external system audits to include the establishment of periodic BA audits or reviews.
  6. The results of the audit shall be shared with the appropriate executive for collaboration and coordination of improvement activities and policy development.
  7. The Compliance Officer shall maintain emergency management procedures for all systems in the event of a major catastrophe, significant breach, or equipment malfunction, to include temporary measures to ensure that patient/patient care and PHI are not compromised.
  8. The Compliance Officer may appoint shift HIPAA Compliance Specialist in their absence. Shift Compliance Specialist must have additional training beyond the basic HIPAA Guidelines to include HIPAA for Managers and Supervisors or an equivalent training course.
  9. Complaints and concerns regarding procedural issues, potential or identified risks, suggestions for improvements, and reports of a breach or potential breaches shall be directed to the Compliance Officer who can be reached at:

### Workforce Members

### Workforce Members shall maintain personal responsibility for maintaining PHI security and system integrity at all times and shall report any breaches, attempted breaches, and potential security issues to the Compliance Officer (to include notification to their immediate supervisor).

* 1. Taking personal responsibility includes taking precautions when handling PHI in any format, not sharing or compromising passwords, not using or transferring PHI to unauthorized electronic devices (laptops, PDA’s, removable storage devices), ensuring that PHI is encrypted if authorized to send electronically, and to limit discussions that may involve PHI in public places, around other Workforce Members that do not have the authorization to listen to potential PHI disclosures, and among family and friends.
  2. Workforce Members must protect their passwords and PHI that could be visible by others, by signing out of devices when unattended. Report any unusual e-mails or password compromises to your immediate supervisor. All electronic devices used in conjunction with PHI must be approved in advance by the Compliance Officer.
  3. If a Workforce Member knows or should have known of any violation of the HIPAA Policy or any act that would compromise PHI, the Workforce Member is obligated to bring the violation to the attention of your supervisor or the Compliance Officer.
  4. Supervisors are required to report violations to the Compliance Officer and will not disclose the source of the information when legally acceptable for the source to remain confidential. Disclosures that are made by Workforce Members that accidentally violate the policy that does not result in a reportable breach of PHI will not be subject to severe disciplinary action, if such violations are found to be accidental, non-malicious, and are disclosed to help improve the security of PHI.
  5. Any Workforce Member that knowingly or maliciously violates the HIPAA Policy may be subject to severe disciplinary action, up to and including suspension and termination of employment for the first occurrence. Incidents of this nature will be reviewed by Human Resources and Legal Counsel.
  6. Workforce Members are advised that **intentional release or participation in potential criminal activities** associated with or involved with the release of PHI may also be subject to criminal and/or civil penalties to the maximum allowable by law. The Compliance Officer reports all suspected criminal actives related to HIPAA laws to the local law enforcement agency.

A definition of ***Workforce Member*** can be found in [Quick Information Guide 3.0: HIPAA Definitions.](#_bookmark28)

### Business Associates

* 1. Business Associates are required to sign and adhere to the CSM Team business associate agreement in order to provide goods and services as a “covered entity” as defined by HIPAA, HITECH, and the Final Omnibus Rule. Business Associates must not make assumptions about Workforce Members' authorization for access to PHI and must ensure that PHI is not accidentally transmitted or requested from unauthorized sources.
  2. Business Associates must have the appropriate protections and systems in place to prevent, detect, and respond to malware, viruses, and other sources used to breach PHI data. All breaches of PHI must be reported immediately to the Compliance Officer and the manager or supervisor on duty at the covered entity or to the **emergency contact number located in Policy G-101 Emergency Contact Information**.
  3. “A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronically protected health information in accordance with the HIPAA Security Rule.”
  4. Violations of the Medical Ligeia Policy or violations of the HIPAA, HITECH, and Final Omnibus Rules may result in termination of the business associates’ contract for goods and services. Cancellation of Agreements under this provision are not subject to penalties or liquidated damages due to early termination.

A definition of a ***business associate*** can be found in [Quick Information Guide 3.0: HIPAA Definitions.](#_bookmark28)

## G-109 Breach and Notification Guidelines

Introduction

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the HITECH Act. CSM Team is a “covered entity” that must abide by the rule, and have a process for communicating to individuals, groups of individuals, the public, media, and the Secretary of HHS.

Scope

This policy covers all Workforce Members, business associates, and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team In the event it is not clear if this policy applies to you, please contact the Compliance Officer.

### Exceptions to the Breach Notification Rule

* 1. A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.
  2. The Compliance Officer will conduct a review of breaches and disclosure of protected health information to determine if there was an actual and reportable breach or if there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
  3. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; The unauthorized person who used the protected health information or to whom the disclosure was made; Whether the protected health information was actually acquired or viewed; and the extent to which the risk to the protected health information has been mitigated.
  4. Covered entities and business associates, where applicable, have the discretion to provide the required breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the protected health information has been compromised.
  5. There are ***three exceptions to the definition of “breach.”*** The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the scope of authority.
  6. The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
  7. The final exception applies if the Covered Entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.
  8. Covered Entities and business associates must only provide the required notifications if the breach involved unsecured protected health information. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.

Breach Notification Requirements

Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

### Individual Notice

### Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.

* 1. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside.
  2. The covered entity must include a toll- free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach.
  3. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.
  4. These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or business associate, as applicable).
  5. A breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate. Covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual.

### Media Notice

### 

### Covered entities that experience **a breach affecting more than 500 residents of a state or jurisdiction** are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the state or jurisdiction.

* 1. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area.
  2. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

### Notice to the Secretary

### In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site:

[(http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html)](http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html).

The website is used to electronically submit a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

### Notification by a Business Associate

* 1. If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any other available information required to be provided by the covered entity in its notification to affected individuals.

### Responding to Possible Breaches

* 1. Given the potential consequences, it is critical that covered entities and business associates respond appropriately to potential HIPAA breaches to avoid or minimize their liability. Below are steps that you may follow to help identify and timely respond to HIPAA breaches.
  2. **Stop the breach.** Immediate action may help avoid or mitigate the effects of a breach. Terminate improper access to PHI; retrieve any PHI that was improperly disclosed and obtain assurances from recipients that they have not used or disclosed the PHI, and/or will not, further use or disclose PHI that was improperly accessed. Document your actions and the recipient’s response.
  3. **Contact the privacy officer.** Each covered entity must have a designated privacy officer who (hopefully) has the training and experience to properly investigate and respond to a potential breach. Deadlines for responding to breaches generally run from the date that anyone in the organization knew of the breach except the person committing the breach (*see* 45 CFR 164.404(b); 78 FR 5647); accordingly, workforce members should be trained to notify the privacy officer as soon as they become aware of a breach so that appropriate steps can be taken to investigate, mitigate, and respond to any potential breach.
  4. **Respond promptly.** Swift, appropriate action is critical for at least four reasons. First, covered entities have an affirmative obligation to mitigate the effects of any breach. (45 CFR 164.530(f)). Second, prompt action may help avoid or mitigate further breaches, which is an important factor in determining whether a breach must be reported. (45 CFR 164.402). Third, as discussed above, a covered entity or business associate may avoid penalties if they correct a violation within 30 days. (45 CFR 160.410(b)). And fourth, the breach notification rule requires that notice of reportable breaches be given “without unreasonable delay,” but no later than 60 days after discovery. (45 CFR 164.404).
  5. **Investigate appropriately.** Confirm the “who, what, when, why, how, and how much” with persons involved, including persons who committed the alleged violation; persons who may have received PHI improperly; and other relevant witnesses. Confirm the nature and amount of the PHI that was accessed, used, or disclosed, and why they accessed or disclosed the PHI. Ensure there was no redisclosure and that there will be no further redisclosure. In your discussions, ensure that you do not inadvertently disclose additional PHI. Also, beware acting too swiftly: sometimes, a full investigation reveals additional facts that confirm no reportable breach occurred. Do not report a suspected breach before you have actually concluded that a reportable breach occurred. Document your investigation, including obtaining witness statements and sending confirming letters as appropriate. For example, you may want to send a letter to alleged recipients confirming the extent of their access or disclosure of PHI and warning them of the penalties that may apply if they further use or disclose PHI improperly. (*See* 42 USC 1320d-6).
  6. **Mitigate the effects of the breach.** HIPAA requires that a covered entity mitigate any harmful effects of a breach to the extent practicable. (45 CFR 164.530(f)). Mitigation may include retrieving, deleting, or destroying improperly disclosed PHI; terminating access or changing passwords; remote wiping mobile devices; modifying policies or practices; warning recipients of potential penalties for further violations; *etc.* In some cases, it might include paying for the cost of a credit monitoring service or similar action, and/or notifying affected individuals even if the breach is not required to be reported under the breach notification rules.
  7. **The response will depend on the circumstances**. If a covered entity knows that a business associate is violating HIPAA, it must either take steps to cure the breach or terminate the business associate agreement. (45 CFR 164.504(e)(1)).
  8. **Correct the breach.** Remember: a covered entity may avoid HIPAA penalties if it did not act with willful neglect and corrects the problem within 30 days. (45 CFR 160.410(b)). Change processes; implementing new safeguards; modifying policies; training employees; *etc.* (*See* 75 FR 40879).
  9. **Impose sanctions.** HIPAA requires that covered entities impose and document appropriate sanctions against workforce members who violate HIPAA or privacy policies. (45 CFR 164.530(e)). The sanction should fit the crime: it may range from a written warning and additional training to suspension or termination.
  10. **Determine if the breach must be reported to the individual and HHS**. Under the breach notification rule, covered entities are only required to self-report if there is a “breach” of “unsecured” PHI. (45 CFR 164.400 *et seq.*).
  11. **Unsecured PHI**. “Unsecured” PHI is that which is “not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology” specified in HHS guidance. (45 CFR 164.402). Currently, there are only two ways to “secure” PHI:
  12. I**n the case of electronic PHI, by encryption that satisfies HHS standards, or (2) in the case of e-PHI or PHI maintained in hard copy form, by its complete destruction** **(74 FR 42742)**. Breaches of “secured” PHI need not be reported. Most potential breaches will involve “unsecured” PHI.
  13. **Breach.** The unauthorized “acquisition, access, use, or disclosure” of unsecured PHI in violation of the HIPAA privacy rule is presumed to be a reportable breach unless the covered entity or business associate determines that there is a low probability that the data has been compromised or the action fits within an exception. (45 CFR 164.402; *see* 78 FR 5641). Thus, the covered entity or business associate must determine the following:
  14. **Was there a violation of the privacy rule?** Breach notification is required only if the acquisition, access, use, or disclosure results from a privacy rule violation; no notification is required if the use or disclosure is permitted by the privacy rules. (45 CFR 164l.402).
  15. **For example, a covered entity may generally use or disclose PHI for purposes of treatment, payment, or healthcare operations without the individual’s authorization unless the covered entity has agreed otherwise.** (45 CFR 164.506). Disclosures to family members and others involved in the individual’s care or payment for their care is generally permitted if the patient has not objected, and the provider otherwise determines that disclosure is in the patient’s best interest. (45 CFR 164.510).

HIPAA allows certain other disclosures that are required by law or made for specified public safety or government functions. (45 CFR 164.512). Disclosures that are incidental to permissible uses or disclosures do not violate the privacy rule if the covered entity employed reasonable safeguards. (45 CFR §§ 164.402 and 164.502(a)(1)(iii)). When in doubt as to whether a disclosure violates the privacy rule, you should check with your privacy officer or a qualified attorney.

* 1. **Does the violation fit within breach exception?** The following do *not* constitute reportable “breaches” as defined by the HIPAA privacy rule:
  2. **Unintentional acquisition, access, or use of PHI by a workforce member if such acquisition, access, or use was made in good faith and within the scope of the workforce member's authority and does not result in further use or disclosure not permitted by the privacy rules**. (45 CFR 164.402). For example, no breach notification is required where an employee mistakenly looks at the wrong patient's PHI but does not further use or disclose the PHI. (74 FR 42747).
  3. **An inadvertent disclosure by a person who is authorized to access PHI to another authorized person at the same covered entity or business associate and the PHI is not further used or disclosed in a manner not permitted by the privacy rules**. (45 CFR 164.402). For example, no breach notification is required if a medical staff member mistakenly discloses PHI to the wrong nurse at a facility, but the nurse does not further use or disclose the PHI improperly. (74 FR 42747-48).
  4. **A disclosure in which the person making the disclosure has a good faith belief that the unauthorized recipient would not reasonably be able to retain the PH**I. (45 CFR 164.402). For example, no notification is required if a nurse mistakenly hands PHI to the wrong patient but immediately retrieves the information before the recipient has a chance to read it. (74 FR 42748).
  5. **Is there a “low probability that the data has been compromised?”** No breach report is required if “there is a low probability that the [PHI] has been compromised based on a risk assessment” of at least the following factors listed in 45 CFR 164.402.
  6. **The nature and extent of the PHI involved, including the type of information, identifiers, and the likelihood of identification.** For example, PHI involving financial data (*e.g.*, credit card numbers, social security numbers, account numbers, *etc.*), sensitive medical information (*e.g.*, mental health, sexually transmitted diseases, substance abuse, *etc.*), or detailed clinical information (*e.g.*, names and addresses, treatment plan, diagnosis, medication, medical history, test results, *etc.*) create a higher probability that data has been compromised and must be reported. (78 FR 5642-43). Conversely, merely disclosing the patient’s name without disclosing their health condition may not be reportable.
  7. The unauthorized person who impermissibly used the PHI or to whom the disclosure was made. For example, disclosure to another health care provider or a person within the entity's organization would presumably involve a low probability that the data is compromised because such persons are more likely to comply with their confidentiality obligations and are unlikely to misuse or further disclose the PHI. Similarly, there is a lower risk of compromise if the entity who receives the PHI lacks the ability to identify entities from the limited information disclosed. (78 FR 5643).
  8. Whether the PHI was actually acquired or viewed. For example, there is likely a low risk if a misdirected letter is returned unopened or a lost computer is recovered, and it is confirmed that PHI was not accessed. Conversely, there is a higher risk where the recipient opens and reads a misdirected letter even though she reports the letter to the covered entity. (78 FR 5643).
  9. Whether the risk to the PHI has been mitigated. For example, there may be a lower risk if a fax is directed to the wrong number, but the recipient confirms that they returned or destroyed the PHI; the PHI was not accessed, used or disclosed, and will not be further used or disclosed; and the recipient is reliable. (78 FR 5643). This factor highlights the need for covered entities and business associates to immediately identify and respond to potential breaches to reduce the probability that PHI is compromised and the necessity of breach reporting.
  10. The risk assessment should involve consideration of all of these factors in addition to others that may be relevant. One factor is not necessarily determinative, and some factors may offset or outweigh others, depending on the circumstances. (*See* 78 FR 5643). If you conclude that the risk assessment demonstrates a low probability that the PHI has been compromised, you should document your analysis and you may forego breach notification. On the other hand, if the risk assessment fails to demonstrate a low probability that the PHI has been compromised, you are required to report the breach to the affected individual and HHS as described below.

CSM Team Compliance Officer must be informed of all business associate Breach Notifications. In the event the Compliance Officer is not available, inform the Administrator or Director of Human Resources.

Examples of Specific Exceptions to the Breach Notification Rule

1. Private Practice Implements Safeguards for Waiting Rooms

Covered Entity: Private Practice

Issue: Safeguards; Impermissible Uses and Disclosures

A staff member of a medical practice discussed HIV testing procedures with a patient in the waiting room, thereby disclosing PHI to several other individuals. Also, computer screens displaying patient information were easily visible to patients. Among other corrective actions to resolve the specific issues in the case, Office for Civil Rights (OCR) required the provider to develop and implement policies and procedures regarding appropriate administrative and physical safeguards related to the communication of PHI. The practice trained all staff on the newly developed policies and procedures. In addition, OCR required the practice to reposition its computer monitors to prevent patients from viewing information on the screens, and the practice installed computer monitor privacy screens to prevent impermissible disclosures.

1. Entity Rescinds Improper Charges for Medical Record Copies to Reflect Reasonable, Cost-Based Fees

Covered Entity: Private

Practice Issue: Access

A patient alleged that a covered entity failed to provide him access to his medical records. After OCR notified the entity of the allegation, the entity released the complainant’s medical records but also billed him $100.00 for a “records review fee” as well as an administrative fee. The Privacy Rule permits the imposition of a reasonable cost-based fee that includes only the cost of copying and postage and preparing an explanation or summary if agreed to by the individual. To resolve this matter, the covered entity refunded the $100.00 “records review fee.”

1. Private Practice Revises Process to Provide Access to Records

Covered Entity: Private

Practices Issue: Access

A private practice failed to honor an individual's request for a complete copy of her minor son's medical record. OCR's investigation determined that the private practice had relied on state regulations that permit a covered entity to provide a summary of the record. OCR provided technical assistance to the covered entity, explaining that the Privacy Rule permits a covered entity to provide a summary of patient records rather than the full record only if the requesting individual agrees in advance to such a summary or explanation. Among other corrective actions to resolve the specific issues in the case, OCR required the covered entity to revise its policy. In addition, the covered entity forwarded the complainant a complete copy of the medical record.

1. Private Practice Revises Process to Provide Access to Records Regardless of Payment Source

Covered Entity: Private

Practices Issue: Access

At the direction of an insurance company that had requested an independent medical exam of an individual, a private medical practice denied the individual a copy of the medical records. OCR determined that the private practice denied the individual access to records to which she was entitled by the Privacy Rule. Among other corrective actions to resolve the specific issues in the case, OCR required that the private practice revise its policies and procedures regarding access requests to reflect the individual's right of access regardless of payment source.

1. Private Practice Provides Access to All Records, Regardless of Source

Covered Entity: Private Practice Issue: Access

A private practice denied an individual access to his records on the basis that a portion of the individual's record was created by a physician not associated with the practice. While the amendment provisions of the Privacy Rule permit a covered entity to deny an individual's request for an amendment when the covered entity did not create that the portion of the record subject to the request for amendment, no similar provision limits individuals' rights to access their protected health information. Among other steps to resolve the specific issue in this case, OCR required the private practice to revise its access policy and procedures to affirm that, consistent with the Privacy Rule standards, patients have access to their record regardless of whether another entity created information contained within it.

1. Physician Revises Faxing Procedures to Safeguard PHI

Covered Entity: Health Care

Provider Issue: Safeguards

A doctor's office disclosed a patient's HIV status when the office mistakenly faxed medical records to the patient's place of employment instead of to the patient's new health care provider. The employee responsible for the disclosure received a written disciplinary warning, and both the employee and the physician apologized to the patient. To resolve this matter, OCR also required the practice to revise the office's fax cover page to underscore a confidential communication for the intended recipient. The office informed all its employees of the incident and counseled staff on proper faxing procedures.

1. Private Practice Ceases Conditioning of Compliance with the Privacy Rule

Covered Entity: Private Practice

Issue: Conditioning Compliance with the Privacy Rule

A physician practice requested that patients sign an agreement entitled “Consent and Mutual Agreement to Maintain Privacy.” The agreement prohibited the patient from directly or indirectly publishing or airing commentary about the physician, his expertise, and/or treatment in exchange for the physician’s compliance with the Privacy Rule. A patient’s rights under the Privacy Rule are not contingent on the patient’s agreement with a covered entity. A covered entity’s obligation to comply with all requirements of the Privacy Rule cannot be conditioned on the patient’s silence. OCR required the covered entity to cease using the patient agreement.

that conditioned the entity’s compliance with the Privacy Rule. Additionally, OCR required the covered entity to revise its Notice of Privacy Practices.

## G-110 Minimum Necessary Access

Introduction

The HIPAA Privacy Rule requires CSM Team ™, (covered entity) to make reasonable efforts to limit use, disclosure of, and requests for protected health information to the minimum necessary to accomplish the intended purpose. The standard requires an approach consistent with the best practices and guidelines already used by many providers and plans today to **limit the unnecessary sharing of medical information**.

The minimum necessary standard requires the covered entity to evaluate its’ practices and enhance protections as needed to limit unnecessary or inappropriate access to protected health information. The Privacy Rule allows for professional judgment to appropriately limit access to PHI, sacrificing the quality of health care services.

In the CSM Team environment, Workforce Members must only access PHI that is necessary to complete job tasks for which they are properly trained and authorized to access. In the event that PHI is observable by a Workforce Member that does not have the authorization to view, possess, transport, or transfer PHI, the Workforce Member is required to notify their immediate supervisor or Compliance Officer to appropriately remove unauthorized access or possession. It should be noted that identifying HIPAA Breach risk by non-authorized personnel is encouraged to create an environment of safety and security for PHI in the public and behind-the-scenes environment.

Scope

This policy covers all Workforce Members, business associates, and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team In the event it is not clear if this policy applies to you, please contact the Compliance Officer. All Workforce Members are responsible for maintaining the confidentiality and security of Protected Health Information (PHI).

### Minimum Necessary Access to Protected Health Information (PHI)

* 1. Only CSM Team workforce Members designated as authorized by the Compliance Officer or designee are allowed to access the information defined in the designated record set without prior patient written authorization or unless the purpose falls within the scope of allowable disclosures under HIPAA (i.e., treatment) which includes the information needed to ask medically related questions, provide healthcare services, handle associated paperwork, and interact with patient or patient for all types of interactions that involve PHI.
  2. All CSM Team patient information is considered confidential, and only the information needed for the intended purpose should be used by and disclosed to covered Workforce Members who have a “need to know” (i.e., Minimum Necessary).
  3. CSM Team Workforce Member with a “need to know” is defined as someone who needs the information because the information is directly related to the duties and activities the person is required to perform as described in their job description. Without such information, the staff member would not be able to carry out these functions.
  4. Workforce Members who are patients of CSM Team or who have dependents, family members, co-workers, or friends who are patients of the CSM Team must follow standard procedures, applicable to all patients, for accessing their own patient information or the patient information of their dependents, family members, co-workers, or friends.
  5. Patient records should be requested through the responsible designee on duty, who shall notify the Compliance Officer. If the request is made by someone other than the patient, either a HIPAA authorization or a power of attorney indicating that the employee is the patient’s representative would need to be present in the file or submitted prior to the release of PHI.
  6. Staff members may not discuss PHI with their friends, family members, spouses, or any other individual unless allowable by HIPAA (i.e., have knowledge that an individual is participating in healthcare decisions or payment for healthcare for the patient or a power of attorney indicating that the employee is the patient’s representative.).
  7. PHI is protected by law. Inappropriate use or disclosure of CSM Team individually identifiable health information will be reported to the CSM Team Compliance Officer, or designee.
  8. Violations of the “Minimum Necessary Access” rules, whereby an exception does not exist or is not appropriate for the reported use, may be subject to the Workforce Member to disciplinary action, up to and including termination of employment.
  9. Intentional violations of the “Minimum Necessary Access” policy that involves criminal activity will be reported to law enforcement agencies and prosecuted to the fullest extent of the law.

## G-111 Training Requirements

Introduction

The **HIPAA Security Awareness and Training** §164.308(a)(5) requires CSM Team to provide Security Awareness Training. The **HIPAA Privacy Rule** requires CSM Team to train workforce members to ensure an understanding of privacy procedures. HIPAA Security Awareness Training must include information regarding a minimum of four specifications: Security Reminders, Protection from Malicious Software, Log-in Monitoring, and Password Management. These topics can be combined into a single training course, providing that the subject matter is appropriate for the level of access to PHI by the workforce member receiving the training.

Scope

This policy covers all Workforce Members and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team Business associates must have similar training requirements that are subject to audit by CSM Team In the event it is not clear if this policy applies to you, please contact the Compliance Officer.

### Training Guidelines

* 1. New workforce members shall be provided training within their first 10 days of employment unless they can verify equivalent training that they have been deemed competent within the past twelve months in writing or by a certificate of completion.
  2. Retraining shall be given whenever environmental or operational changes affect the security of PHI, which may include new or updated policies and procedures; new or upgraded software or hardware; new security technology; or changes in the Privacy, Security, and Breach Notification Rule.
  3. A review of HIPAA guidelines, additional information such as courses for managers and supervisors, the impact of social media and other HIPAA topics are appropriate to meet annual training requirements.
  4. All training shall be documented and kept in the employee file for a period of no less than seven (7) years.
  5. Workforce members who violate HIPAA policies, including unintentional violations or breaches are subject to retraining after an incident or whenever the supervisor or Compliance Officer deems it necessary.

# Section II – Privacy and Disclosure Rights

## Privacy and Notification Rule

### Introduction

The HIPAA Privacy Rule gives patients or their representative a fundamental new right to be informed of the privacy practices of their health plans and of most of their health care providers, as well as to be informed of their privacy rights with respect to their personal health information. Covered entities are required to develop and distribute a notice that provides a clear explanation of these rights and practices. The notice is intended to focus patient or their representatives on privacy issues and concerns and to prompt them to have discussions with their health plans, health care providers, and the organization's contact information at each location, with the information needed to exercise their rights.

### Scope

This policy covers all Workforce Members, business associates, and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team In the event it is not clear if this policy applies to you, please contact the Compliance Officer.

### The Privacy Rule and Notification Rule

CSM Team is covered by the medical information privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA). The organization must comply with HIPAA and the Regulations in the use and disclosure of health information by which patients and caregivers can be individually identified, also known as Protected Health Information (PHI). The organization at each location is required under Section 164.520 to provide patients this notice (in paper or electronic format) of the privacy practices concerning their PHI.

### Notice Availability

* 1. The location must post the “Privacy Notice” in a ***clear and prominent location*** where a patient or their representative requests healthcare services, check-in desk, or waiting area.
     + 1. The location must make its notice available to any person who asks for it, whether or not they are.

seeking services being offered by the organization at each location as a “covered entity”.

* + - 1. The location must prominently post and make available its notice on its web site (or corporate website) and provide a method to receive a paper copy of the Privacy Notice.
      2. The location may e-mail the notice to a patient or their representative if the individual agrees to receive an electronic notice; however, a paper copy shall always be made available.
      3. The location may provide the Notice by e-mail if the individual agrees to receive electronic Notice. If the email transmission has failed, each location must provide a paper copy.
      4. If the first delivery of the Notice to an individual is electronic the location must provide electronic “Notice” automatically and contemporaneously in response to the individual's first request for service.
      5. In an emergency, the location will provide the Notice as soon as it is reasonably available after the emergency situation has subsided and, relief efforts if required, have restored the location’s operations to normal operating conditions.

### Privacy Notice Requirements

* + - 1. CSM Team will provide a Notice that is written in plain language on how each location may use and disclose Protected Health Information (PHI).
      2. The Notice must contain this statement as a header: “***THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY***.”
      3. The patient rights with respect to the information and how the individual may exercise these rights, including how the individual may ask questions regarding the Privacy Notice or file complaints on

each location’s use of the patients’ (PHI).

* + - 1. The covered entity’s legal duties with respect to the information, including a statement that the covered entity is required by law to maintain the privacy of protected health information.
      2. A description and at least one example of the types of uses and disclosures that the organization at the location is permitted to make for treatment, payment, and health care operations.
      3. A description of each of the other purposes at each location is permitted or required to use or disclose PHI without the individual's written consent.
      4. If a use or disclosure is prohibited or materially limited by other laws, the description of such use/disclosure must be reflected in the notice.
      5. The description and examples must include sufficient detail to put the individual on notice of the uses and disclosures that are permitted or required by the privacy regulations and other applicable laws.
      6. A statement that other uses and disclosures may be made only with the patient or their representative’s written authorization and that the individual may revoke such authorization.
      7. A statement that the organization is required by law to maintain the privacy of PHI and to provide a patient or their representatives with notice of its legal duties and privacy practices.
      8. A statement that the organization is required to abide by the terms of the Notice currently in effect.
      9. A statement that the organization reserves the right to change the terms of its Notice and to make the new Notice provisions effective.
      10. A statement that describes how the organization will provide patents and their representatives with a revised Notice.
      11. The Notice will contain a statement that individuals may complain to the organization at the location and to the Secretary of the Department of Health and Human Services if they believe their privacy rights have been violated. This statement will include how the individual may file a complaint with the organization and that the individual will not be retaliated against for filing a complaint.
      12. The Notice must contain the name or title and telephone number of a person or office to contact for further information.
      13. The Notice must include the date with which the Notice is first in effect, which may not be earlier than the date on which the Notice is printed or otherwise published.
      14. The organization will state in the Notice that it reserves the right to revise or change its policies and procedures and that the revision may or may not affect all PHI, including previously obtained PHI that the organization at the location it maintains.
      15. When there is a change in the law that necessitates a revision to the organization’s policies and procedures, each location must promptly document and implement the change to include revisions to the Notice to reflect the change in the law.
      16. The organization may change its policy at any time; however, implementation cannot begin until the notice has been revised and posted. The date of implementation will be on or after the effective date stated in the Notice.
      17. The organization at the location is required to promptly revise and distribute its notice whenever it makes material changes to any of its privacy practices, and the notice must include an effective date.

### Notice Requiring Separate Statements

The Notice must include separate statements if the location plans to engage in any of the following:

* + - 1. The organization at the location may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits or services that may be of interest to the individual.
      2. The organization at the location may contact the individual to raise funds for the organization.

### Notice of Individual Rights

* + - 1. The Notice must contain a statement of the individual's rights with respect to PHI and a brief description of how the individual may exercise these rights.
      2. The right to request restrictions on certain uses and disclosures of PHI, including a statement that the organization at the location is not required to agree to a requested restriction.
      3. The right to receive confidential communication of PHI.
      4. The right to inspect and copy PHI.
      5. The right to request an amendment to PHI.
      6. The right to receive an accounting of disclosures of PHI.
      7. The right to receive a paper copy of the Notice.

### Notice Revisions

* + - 1. The organization at the location will retain copies of the Notice (original and revisions), written acknowledgments of receipt, and documentation of good faith efforts.
      2. The organization at the location will retain documentation for six (6) years from the last date in effect.

### References

Title 45 C.F.R. §164.520

## Permitted Disclosures

### Introduction

CSM Team is required to maintain the privacy of Protected Health Information (PHI) and to provide patients and their representatives how their PHI may be used and disclosed. The uses and disclosures of PHI by the Covered entity may include identifying information about past, present and future physical and mental health or conditions, and the provision of healthcare goods and services or payments for these goods and services. There are uses and disclosures that require prior authorization from the patient, caregiver, or a patient’s representative, as well as uses and disclosures that do not require prior authorization.

The uses and disclosures are subject to change and will be made available in electronic and paper format, at the Covered Entity where services are rendered, on the official website or upon request. The uses and disclosures of PHI shall be maintained in the CSM Team official Privacy Notice as required under HIPAA laws and regulations.

Some types of PHI, such as HIV information, genetic information, alcohol and/or substance abuse records, and mental health records may be subject to special confidentiality protections under applicable state or federal law and CSM Team will abide by all applicable protections. Additional information will be made available by contacting the Compliance Officer for location-specific questions and information.

### Scope

This policy covers all Workforce Members, business associates, and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team In the event it is not clear if this policy applies to you, please contact the Compliance Officer or designee.

### The Privacy Rule and Notification Rule Consent and Authorization

* 1. CSM Team is subject to the medical information privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA).
  2. The Privacy Rule permits but does not require, the CSM Team to voluntarily to obtain patient consent for uses and disclosures of protected health information for treatment, payment, and health care operations.
  3. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization. An authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual.

1.4 In situations where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of PHI unless it also satisfies the requirements of a valid authorization. An authorization must provide recorded in a detailed document that gives the CSM Team permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual.

### Permitted Uses and Disclosures of Protected Health Information (PHI)

* + - 1. CSM Team can use PHI for the treatment, payment, or health care operations, as permitted by and in compliance with § 164.506. The term “uses” and “disclosures” within the context of this section are interchangeable and are defined as “disclosures.”
      2. CSM Team may disclose PHI related to a patient’s treatment which may include the provision, coordination, or management of health care and related services (including coordination and management by a provider with a third party; consultation between health care providers relating to a patient; or referral of a patient for health care from one provider to another). In the covered entity setting, this may include a discussion regarding a patient with a provider or a clinician for consultations prevention of medication reactions, and patient medication and health history.
      3. CSM Team may disclose PHI to secure payment or provide information to health plans associated with a patient’s benefits. This includes, but is not limited to, activities related to coverage and eligibility determinations, billings, claims management, collections, review of services related to medical necessity or justification for charges, UR activities, and certain disclosures (e.g., name, address, DOB, account number) to consumer reporting agencies.
      4. CSM Team may disclose PHI during business operations. Operations are defined as necessary activities to conduct quality assessments and improvement activities, including contacting patients and health care providers with information about treatment alternatives. CSM Team may use and disclose medical information to assess the use or effectiveness of certain medications, develop and monitor medical protocols, and provide medication reminders within the permissible limits of the Privacy Rule.
      5. Privacy principles do not prohibit incidental disclosure of patient information so long as reasonable safeguards are taken to minimize the disclosure. Reasonable safeguards include:
         1. Avoiding conversations that include PHI in front of other patients.
         2. Lowering voices when discussing patient information in person over the phone.
         3. Avoiding conversations about patients in public places, such as outside of the covered entity area, front desk, and walkways.
      6. Conversations discussing PHI should be conducted in a private area or room, especially when discussions involve highly confidential information (i.e., Mental Illness or Developmental Disability, HIV/AIDS Testing or Treatment, Communicable Diseases, Venereal Disease(s), Substance (i.e., alcohol, drugs) Abuse, Abuse of an Adult with a Disability, Sexual Assault, Child Abuse and Neglect, Genetic Testing, Artificial Insemination, and Domestic Violence).
      7. If a workforce member overhears other workforce members or business associates discussing PHI inappropriately, it is acceptable to request that person “Breaching HIPAA Rules” abide by the Privacy Rule or report it to their immediate supervisor.

## Mandatory Disclosures

### Introduction

A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual’s protected health information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or

1. as the individual who is the subject of the information (or the individual’s personal representative) authorizes in

writing.

CSM Team is a covered entity and must disclose Protected Health Information (PHI) in two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and (b) to the U.S. Department of Health and Human Services (HHS) official for the purpose of an investigation, review, or enforcement action.

There are certain situations that involve other organizations, such as the military, law enforcement, the judicial system, and others, where disclosure of PHI is required due to an investigation or other permitted use under the Privacy Rule that takes precedence over an individual’s right to privacy under HIPAA.

When a workforce member has requested PHI due to a mandatory disclosure requirement under HIPAA, it does not prevent the workforce member from requiring certain information and verification that the “authority” requesting access to PHI. In the event that a workforce member receives a request for a mandatory request of PHI, they must notify their immediate supervisor or the Compliance Officer.

### Scope

This policy covers all Workforce Members, business associates, and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team In the event it is not clear if this policy applies to you, please contact the Compliance Officer.

### Mandatory Disclosures

* + 1. In the event of a request for an official Mandatory Disclosure of Protected Health Information (PHI), the following procedures must be followed.
    2. The workforce member is to tell the requestor that the workforce member is required to notify the Compliance Officer and will need to go through a brief process prior to the release of requested records.
    3. In the event that the request is made in person, the workforce member is to immediately notify the Compliance Officer.
  1. In the event that the Compliance Officer is not immediately available, the workforce member will notify and engage the on-duty manager or supervisor. The manager or supervisor must step in and take over the conversation with the requestor.
  2. The on-duty manager or supervisor will politely ask the requestor to wait momentarily while the on-duty manager or supervisor notifies the Compliance Officer.
  3. If the Compliance Officer is not available, a designee, manager, or supervisor may comply with the request, providing the designee, manager, or supervisor has been specifically trained on this policy and collects all the pertinent identification from the requestor and a signed release form.
  4. If the requestor appears in person, verify that the person is an “Official” that is listed in this policy.
  5. Using the Mandatory Disclosure Form (located in Appendix C – HIPAA Forms). Make certain to gather all required information, including name, badge number, or other agency identification, credentials, or proof of government status.
  6. Request to make a photocopy of the “Official Request” and the identification of the requestor, by taking a photocopy of their identification and writing down their name and identification number on the printed copy, sign, and date the copy.
  7. In the event that there is not a written “Official Request,” the requestor must fill out the section of the form as to the reason for the request, the name of the person whose records are being requested, the record being requested, and any other pertinent information.
  8. The release of copies or information must be specific, such as “medical record, prescription records, personal identification information, or another document/information.” The information that is.

requested is “***ONLY***” the minimum amount of information necessary is to be released for the stated purpose.

* 1. If a Law Enforcement Officer or other government official requests to speak with the patient, access is subject to the Compliance Officer’s or designee’s opinion that such access would not impede the patient’s care.
  2. Upon approval by the Compliance Officer or designee, the patient must be asked whether he/she wants to speak to government officials. The patient is not required to talk to the official, and CSM Team will respect the patient’s wishes. This applies even if the patient is an alleged perpetrator of a crime.

Mental health, HIV/AIDS, and genetic information may not be disclosed without the written consent of the patient or his/her legal representative.

### Judicial & Administrative Proceedings

* + 1. The Compliance Officer or designee may disclose protected health information in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized) or in certain conditions in response to a subpoena, discovery request or another lawful process.
    2. All requests of this type must be submitted to the Compliance Officer, who will inform the CSM Team legal counsel, prior to fulfilling these requests.

### Law Enforcement

* 1. In the event that a member of law enforcement requests PHI, the Compliance Officer or designee may release PHI under the following circumstance.
     1. In response to a court order, subpoena, warrant, summons, or similar process.
     2. To identify or locate a suspect, fugitive, material witness or missing person.
     3. To identify the victim of a crime, even if unable to obtain the victims’ authorization.
     4. To identify persons or facts regarding a death that is being investigated as a result of criminal conduct.
     5. This list is not meant to be all-inclusive, and the Compliance Officer shall use good judgment when responding to all requests for PHI from law enforcement officials.

### Report of Abuse, Neglect or Domestic Violence

* 1. The Compliance Officer or designee may release PHI protected health information to a public health authority that is permitted by law to receive reports of child abuse or neglect and to notify the appropriate government authority if the Compliance Officer or designee believes the individual has been the victim of abuse, neglect, or domestic violence. Such disclosures will only be made when required or authorized by law.
  2. Workforce Members are to report any suspicious activity that appears to involve abuse, neglect, or domestic violence immediately to the supervisor.

### Public Health Authorities

* + 1. Disclosures of PHI may be released to Public Health Authorities by the Compliance Officer or designee for the following types of public health concerns or emergency management.
       1. To prevent or control disease, injury, or disability.
       2. To report reactions to medications or problems with products.
       3. To notify people of recalls of products they may be using, and to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition.
       4. To avert a serious threat to health or safety.
       5. To prevent or lessen a serious and imminent threat to the health or safety of a person or the public. Any disclosure would be to someone who is able to help prevent the threat.
       6. In response to a natural or man-made disaster, where PHI is needed to provide the appropriate care for affected individuals.

### The Military and Homeland Security

* + 1. Military officials may request PHI for members of the military and for other national security purposes. All such requests must be handled by the Compliance Officer.
    2. PHI may be requested by military or Homeland Security for local or national security and intelligence purposes authorized by the National Security Act, and for protective services of the President and for certain military functions related to federal military personnel as required by military command authorities.
    3. The Compliance Officer will have to use discretion and is advised to seek assistance from CSM Team legal counsel for the release of PHI about foreign military personnel to the appropriate foreign military authority.

## Disclosure to Personal Representative

### Introduction

CSM Team recognizes the rights of patients to appoint a personal representative to inspect and receive a copy of Protected Health Information. A personal representative can be identified as a person who can make healthcare decisions for the patient using a power of attorney or other means that may be determined by state laws and the actions of the patient. An affirmative action taken by a patient in the absence of a power of attorney may include allowing a person who is accompanying the patient, who, by the patients’ actions, allows the personal representative to make healthcare decisions for the patient.

The Workforce Member should not attempt to decide on the patient and personal representative relationship in terms of the release of PHI. In order for a person or other entity to be deemed a “personal representative,” the patient must verbally state this in the presence of the Compliance Officer, or designee, or in writing,

All requests by a patient (or his or her Personal Representative) to access his or her PHI other than a review of CSM Team services, shall be submitted in writing, on the “Form- Request for Access,” and delivered to the Compliance Officer for evaluation and response no later than thirty (30) days after CSM Team receives the request. Unless the patient’s request is denied, CSM Team will: (a) arrange for patient’s access to PHI at a convenient time and place, or (b) provide a copy of the PHI in accordance with the patient’s request following payment of the Preparation Costs. If the patient’s request is denied, the Compliance Officer must provide a written explanation to the patient on CSM Team “Form- Response to Request for Access”.

The personal representative of a minor child is usually the child’s parent or legal guardian. State laws may affect guardianship. In cases where a custody decree exists, the personal representative is the parent(s) who can make health care decisions for the child under the custody decree. The Compliance Officer must be advised of any situation when the representative of a minor child is in question.

In cases when of patient death, the personal representative for the deceased is the executor or administrator of the deceased individual’s estate or the person who is legally authorized by a court or by state law to act on the behalf of the deceased individual or his or her estate. All requests for records of descendants must be directed to the Compliance Officer.

### Scope

This policy covers all Workforce Members, business associates, and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team In the event it is not clear if this policy applies to you, please contact the Compliance Officer or designee. In some cases, legal counsel must be consulted by the Compliance Officer prior to fulfilling a request for PHI through a personal representative.

### Process for Patient Rights to be Granted to a Personal Representative

* 1. CSM Team shall acknowledge Personal Representatives for patients regarding the access and release of PHI that have submitted any of the following documentation: court order, guardianship, notarized and authenticated statement granting such rights, or approval of a Personal Representative by submission of a “Personal Representative” application (Form PR-100) that is approved by the Compliance Officer, prior to the release of PHI in any form.
  2. The Compliance Officer or designee may, in their own judgment, release certain PHI deemed to be helpful in the care of the patient, to prevent harm and potential drug interactions, or other safety considerations, based on their professional and objective judgment. Workforce Member requires authorization from the Compliance Officer or designee prior to a release of PHI under these circumstances.

### Personal Representatives Rights to Protected Health Information (PHI)

* 1. Access to their own information, consistent with certain limitations.
  2. An accounting of disclosures that CSM Team has made throughout the duration of time that such information is available, subject to availability and other limitations.
  3. All requests shall be provided on the “Form-Request for Accounting” and delivered to the Compliance Officer for evaluation and response within sixty (60) days.
  4. The accounting period cannot be more than six (6) years prior to the date of the request.
  5. An accounting does not have to include any disclosure that CSM Team is not required to document.
  6. The Representative may request that CSM Team restrict the uses and disclosure of PHI, which shall be granted on an individual basis by the Compliance Officer.
  7. CSM Team shall accommodate reasonable requests by clients or participants or their personal representatives to receive communications by alternative means, such as by mail, e-mail, fax, or telephone; and should accommodate reasonable requests by clients or participants or their personal representatives to receive communications at an alternative location.
  8. CSM Team may deny access to sensitive health information or health services that must be handled with strict confidentiality under State laws. CSM Team will comply with the more restrictive requirements.
  9. All such requests are subject to review by the Compliance Officer.

### Denial of Access to Protected Health Information

* 1. CSM Team may deny clients or participants or their personal representatives, with reasons in writing, access to their own health information if Federal or State law prohibits the disclosure.
  2. Under Federal law, clients or participants have the right to access, inspect, and obtain copies of health information on their own cases in CSM Team files or records except for:
     1. Psychotherapy notes; Information compiled for use in civil, criminal, or administrative proceedings; Information that is subject to the Federal Clinical Labs Improvement Amendments of 1988, or exempt pursuant to 42 CFR 493.3(a)(2); Information that, in good faith and using professional judgment, the Compliance Officer or Designee believes could cause harm to the client, participant or to any other person; Documents protected by attorney work-product privilege and Information where release is prohibited by State or Federal laws.
  3. CSM Team may deny, with reasons in writing, a request for access made by the

client’s or participant’s personal representative for any of the grounds stated above, or if, in good faith and using professional judgment, the Compliance Officer believes that disclosure of such information to the personal representative or to any other person to whom the client or participant has authorized disclosure could cause harm to the client, participant or to any other person, or that the requestor has caused or may cause harm to the client or participant or any other person.

* 1. All requests shall be provided on the “Form-Request for Accounting” and delivered to the Compliance Officer for evaluation and response within sixty (60) days. The accounting period cannot be more than six (6) years prior to the date of the request. An accounting does not have to include any disclosure that CSM Team is not required to document.
  2. Prior to denial of a request by a patient or a personal representative or anyone else disclosure or access to PHI because there is a good faith belief that disclosure or access could cause harm to the client or participant or to another person, the decision to deny must be made by a licensed health care professional with reasons in writing and DHH must make a review of this denial available to the client/participant and/or requestor. If the requestor wishes to have this denial reviewed, the review must be done by a licensed health care professional who was not involved in the original decision.

#### Reference(s):

45 CFR Part l64.522-164.

# Section III – Business Associates

## Business Associates Overview

### Introduction

The Privacy Rule allows covered providers and health plans to disclose protected health information to these “business associates” if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the CSM Team will safeguard the information from misuse and will help the CSM Team comply with the Privacy Rule. Covered entities may disclose protected health information to an entity in its role as a business associate only to help the CSM Team carry out its health care functions – not for the business associate’s independent use or purposes, except as needed for the proper management and administration of the business associate.

A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of or provides services to CSM Team. A member of the CSM Team workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of CSM Team the Privacy Rule lists some of the functions or activities, as well as the services that make a person or entity a business associate if the activity or service involves the use or disclosure of protected health information. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

Business associate functions and activities include claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate services are legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial. This list is not meant to be exhaustive, and the “business associate” is defined within the context of 45 CFR 160.103.

A CSM Team contract or other written arrangement with its business associate must contain the elements specified at 45 CFR 164.504(e). For example, the contract must: Describe the permitted and required uses of protected health information by the business associate; Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law and require the business associate to use appropriate safeguards to prevent use or disclosure of the protected health information other than as provided for by the contract.

Whenever CSM Team knows of a material breach or violation by the business associate of the contract or agreement, the CSM Team is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a CSM Team is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).

Introduction

The practical application for determining the need for business associate agreements is based on the possession or processing of PHI on behalf of the CSM Team for which the business associate has the same duty to protect the security and integrity of all CSM Team PHI that it receives, stores, or transmits.

Scope

All CSM Team Workforce Members shall be responsible for protecting PHI from unauthorized access, use, or disclosure. Except as authorized by the Compliance Officer, no interference with the storage of PHI or any hardware, software, or procedural mechanism that records or examines the activity of electronic PHI (“EPHI”) in CSM Team information system shall be permitted.

This policy covers all Workforce Members, business associates, and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team In the event it is not clear if this policy applies to you, please contact the Compliance Officer.

### Identification of Business Associates

* 1. "Business associate" is defined as a person or entity that is not part of the CSM Team covered workforce and performs certain functions on behalf of CSM Team that involve the use or disclosure of the CSM Team Protected Health Information (PHI), including uses for purposes related to payment and/or healthcare operations.
  2. Business associates functions or activities include claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or any other function or activity regulated by the Privacy Rule; or legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the CSM Team™, or to or for an organized health care arrangement in which the CSM Team participates.
  3. Business associates do not include an employee of CSM Team or other Workforce Members who disclose Protected Health Information for treatment purposes; or any other individuals that the CSM Team considers being members of its covered workforce; or individuals who may obtain incidental disclosures of Protected Health Information, where access to Protected Health Information is minimal, if at all, and where the receipt of such Protected Health Information is not part of the individual's job duties for CSM Team
  4. The Compliance Officer shall provide guidance in determining whether or not a contracting business activity meets the requirements for a business associate agreement.
  5. In the event that the Compliance Officer is unable to make the determination as to whether or not the activities and responsibilities of a contracted service require a business associates’ agreement, the Compliance Officer shall seek legal opinion for written guidance.

### Business Associates Agreement Execution

### Individuals or entities determined to be business associates of CSM Team must execute a business associate agreement.

### CSM Team provides a business associate agreement template for this purpose, which can be found in Appendix C – HIPAA Forms.

### If a business associate provides a business associate agreement for this purpose, it must be equivalent to the terms and conditions of the CSM Team business associate agreement.

### If a dispute or issues arise from using CSM Team business associate agreement, the Compliance Officer shall be immediately notified.

### A business associate agreement may be executed only by the designated official of CSM Team with oversight provided by the Compliance Officer.

### Sanctions

### Workforce Members that are not authorized to enter into a contractual agreement(s) on behalf of the CSM Team are subject to disciplinary action, up to and including termination of employment or assignment.

* 1. Business associates found to be in violation of policies or laws regarding fulfilling the terms and conditions of the business associate agreement are subject to cancellation of service agreement and may be reported if found to be in violation of HIPAA laws to the appropriate authorities.

# Section IV – Security Rule

## HIPAA Security Rule Basics

### Introduction

The security standards are divided into the categories of administrative, physical, and technical safeguards as noted in the Security Rule 45 CFR §164.304.

**Administrative Safeguards include** Security Management Processes, assigned security responsibilities, workforce security, information access management, security awareness and training, security incident procedures, contingency planning, evaluation, and business associate agreements and other related contact management.

**Physical safeguards include** facility access controls, workstation use, workstation security, and device and media controls.

**Technical Safeguards include** access control, audit controls, integrity, person or entity authentication, and transmission security.

When the **final Security Rule** was published, the security standards were designed to be “technology-neutral” to accommodate changes. The rule does not prescribe the use of specific technologies so that the health care community will not be bound by specific systems and/or software that may become obsolete. HHS also recognizes that the security needs of covered entities can vary significantly. This flexibility within the rule enables each entity to choose technologies to best meet its specific needs and comply with the standards.

The first standard under the Administrative Safeguards section is the Security Management Process. This standard requires covered entities to: “***Implement policies and procedures to prevent, detect, contain and correct security violations***.” The purpose of this standard is to establish the administrative processes and procedures that a covered entity will use to implement the security program in its environment. There are four implementation specifications in the Security Management Process standard.

Risk Analysis (Required) § 164.308(a)(1)(ii)(A): The Risk Analysis implementation specification requires covered entities to: “***Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronically protected health information held by the covered entity***.”

Risk Management (Required) § 164.308(a)(1)(ii)(B): Risk Management is a required implementation specification. It requires an organization to make decisions about how to address security risks and vulnerabilities. The Risk Management implementation specification states that covered entities must: “***Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a***).”

Sanction Policy (Required) § 164.308(a)(1)(ii)(C) Another implementation specification in the Security Management Process is the Sanction Policy. It requires covered entities to: “Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.” Appropriate sanctions must be in place, so workforce members understand the consequences of failing to comply with security policies and procedures to deter noncompliance.

Information System Activity Review (Required) § 164.308(a)(1)(ii)(D) The Security Management Process standard also includes the Information System Activity Review implementation specification. This required implementation specification states that covered entities must: “**Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports**.”

In the following policies of the Security Rule Section, there are many straightforward actions that Workforce Members accomplish on a daily basis to assist the organization with maintaining the security of Protected Health Information (PHI) and the systems that are used for access, storage, and transmission of PHI data. It is important that Workforce members take personal responsibility to ensure that the organization is not left venerable by logging off or shutting down workstations, protecting passwords, and reporting any unusual activity to the Compliance Officer.

There are also many technical standards that workforce members may not have sufficient experience to manage, such as making sure that security software updates are made on a timely basis or that audits are completed on the security systems used to protect the PHI data. Workforce Members are encouraged to ask questions and work with their supervisors and the Compliance Officer to create a culture of security to protect the integrity of the PHI we are entrusted with by our patients.

CSM Team must not rely solely on security systems provided by others such as providers, hospitals, payers, and other covered entities for which the CSM Team receives or transmits PHI to meet the requirements of the Security Rule. CSM Team must implement and maintain security measures to ensure the integrity of the systems used by the CSM Team and for those in which the CSM Team interacts through to maintain compliance with the Security Rule.

### Scope

This policy covers all Workforce Members, business associates, and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team. This policy provides the framework for Section IV – the Security Rule. In the event it is not clear if this policy applies to you, please contact the Compliance Officer or designee.

### Administrative Safeguards

* 1. CSM Team is subject to the Security Rule provisions of the Health Insurance Portability and Accountability Act (HIPAA).
  2. CSM Team must maintain administrative safeguards that require actionable policies and procedures to take appropriate and timely administrative actions, and to prevent, detect, contain, and correct security violations.
  3. Administrative safeguards must involve the selection, development, implementation, and maintenance of security measures to protect PHI and to manage the conduct of Workforce Members in relation to the protection of that information.
  4. A central requirement is that you perform a security risk analysis that identifies and analyzes risks to PHI and then implements security measures to reduce the identified risks.
  5. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization. An authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual.

### Physical Safeguards

### Safeguards are physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

* 1. CSM Team must limit physical access to its facilities while ensuring that authorized access is allowed.
  2. CSM Team must implement policies and procedures to specify the proper use of and access to workstations and electronic media.
  3. CSM Team must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronically protected health information (e-PHI).

### Technology Safeguards

### CSM Team must implement technical policies and procedures that allow only authorized persons to access electronically protected health information (e-PHI).

* 1. CSM Team must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e- PHI.
  2. CSM Team must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed, which includes electronic measures.
  3. CSM Team must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

1. Organizational Standards
   1. CSM Team is required to comply with every Security Rule "Standard." However, the Security Rule categorizes certain implementation specifications within those standards as "addressable," while others are "required."
   2. The "required" implementation specifications must be implemented. The "addressable" designation does not mean that an implementation specification is optional.
   3. CSM Team is permitted to determine whether the addressable implementation specification is reasonable and appropriate. If it is not, the Security Rule allows CSM Team to adopt an alternative measure that achieves the purpose of the standard if the alternative measure is reasonable and appropriate.
   4. The Compliance Officer must maintain Organizational Standards for the Security Rule through policies and procedures, ongoing risk analysis, implementation and maintenance of accessibility guidelines and rules, and enlistment of the necessary resources to ensure compliance with the Security Rule. Lack of resources is an unacceptable cause of a PHI breach or security vulnerability.
   5. The Security Rule standards require CSM Team to have contracts or other arrangements with business associates that will have access to the CSM Team phi.
   6. The standards provide the specific criteria required for written contracts or other arrangements that involve business associates (BA) and PHI that is transmitted, stored, disposed of, or accessed between the BA and the CSM Team.
   7. If CSM Team knows or becomes aware of an activity or practice of the business associate that constitutes a material breach or violation of the business associate’s obligation, the Compliance Officer must take reasonable steps to cure the breach or end the violation.
   8. Violations include the failure of business associates to implement safeguards that reasonably and appropriately protect e-PHI.
   9. The Compliance Officer is to maintain ongoing knowledge of the Security Rule and the Department of Health and Human Services national standards for confidentiality, integrity, and availability of e-PHI.
   10. The Department of Health and Human Services (HHS), Office for Civil Rights (OCR) is responsible for administering and enforcing these standards, in concert with its enforcement of the Privacy Rule, and may conduct complaint investigations and compliance reviews.

### Policies and Procedures

* + - 1. CSM Team is required to adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule.
      2. CSM Team must maintain, until six years after the date of their creation or last effective date (whichever is later), written security policies and procedures and written records of required actions, activities, or assessments.
      3. The CSM Team Compliance Officer must periodically review and update its documentation in response to environmental or organizational changes that affect the security of PHI and approve all changes to the written policies regarding the Security Rule and provide the necessary updates and training to Workforce Members.
      4. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization. An authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual.

### Risk Analysis

* 1. CSM Team must ensure that the Compliance Officer has sufficient knowledge and access to tools and resources (internal and/or external) for conducting an ongoing risk analysis.
  2. The risk analysis must include information systems that include hardware, software, information, data, applications, communications, and people (Workforce Members and business associates).
  3. The risk analysis process includes, but is not limited to, the following activities: evaluate the likelihood and impact of potential risks to e-PHI; Implement appropriate security measures to address the risks identified in the risk analysis; document the chosen security measures and, where required, the rationale for adopting those measures; and maintain continuous, reasonable, and appropriate security protections.
  4. The risk analysis must be completed on an annual basis, and it is highly recommended that periodic reviews of the effectiveness of the policies and procedures based on feedback from ongoing monitoring efforts.

### State Guidelines

* 1. States have additional guidelines for E-Prescribing that CSM Team must incorporate into the Security Rule policies. See QC-3 HIPAA State Guidelines (subject to change without notice).

### Sources

U.S. Department of Health and Human Services, Summary of the HIPAA Rule (Last Reviewed on June 16, 2017).

The Office of the National Coordinator for Health Information Technology, Guide to Privacy and Security of Electronic Health Information.

## Administrative Safeguards

### Introduction

All covered entity personnel shall be responsible for protecting PHI from unauthorized access, use, or disclosure. Except as authorized by the Compliance Officer or designee, no interference with the storage of PHI or any hardware, software, or procedural mechanism that records or examines the activity of electronic PHI (“EPHI”) in the covered entity’s information system shall be permitted.

### Scope

This policy covers all Workforce Members, business associates, and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team In the event it is not clear if this policy applies to you, please contact the Compliance Officer.

### Security Management Processes

* + - 1. The Compliance Officer shall maintain and update the security management processes to be proactive and respond to any changes in the information technology environment that poses a threat to the security and integrity of Protect Health Information (PHI) and the systems that are used to store, transmit, receive, visualize or dispose of PHI.
      2. Shall identify and deploy resources sufficient to support the Compliance Officer to carry out these duties in a timely manner.
      3. In collaboration with the Compliance Officer, assign security responsibilities to the appropriate staff or qualified outside vendor(s).
         1. Qualified vendors must be willing and capable of entering into a business associate agreement as applicable and have the necessary resources to complete assigned responsibilities in accordance with HIPAA rules.
      4. Shall have the final approval for the policies and procedures for HIPAA-compliance.
      5. Shall maintain signature authority for entering into service agreements with business associates with input from the Compliance Officer.
      6. Shall employ or contract with individuals or companies that have sufficient knowledge and resources to assemble and maintain a high-security data system, with a major emphasis on security, malware and virus protection and access controls.

### Security Management Processes Continued.

* + - 1. The Compliance Officer shall create, review, and update policies relating to HIPAA privacy and security on an ongoing basis, along with tools and methods to periodically test the effectiveness of the policies and the technology security.
      2. The Compliance Officer shall ensure that workforce members are properly training prior to having access to PHI or systems that contain PHI.
      3. The Compliance Officer or designee shall assign usernames and passwords to all staff that require access to covered entity information systems.
      4. The Compliance Officer shall maintain policies and processes on control of paper documents to ensure that workforce members are diligent in their producing, handling, utilizing, transporting, and disposing of PHI properly.
      5. The Compliance Officer shall establish and maintain security incident procedures to include notifications to affected individuals, the media, and the Secretary of HHS in the event of a Breach.
      6. The Compliance Officer shall review all business associate agreements and assign verification of liability insurance.
      7. The Compliance Officer shall make periodic reviews of business associates’ compliance with security standards through direct observation, audit, or annual performance review.
      8. The Compliance Officer shall conduct risk assessments for emergency planning and contingency planning in collaboration with key Workforce Members and community resources as appropriate. The risk assessment shall be completed on no less than an annual basis, to include updating of contingency plans.

## Physical Safeguards

### Introduction

The Security Rule defines Physical safeguards are physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. The standards under physical safeguards include facility access controls, workstation use, workstation security, and device and media controls. The Security Rule requires covered entities to implement physical safeguard standards for their electronic information systems, whether such systems are housed on the covered entity’s premises or at another location.

### Scope

All CSM Team Workforce Members shall be responsible for protecting PHI from unauthorized access, use, or disclosure. Except as authorized by the Compliance Officer, no interference with the storage of PHI or any hardware, software, or procedural mechanism that records or examines the activity of electronic PHI (“EPHI”) in CSM Team information system shall be permitted.

This policy covers all Workforce Members, business associates, and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team In the event it is not clear if this policy applies to you, please contact the Compliance Officer.

### Physical Safeguards

* + - 1. CSM Team shall designate specific Workforce Members and/or business associates that are responsible for installing and maintaining physical safeguards.
      2. All Workforce Members and business associates shall take appropriate measures to apply physical safeguards to their work area and electronic devices to avoid unauthorized access to PHI and data systems.
      3. Physical safeguards of PHI include protecting PHI from accidental or intentional unauthorized use or disclosure, which includes safeguarding sensitive information, usernames, passwords, updated security software, safe browsing habits, securing desktop and mobile devices, use of screen savers, protection against theft of devices in public areas, and security of servers and data transmission routes.
      4. Physical access includes limiting accidental disclosures such as discussion in open areas, leaving PHI in plain view, or discussing PHI with patients and their authorized representatives in close proximity to others.
      5. Physical safeguards must include physical access controls to areas where PHI is stored or in use, by keeping doors, cabinets, windows, and other access points locked and protected from unauthorized entry.

### Facility Access Controls

* + - 1. CSM Team shall provide warning signs of restricted areas in plain view of the general public.
      2. CSM Team shall provide surveillance cameras and security systems to record access to restricted areas and to notify law enforcement in the event of a beach in physical security.
      3. Workforce Members are to be identified with Identification Badges that are to be always worn while on CSM Team premises.
      4. Identification Badges that allow for access to restricted areas are to be secured by Workforce Member when not in use.
      5. Loss of Identification Badges is to be immediately reported to the Compliance Officer or designee.
      6. Business associates must be properly identified when accessing restricted areas.
      7. Workforce Members are to prevent access of business associates’ staff that cannot be properly identified from accessing restricted areas, which, if necessary, may include notification of the Compliance Officer or law enforcement.
      8. Business associates must be escorted when accessing restricted areas by an authorized Workforce Member.
      9. A written log or equivalent must be used to identify the date, time, person, and reason for access to restricted areas.
      10. The Compliance Officer or designee shall maintain a method of validating access controls to physical locations, data systems, and software programs.
      11. The Compliance Officer must have a method for maintaining a record of access to physical locations that use electronic badges, and for all electronic access to systems. Equipment and software where there are access to PHI or systems that store or transmit PHI.
      12. The Compliance Officer or designee shall have a method of immediately restricting access to electronic access to systems, equipment, and software where there is access to PHI or systems that store or transmit PHI.
      13. Repairs and updates to access controls must be documented in a log or equivalent, to include the date, time, person making the repair or update, and the reason for the repair or update.

### Workstations, Email, and Data Storage Accounts

* + - 1. A workstation is defined as “an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and has electronic media stored in its immediate environment.
      2. Workstations must have access controls such as passwords and/or authentication for access.
      3. Screen savers shall be used to automatically restrict access when systems or devices are not in use.
      4. All-access controls and restrictions apply to all workstations accessed outside of the CSM Team premises, such as remote access in any form or format.
      5. Remote access must be approved by the Compliance Officer or designee in advance of such access.
      6. Email and data storage accounts must be authorized for individual use by the Compliance Officer or designee.
      7. CSM Team email accounts shall not be used for personal business, auto-forwarded, or stored in cloud-based accounts (i.e., Google Drive or Dropbox) or external hard drives, without the expressed written permission of the Compliance Officer or designee.
      8. Passwords for email and authorized data storage accounts are to be kept private and not shared with others.
      9. In the event that password(s) is (are) compromised, the Compliance Officer or Designee is to be immediately notified.
      10. Passwords and access are to be immediately restricted upon suspension and voluntary or involuntary termination of employment or assignment.
      11. Single Sign-on (SSO) access must be approved by the Compliance Officer or designee.
      12. Passwords are not to be disclosed verbally or electronically with others.
      13. Sharing of password(s) with others is grounds for disciplinary action.
      14. Workforce Members must logoff of all devices when not in use.

### Loss of Data or Devices

* + - 1. Any loss of data, such as loss of external or internal hard drives, successful hacking attempts, physical loss of equipment and devices are to be immediately reported to the Compliance Officer or designee.
      2. A record that includes identification of all devices that provide and/or are authorized for use must be maintained by the Compliance Officer or designee.
      3. Records must be updated whenever there is an addition, loss, discontinuance, or disposal of data access and storage devices.
      4. Devises that are recycled or disposed of must be managed to remove all identifiable PHI and means of access according to Section V – Disposal policies and procedures.

### Sanctions

* + - 1. Workforce Members that do not follow policies for maintaining the security and integrity of physical safeguards are subject to disciplinary action, up to and including termination of employment or assignment.
      2. Business associates found to be in violation of physical safeguard policies and/or do not ensure the security and integrity of physical safeguards are subject to cancellation of service agreement and may be reported if found to be in violation of HIPAA laws to the appropriate authorities.

## Technical Safeguards

### Introduction

The Security Rule defines technical safeguards in § 164.304 as “the technology and the policy and procedures for its use that shield electronically protected health information and control access to it.” The Security Rule is based on the fundamental concepts of flexibility, scalability, and technology neutrality. Therefore, no specific requirements for types of technology to implement are identified. The Rule allows CSM Team to use any security measures that allow it reasonably and appropriately to implement the standards and implementation specifications. CSM Team must determine which security measures and specific technologies are reasonable and appropriate for implementation.

45 CFR § 164.306(b), the Security Standards: General Rules, Flexibility of Approach, provides key guidance for focusing compliance decisions, including factors a covered entity must consider when selecting security measures such as technology solutions. In addition, the results of the required risk analysis and risk management processes at §§ 164.308(a)(1)(ii)(A) & (B) will also assist the entity to make informed decisions regarding which security measures to implement. The Security Rule does not require specific technology solutions.

There are many technical security tools, products, and solutions that a covered entity may select. Determining which security measure to implement is a decision that CSM Team must make based on what is reasonable and appropriate for their specific organization, given their own unique characteristics, as specified in § 164.306(b) the Security Standards: General Rules, Flexibility of Approach. Some solutions may be costly, especially for smaller Pharmacies. While cost is a factor and CSM Team may consider when deciding on the implementation of a particular security measure; it is not the only factor. The Security Rule is clear that reasonable and appropriate security measures must be implemented, see 45 CFR 164.306(b), and that the General Requirements of § 164.306(a) must be met.

Access Control Standards include four specifications; Unique User Identification (Required), Emergency Access Procedure (Required), Automatic Logoff (Addressable), Encryption, and Decryption (Addressable).

### Scope

All CSM Team Workforce Members shall be responsible for protecting PHI from unauthorized access, use, or disclosure. Except as authorized by the Compliance Officer, no interference with the storage of PHI or any hardware, software, or procedural mechanism that records or examines the activity of electronic PHI (“EPHI”) in CSM Team information system shall be permitted.

This policy covers all Workforce Members, business associates, and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team In the event it is not clear if this policy applies to you, please contact the Compliance Officer.

### Unique User Identification

* 1. CSM Team shall designate a unique user identification name for Workforce Members and/or business associates that access systems and data.
  2. The username may include a first name, initials, last name, and a number or any combination thereof.
  3. The unique user identification shall be used to track specific activity when the user is logged into the CSM Team or business associate domain, and information systems.
  4. The password associated with the unique user identification shall not contain the name of the person, or easy to identify sequences of letters or numbers.
  5. The password shall contain, at a minimum, a capitalized letter, a number, and a symbol (if permitted).
  6. The password shall be challenging for hackers and unauthorized users to assist in preventing unauthorized access.

### Software and Hardware

* 1. All software and hardware purchases must receive pre-approval by the Compliance Officer or designee and must follow a consistent documented request process.
  2. Use of hardware and all other devices capable of receiving, storing, and transmitting PHI must receive prior approval and must follow a consistent documented request process.
  3. The use of personal electronic devices that have not received written authorization for use by the Compliance Officer or designee is strictly forbidden.
     1. The use of personal electronic devices without prior authorization may result in disciplinary action, up to and including termination of employment.
  4. The installation of unauthorized software is strictly forbidden.
     1. Only properly licensed, obtained, and approved software may be installed on computers that use, store, or come in contact with electronically protected health information (ePHI).
  5. Business associates must have safeguards, policies, and processes in place that meet the security standard requirements.
  6. Unauthorized duplication or distribution of CSM Team licensed software is strictly prohibited.

.

* 1. The Compliance Officer must approve the use of custom-built applications.

### Virus and Malware Protection

* 1. Workforce Members are required to avoid downloading from unknown sources as they may contain malicious software, social engineering acts and hoaxes are designed to disrupt computer systems, gather the information that leads to loss of privacy or exploitation, or gains unauthorized access to system resources.
  2. All CSM Team information systems, including servers, desktop computers, laptops, and other devices accessing the CSM Team information systems and databases must have an automated anti-malware management system. Disabling, altering, deleting, or preventing these programs or other security settings from updating is strictly prohibited.
  3. The deliberate creation, use, storage, distribution, and/or possession of malware is expressly prohibited. The intentional storage, distribution, and/or possession of malware may be construed as a failure to safeguard information systems.
  4. Removal of unauthorized software: Unauthorized, malicious or nuisance software can be installed on a computer without the knowledge of the user. If unauthorized software is discovered to be or suspected to be installed on any system, the Compliance Officer or designee must be contacted immediately.
  5. Workforce Members shall not use information systems to send unsolicited or bulk advertisements or commercial messages. Workforce Members Users shall take due care when opening suspicious or unexpected emails with attachments from unknown users. When uncertain, users shall contact the Compliance Officer or designee for assistance and/or guidance.
  6. Users of information systems must recognize and avoid social engineering links. Users should not engage in requested actions, whether that is a human or electronic request, without knowing the requested information and the person making the request. Workforce Members are required to inform the Compliance Officer or designee prior to acceptance.

.

* 1. The creation or forwarding of hoax messages is expressly prohibited. Workforce Members who receive virus-related warnings are required to inform the Compliance Officer or designee.
  2. System administrators may remove, with or without prior notification, any malicious or unauthorized software.

### Remote Access

* 1. Remote access requires prior approval of the Compliance Officer or designee.
  2. Remote access to information systems must be managed and protected by Workforce Members who are granted remote access.

### Emergency Access Procedures

* 1. CSM Team shall maintain a method to provide services during an emergency that limits or prevents access to information systems and/or devices.
     1. In the event that an emergency or disaster’s severity prevents access to vital data that is required for providing services to patients and their representatives, the on-duty manager shall seek guidance from the Compliance Officer (if available) and should use good and reasonable judgment for any services provided during an emergency or disaster.
     2. The on-duty manager or designee shall maintain a written record of all services provided during an emergency or disaster.
  2. In the event of an emergency that prevents access to systems and data, please refer to [Section VI – Disaster Preparedness and Response.](#_bookmark24)

### Automatic Logoff

* 1. CSM Team shall maintain an automatic logoff for all systems and devices used that stores or transmits PHI data.
  2. The Compliance Officer or designee shall determine the maximum amount of time for systems and devices to automatically logoff, which must not exceed fifteen (15) minutes to activate a timeout or open a secure screen that requires the user to log back in.

### Encryption and Decryption

* 1. Encryption is the process of transforming information using an algorithm to make data unreadable to anyone except those possessing special knowledge, often referred to as a key or password.
  2. CSM Team shall adhere to the U.S. National Institute of Standards and Technology for encryption and decryption data management.

### Sanctions

* 1. Workforce Members that do not follow policies for maintaining the security and integrity of physical safeguards are subject to disciplinary action, up to and including termination of employment or assignment.
  2. Business associates found to be in violation of physical safeguard policies and/or do not ensure the security and integrity of physical safeguards are subject to cancellation of service agreement and may be reported if found to be in violation of HIPAA laws to the appropriate authorities.

## Storage, Transportation, Transfer, and Transmission of PHI

### Introduction

In order to determine the technical security measures to implement and comply with this standard, CSM Team must review the current methods used to transmit EPHI. When EPHI is transmitted through email, over the Internet, or via some form of private or point-to-point network, CSM Team must identify the available and appropriate means to protect EPHI as it is stored, transported, transferred, or transmitted.

Paper documents are often scanned, faxed, or downloaded in electronic formats. CSM Team maintains paper documents and labels containing PHI that must be given the same security considerations.

### Scope

All CSM Team Workforce Members shall be responsible for protecting PHI from unauthorized access, use, or disclosure. Except as authorized by the Compliance Officer, no interference with the storage of PHI or any hardware, software, or procedural mechanism that records or examines the activity of electronic PHI (“EPHI”) in CSM Team information system shall be permitted.

This policy covers all Workforce Members, business associates, and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team In the event it is not clear if this policy applies to you, please contact the Compliance Officer.

This policy applies to Electronic Protected Health Information (ePHI) while the data is in transit over an electronic communications network and when the transmission is initiated by CSM Team All applications that transfer ePHI over an electronic communications network (e.g., email, file transfer, a web browser) are subject to this policy.

### Storage of Data (ePHI)

* + - 1. All software and hardware purchases must receive pre-approval by the Compliance Officer or designee and must follow a consistent documented request process.
      2. Use of hardware and all other devices capable of receiving, storing, and transmitting PHI must receive prior approval and must follow a consistent documented request process.
      3. The use of personal electronic devices that have not received written authorization for use by the Compliance Officer or designee is strictly forbidden.
      4. The use of personal electronic devices without prior authorization may result in disciplinary action, up to and including termination of employment.
      5. The installation of unauthorized software is strictly forbidden.
      6. Only properly licensed, obtained, and approved software may be installed on computers that use, store, or come in contact with Electronic Protected Health Information (ePHI).
      7. Business associates must have safeguards, policies, and processes in place that meet the security standard requirements.
      8. Unauthorized duplication or distribution of CSM Team licensed software is strictly prohibited.
      9. The Compliance Officer must approve the use of custom-built applications.

# Section V – Disposal and Destruction of PHI

## Disposal of Printed PHI

### Introduction

The HIPAA Privacy Rule requires that the appropriate administrative, technical, and physical safeguards be always in place and available to protect the privacy of protected health information (PHI) in any form, as stated in 45 CFR 164.530(c). CSM Team must implement reasonable safeguards to limit incidental and avoid prohibited uses and disclosures of PHI, including the disposal of such information. The HIPAA Security Rule requires CSM Team to implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of electronic PHI from electronic media before the media are made available for reuse per 45 CFR 164.310(d)(2)(I) and (ii). Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI and may result in significant HIPAA breaches subject to penalties and fines.

CSM Team must ensure that Workforce Members receive training on and follow the disposal policies and procedures of the CSM Team as necessary and appropriate for each workforce member as noted in 45 CFR 164.306(a)(4), 164.308(a)(5), and 164.530(b) and (i). Therefore, any workforce member involved in disposing of PHI, or who supervises others who dispose of PHI, must receive training on disposal. This includes any volunteers. See 45 CFR 160.103 (definition of “workforce”).

CSM Team is not permitted to simply abandon PHI or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons. However, the Privacy and Security Rules do not require a particular disposal method. CSM Team must review its own circumstances to determine what steps are reasonable to safeguard PHI through disposal and develop and implement policies and procedures to carry out those steps. In determining what is reasonable, the CSM Team should assess potential risks to patient privacy, as well as consider such issues as the form, type, and amount of PHI to be disposed. For instance, the disposal of certain types of PHI such as name, social security number, driver’s license number, debit or credit card number, diagnosis, treatment information, or other sensitive information may warrant more care due to the risk that inappropriate access to this information may result in identity theft, employment or other discrimination, or harm to an individual’s reputation.

In general, examples of proper disposal methods may include, but are not limited to:

For PHI in paper records, shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.

Maintaining labeled prescription bottles and other PHI in opaque bags in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.

For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

### Scope

All CSM Team Workforce Members shall be responsible for protecting PHI from unauthorized access, use, or disclosure. Except as authorized by the Compliance Officer, no interference with the storage of PHI or any hardware, software, or procedural mechanism that records or examines the activity of electronic PHI (“EPHI”) in the CSM Team health information system shall be permitted.

This policy covers all Workforce Members, business associates, and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team In the event it is not clear if this policy applies to you, please contact the Compliance Officer.

### Printed Protected Health Information (PHI)

* + - 1. Printed material which includes PHI may be found in the following documents, labels, or other printed media: patient encounter forms and labels, printouts from IS systems containing PHI, CSM Team notes, index cards or worksheets with patient’s information, photocopies of patient’s insurance cards, patient’s information on post-It notes, personal reminders, emails, memos, telephone call logs, and other written communications that contain PHI. This list is not meant to be all-inclusive.
      2. Documents that contain PHI, which is subject to retention requirements, should be managed carefully to not expose PHI while in use, storage, or transportation.
      3. Workforce Members are prohibited from destroying, altering, or discarding any information (with or without PHI), which may be subject to government investigations, audits, subpoenas, and search warrants. Standard document disposal policies and destruction procedures should be immediately suspended once there is a notification that the documents are part of a government investigation, or a subpoena or search warrant has been served.
      4. Printed materials containing PHI that are not subject to retention requirements, must be destroyed or de-identified by an approved method. It is strictly prohibited to discard PHI into wastebaskets, recycling bins, or other accessible locations or containers.
      5. Printed materials containing PHI that can be shredded or de-identified, must be kept in a locked container prior to transport and disposal.
      6. In the event that there is insufficient space or lockable containers available for storage prior to destruction or de-identification, the Compliance Officer or designee is to be contacted for a resolution, and the materials kept secure until the issue is resolved.

### De-Identification Standard and Methods

* + - 1. Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify an individual and if the CSM Team has no reasonable basis to believe it can be used to identify an individual.
      2. Sections 164.514(b) and(c) of the Privacy Rule contain the implementation specifications that a covered entity must follow to meet the de-identification standard.
      3. The Privacy Rule provides two methods by which health information can be designated as de-identified, which is Expert Determination and Safe Harbor.
      4. The Expert Determination method requires a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and (ii) Documents the methods and results of the analysis that justify such determination.
      5. The Safe Harbor Method requires that no parts or derivatives of any of the listed identifiers be disclosed in healthcare data. This method may be used by CSM Team through a third party, or a Workforce Member that has the expertise and equipment to complete this operation.
      6. The Compliance Officer must pre-approve any Workforce Member or outside company that is utilized for de-identification.
      7. In general, examples of proper disposal methods may include, but are not limited to:
      8. For PHI in paper records, shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
      9. Maintaining labeled prescription bottles and other PHI in opaque bags in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.
      10. For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

### Certificates of Destruction

* + - 1. All materials that contain PHI and are sent out to a contractor for disposal or de-identification, in bulk form, must be identified when destroyed with a Certificate of Destruction.
      2. Internal methods for destroying or de-identification of material that contain PHI must be approved by the Compliance Officer.

### Sanctions

* + - 1. Workforce Members that do not follow policies for disposal of printed PHI are subject to disciplinary action, up to and including termination of employment or assignment.
      2. Business associates found to be in violation of policies or laws regarding disposal or de-identification are subject to cancellation of service agreement and may be reported if found to be in violation of HIPAA laws to the appropriate authorities.

## Disposal of Electronic PHI

### Introduction

The HIPAA Privacy Rule requires that CSM Team apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI) in any form, as stated in 45 CFR 164.530(c). CSM Team must implement reasonable safeguards to limit incidental and avoid prohibited uses and disclosures of PHI, including the disposal of such information. The HIPAA Security Rule requires CSM Team to implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of electronic PHI from electronic media before the media are made available for reuse per 45 CFR 164.310(d)(2)(i) and (ii). Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI and may result in significant HIPAA breaches subject to penalties and fines.

CSM Team must ensure that Workforce Members receive training on and follow the disposal policies and procedures of the CSM Team as necessary and appropriate for each workforce member as noted in 45 CFR 164.306(a)(4), 164.308(a)(5), and 164.530(b) and (i). Therefore, any workforce member involved in disposing of PHI, or who supervises others who dispose of PHI, must receive training on disposal. This includes any volunteers. See 45 CFR 160.103 (definition of “workforce”).

The proper methods for destruction of PHI on electronic media include clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding). Please refer to Policy D-100 Disposal of Printed PHI for a complete introduction to the destruction and de-identification of PHI.

### Scope

All CSM Team Workforce Members shall be responsible for protecting PHI from unauthorized access, use, or disclosure. Except as authorized by the Compliance Officer, no interference with the storage of PHI or any hardware, software, or procedural mechanism that records or examines the activity of electronic PHI (“EPHI”) in the CSM Team information system shall be permitted.

This policy covers all Workforce Members, business associates, and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team In the event it is not clear if this policy applies to you, please contact the Compliance Officer.

### Disposal of Electronic Protected Health Information (PHI)

* + - 1. Printed material which includes PHI may be found in the following documents, labels, or other printed media: patient encounter forms and labels, printouts from IS systems containing PHI, CSM Team notes, index cards or worksheets with patient’s information, photocopies of patient’s insurance cards, patient’s information on post-It notes, personal reminders, emails, memos, telephone call logs, and other written communications that contain PHI. This list is not meant to be all-inclusive.
      2. Documents that contain PHI, which is subject to retention requirements, should be managed carefully to not expose PHI while in use, storage, or transportation.
      3. Workforce Members are prohibited from destroying, altering, or discarding any information (with or without PHI), which may be subject to government investigations, audits, subpoenas, and search warrants. Standard document disposal policies and destruction procedures should be immediately suspended once there is a notification that the documents are part of a government investigation, or a subpoena or search warrant has been served.
      4. Printed materials containing PHI that are not subject to retention requirements, must be destroyed or de-identified by an approved method. It is strictly prohibited to discard PHI into wastebaskets, recycling bins, or other accessible locations or containers.
      5. Printed materials containing PHI that can be shredded or de-identified, must be kept in a locked container prior to transport and disposal.
      6. In the event that there is insufficient space or lockable containers available for storage prior to destruction or de-identification, the Compliance Officer or designee is to be contacted for a resolution, and the materials kept secure until the issue is resolved.

**RESOURCE:** Special Publication 800-88, Revision 1, Guidelines for Media Sanitization has been approved as final as of December 17, 2014

Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. This guide will assist organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information.

### De-Identification Standard and Methods

* + - 1. Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify an individual and if the CSM Team Compliance Officer has no reasonable basis to believe it can be used to identify an individual.
      2. Sections 164.514(b) and(c) of the Privacy Rule contain the implementation specifications that a covered entity must follow to meet the de-identification standard.
      3. The Privacy Rule provides two methods by which health information can be designated as de-identified, which is Expert Determination and Safe Harbor.
      4. The Expert Determination method requires a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and (ii) Documents the methods and results of the analysis that justify such determination.
      5. The Safe Harbor Method requires that no parts or derivatives of any of the listed identifiers be disclosed in healthcare data. This method may be used by CSM Team through a third party, or a Workforce Member that has the expertise and equipment to complete this operation.
      6. The Compliance Officer must pre-approve any Workforce Member or outside company that is utilized for de-identification.
      7. In general, examples of proper disposal methods may include, but are not limited to:
         1. For PHI in paper records, shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
         2. Maintaining labeled prescription bottles and other PHI in opaque bags in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.
         3. For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

### Certificates of Destruction

* 1. All materials that contain PHI and are sent out to a contractor for disposal or de-identification, in bulk form, must be identified when destroyed with a Certificate of Destruction.
  2. Internal methods for destroying or de-identification of material that contain PHI must be approved by the Compliance Officer.

### Sanctions

* + - 1. Workforce Members that do not follow policies for disposal of printed PHI are subject to disciplinary action, up to and including termination of employment or assignment.
      2. Business associates found to be in violation of policies or laws regarding disposal or de-identification are subject to cancellation of service agreement and may be reported if found to be in violation of HIPAA laws to the appropriate authorities.

## Disposal of Electronic Devices and Media

### Introduction

The U.S. National Institute of Standards and Technology describes several different methods can be used to sanitize media (making PHI that is stored in electronics irretrievable). Four of the most common are presented in this section. Users of this guide should categorize the information to be disposed of, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media. The selected method should be assessed as to cost, environmental impact, etc., and a decision should be made that best mitigate the risks to unauthorized disclosure of information.

### Scope

All CSM Team Workforce Members shall be responsible for protecting PHI from unauthorized access, use, or disclosure. Except as authorized by the Compliance Officer, no interference with the storage of PHI or any hardware, software, or procedural mechanism that records or examines the activity of electronic PHI (“EPHI”) in CSM Team information system shall be permitted.

This policy covers all Workforce Members, business associates, and all others that have access to or work with Protected Health Information (PHI) associated with CSM Team In the event it is not clear if this policy applies to you, please contact the Compliance Officer.

### Disposal of Electronic Protected Health Information (PHI) Considerations

* + - 1. Early in the system life cycle, a system is categorized using the guidance found in FIPS 199, NIST SP 800- 60 Rev. 1, or CNSSI 125318, including the security categorization for the system’s confidentiality. This security categorization is revisited at least every three years (or when a significant change occurs within the system) and revalidated throughout the system’s life, and any necessary changes to the confidentiality category can be made. Once the security categorization is completed, the system owner can then design a sanitization process that will ensure adequate protection of the system’s information.
      2. A key decision on sanitization is whether the media are planned for reuse or recycle. Some forms of

media are often reused to conserve an organization’s resources.

* + - 1. While most devices support some form of Clear, not all devices have a reliable Purge mechanism. For moderate confidentiality data, the media owner may choose to accept the risk of applying Clear techniques to the media, acknowledging that some data may be able to be retrieved by someone with the time, knowledge, and skills to do so.
      2. If media are not intended for reuse either within or outside an organization due to damage or other reason, the simplest and most cost-effective method of control may be to destroy it.

### Types of Disposal/Removal of PHI from Electronic Devices and Media

* + - 1. The sanitation method is used to sanitize media is to use software or hardware products to overwrite user addressable storage space on the media with non-sensitive data, using the standard read and write commands for the device. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also should include all user addressable locations.
         1. The security goal of the overwriting process is to replace Target Data with non-sensitive data. Overwriting cannot be used for media that are damaged or not rewriteable and may not address all areas of the device where sensitive data may be retained. The media type and size may also influence whether overwriting is a suitable sanitization method. For example, flash memory-based storage devices may contain spare cells and perform wear leveling, making it infeasible for a user to sanitize all previous data using this approach because the device may not support directly addressing all areas where sensitive data has been stored using the native read and write interface.
  1. The Clear operation may vary contextually for media other than dedicated storage devices, where the device (such as a basic cell phone or a piece of office equipment) only provides the ability to return the device to factory state (typically by simply deleting the file pointers) and does not directly support the ability to rewrite or apply media-specific techniques to the non- volatile storage contents.
     1. Where rewriting is not supported, manufacturer resets and procedures that do not include rewriting might be the only option to Clear the device and associated media. These still meet the definition for Clear as long as the device interface available to the user does not facilitate retrieval of the Cleared data.
  2. Some methods of purging (which vary by media and must be applied with considerations described further throughout this document) include overwrite, block erase, and Cryptographic Erase, through the use of dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the abstraction inherent in typical read and write commands. Destructive techniques also render the device Purged when effectively applied to the appropriate media type, including incineration, shredding, disintegrating, degaussing, and pulverizing. The common benefit across all these approaches is assurance that the data is infeasible to recover using state of the art laboratory techniques. However, Bending, Cutting, and the use of some emergency procedures (such as using a firearm to shoot a hole through a storage device) may only damage the media as portions of the media may remain undamaged and, therefore, accessible using advanced laboratory techniques.

### Types of Disposal/Removal of PHI from Electronic Devices and Media, Continued.

* + - 1. Degaussing renders a Legacy Magnetic Device Purged when the strength of the degausser is carefully matched to the media coercivity. The technique of Coercivity may be difficult to determine based only on the information provided on the label. Therefore, refer to the device manufacturer for coercivity details. Degaussing should never be solely relied upon for flash memory-based storage devices or for magnetic storage devices that also contain non-volatile non-magnetic storage. Degaussing renders many types of devices unusable (and in those cases, Degaussing is also a Destruction technique).
      2. There are many different types, techniques, and procedures for media Destruction. While some techniques may render the Target Data infeasible to retrieve through the device interface and unable to be used for subsequent storage of data, the device is not considered Destroyed unless Target Data retrieval is infeasible using state of the art laboratory techniques. Disintegrate, Pulverize, Melt, and Incinerate. These sanitization methods are designed to completely Destroy the media. They are typically carried out at outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.
         1. Paper shredders can be used to Destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed.
         2. To make reconstructing the data even more difficult, the shredded material can be mixed with non-sensitive material of the same type (e.g., shredded paper or shredded flexible media).
         3. The application of Destructive techniques may be the only option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media; or when the verification of Clear or Purge methods fails (for known or unknown reasons).

### Compliance Officer Responsibilities

* + - 1. The Compliance Officer shall approve the method of destruction for each type of Electronic Devices and Media.
      2. The documentation of destruction shall be issued to the Compliance Officer and kept on record for a period of six (6) years.

### Equipment Destruction Documentation

* + - 1. Following sanitization, a certificate of media disposition should be completed for each piece of electronic media that has been sanitized. A certification of media disposition may be a piece of paper, or an electronic record of the action taken. For example, most modern hard drives include bar codes on the label for values such as model and serial numbers. The person performing the sanitization might simply enter the details into a tracking application and scan each bar code as the media is sanitized. Automatic documentation can be important as some systems make physical access to the media very difficult. When fully completed, the certificate should record at least the following details:
         1. Manufacturer, Model, Serial Number, Organizationally Assigned Media or Property Number (if applicable), Media Type (i.e., magnetic, flash memory, hybrid, etc.), Media Source (i.e., user or computer the media came from), Pre-Sanitization Confidentiality Categorization (optional), Sanitization Description (i.e., Clear, Purge, Destroy), Method Used (i.e., degauss, overwrite, block erase, crypto erase, etc.), Tool Used (including version), Verification Method (i.e., full, quick sampling, etc.), Post-Sanitization Confidentiality Categorization (optional), Post-Sanitization Destination (if known).
         2. For Sanitization and Verification; Position/Title of Person, Date, Location, Phone or Other Contact Information, and Signature

### Sanctions

* + - 1. Workforce Members that do not follow policies for disposal of electronic devices or media containing PHI are subject to disciplinary action, up to and including termination of employment or assignment.
      2. Business associates found to be in violation of policies or laws regarding the disposal of electronic devices or media containing PHI are subject to cancellation of service agreement and may be reported if found to be in violation of HIPAA laws to the appropriate authorities.

Resource for a complete listing of destruction techniques as of 1/1/2017 - The National Institute of Standards and Technology (NIST), Guidelines for Media Sanitation, NIST Special Publication 800-88, Revision 1, December 2014.

Source: [http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf**.**](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.)

# Section VI – Disaster Preparedness and Response

## DI-100 Disaster Preparedness and the Community

### Introduction

The U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), has published a bulletin to ensure that HIPAA covered entities and their business associates are aware of the ways in which patient information may be shared under the HIPAA Privacy Rule in an emergency situation, and to serve as a reminder that the protections of the Privacy Rule are not set aside during an emergency. The HIPAA Privacy Rule protects the privacy of patients’ health information (protected health information) but is balanced to ensure that appropriate uses and disclosures of the information still may be made when necessary to treat a patient, to protect the nation’s public health, and for other critical purposes.

Under the Privacy Rule, covered entities may disclose, without a patient’s authorization, protected health information about the patient as necessary to treat the patient or to treat a different patient. Treatment includes the coordination or management of health care and related services by one or more health care providers and others, consultation between providers, and the referral of patients for treatment. See 45 CFR §§ 164.502(a)(1)(ii), 164.506(c), and the definition of “treatment” at 164.501. For the purpose of this policy, treatment shall include the dispensing of pharmaceutical drugs and related supplies and equipment.

The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information that is necessary to carry out their public health mission. Therefore, the Privacy Rule permits covered entities to disclose needed protected health information without individual authorization:

**To a public health authority, such as the Centers for Disease Control and Prevention (CDC) or a state or local health department, that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability**. This would include, for example, the reporting of disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions. A “public health authority” is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or Territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. See 45 CFR §§164.501 and 164.512(b)(1)(i). For example, a covered entity may disclose to the CDC protected health information on an ongoing basis as needed to report all prior and prospective cases of patients exposed to or suspected or confirmed to have Ebola virus disease.

At the **direction of a public health authority**, to **a foreign government agency** that is acting in collaboration **with the public health authority** - 45 CFR 164.512(b)(1)(i).

To **persons at risk of contracting or spreading a disease or condition** if other law, such as state law, authorizes the covered entity to notify such persons as necessary to prevent or control the spread of the disease or otherwise to carry out public health interventions or investigations - 45 CFR 164.512(b)(1)(iv).

Introduction, Continued.

Disclosures to Family, Friends, and Others Involved in an Individual’s Care and for Notification. **A covered entity may share protected health information with a patient’s family members, relatives, friends, or other persons identified by the patient as involved in the patient’s care**. A covered entity also may share information about a patient as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the patient’s care, of the patient’s location, general condition, or death. This may include, where necessary, to notify family members and others, the police, the press, or the public at large. See 45 CFR 164.510(b).

The covered entity **should get verbal permission from individuals or otherwise be able to reasonably infer that the patient does not object**, when possible; if the individual is incapacitated or not available, covered entities may share information for these purposes if, in their professional judgment, doing so is in the patient’s best interest.

In addition, a covered entity may share protected health information with **disaster relief organizations** that, like the American Red Cross, are authorized by law or by their charters to assist in disaster relief efforts, for the purpose of coordinating the notification of family members or other persons involved in the patient’s care, of the patient’s location, general condition, or death. It is unnecessary to obtain a patient’s permission to share the information in this situation if doing so would interfere with the organization’s ability to respond to the emergency.

**Imminent Danger Health care providers** may share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public consistent with applicable law (such as state statutes, regulations, or case law) and the provider’s standards of ethical conduct - 45 CFR 164.512(j).

**Disclosures to the Media or Others Not Involved in the Care** of the Patient/Notification Upon request for information about a particular patient by name, a hospital or other health care facility may release limited facility directory information to acknowledge an individual is a patient at the facility and provide basic information about

the patient’s condition in general terms (e.g., critical or stable, deceased, or treated and released) if the patient has not objected to or restricted the release of such information, if the patient is incapacitated, or if the disclosure is believed to be in the best interest of the patient and is consistent with any prior expressed preferences of the patient. See 45 CFR 164.510(a). In general, except in the limited circumstances described elsewhere in this Bulletin, affirmative reporting to the media or the public at large about an identifiable patient, or the disclosure to the public or media of specific information about the treatment of an identifiable patient, such as specific tests, test results or

details of a patient’s illness may not be done without the patient’s written authorization (or the written authorization of a personal representative who is a person legally authorized to make health care decisions for the patient). See 45 CFR 164.508 for the requirements for a HIPAA authorization.

**Minimum Necessary for most disclosures**, a covered entity must make reasonable efforts to limit the information disclosed to that which is the “minimum necessary” to accomplish the purpose. (Minimum necessary requirements do not apply to disclosures to health care providers for treatment purposes.) Covered entities may rely on representations from a public health authority or another public official that the requested information is the minimum necessary for the purpose. For example, a covered entity may rely on representations from the CDC that the protected health information requested by the CDC about all patients exposed to or suspected or confirmed to have Ebola virus disease is the minimum necessary for the public health purpose. Internally, covered entities should continue to apply their role-based access policies to limit access to protected health information to only those workforce members who need it to carry out their duties - 45 CFR §§ 164.502(b), 164.514(d).

**Business Associates** - A business associate of a covered entity (including a business associate that is a subcontractor) may make disclosures permitted by the Privacy Rule, such as to a public health authority, on behalf of a covered entity or another business associate to the extent authorized by its business associate agreement.

**Safeguarding Patient Information** - In an emergency situation, covered entities must continue to implement reasonable safeguards to protect patient information against intentional or unintentional impermissible uses and disclosures. Further, covered entities (and their business associates) must apply the administrative, physical, and technical safeguards of the HIPAA Security Rule to electronic protected health information.

**The HIPAA Privacy Rule is not suspended during public health or another emergency**; however, the Secretary of HHS may waive certain provisions of the Privacy Rule under the Project Bio shield Act of 2004 (PL 108-276) and section 1135(b)(7) of the Social Security Act. If the President declares an emergency or disaster and the Secretary declares a public health emergency, the Secretary may waive sanctions and penalties against a covered hospital that does not comply with the following provisions of the HIPAA Privacy Rule: the requirements to obtain a patient's agreement to speak with family members or friends involved in the patient’s care - 45 CFR 164.510(b), the requirement to honor a request to opt-out of the facility directory - 45 CFR 164.510(a), the requirement to distribute a notice of privacy practices - 45 CFR 164.520, the patient's right to request privacy restrictions - 45 CFR 164.522(a)the patient's right to request confidential communications. See 45 CFR 164.522(b).

**If the Secretary issues such a waiver**, it only applies: (1) in the emergency area and for the emergency period identified in the public health emergency declaration; (2) to hospitals that have instituted a disaster protocol; and (3) for up to 72 hours from the time the hospital implements its disaster protocol. When the Presidential or Secretarial declaration terminates, a hospital must then comply with all the requirements of the Privacy Rule for any patient still under its care, even if 72 hours has not elapsed since implementation of its disaster protocol.

**HIPAA Applies Only to Covered Entities and Business Associates** - The HIPAA Privacy Rule applies to disclosures made by employees, volunteers, and other members of a covered entity’s or business associate’s workforce. Covered entities are health plans, health care clearinghouses, and those health care providers that conduct one or more covered health care transactions electronically, such as transmitting health care claims to a health plan. Business associates generally are persons or entities (other than members of the workforce of a covered entity) that perform functions or activities on behalf of or provide certain services to, a covered entity that involves creating, receiving, maintaining, or transmitting protected health information.

Business associates also include subcontractors that create, receive, maintain, or transmit protected health information on behalf of another business associate. The Privacy Rule does not apply to disclosures made by entities or other persons who are not covered entities or business associates (although such persons or entities are free to follow the standards on a voluntary basis if desired). There may be other state or federal rules that apply.

# Quick Information Guide 1.0: Civil and Criminal Penalties

### (HIPAA) HITECH Act Enforcement Interim Final Rule

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

Section 13410(d) of the HITECH Act, which became effective on February 18, 2009, revised section 1176(a) of the Social Security Act (the Act) by establishing:

* Four categories of violations that reflect increasing levels of culpability.
* Four corresponding tiers of penalty amounts that significantly increase the minimum penalty amount for each violation.
* A maximum penalty amount of $1.5 million for all violations of an identical provision.

It also amended section 1176(b) of the Act by:

* Striking the previous bar on the imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation (such violations are now punishable under the lowest tier of penalties); and providing a prohibition on the imposition of penalties for any violation that is corrected within a 30-day time period, as long as the violation was not due to willful neglect.

The Enforcement Provisions are not found in the HHS Regulations; rather they are Congressionally promulgated statutes found in the U.S. Code:

42 U.S.C. §§ 1320d-5 & 1320d-6 & 42 U.S.C. § 1320d-5 Civil Violations. 42

U.S.C. § 1320d-6 Criminal Violations

### General Penalty for Failure to Comply with Requirements and Standards U.S.C. § 1320d-5 (Civil Violations)

* Punishes any violation of regulations.
* Maximum penalty of $100 per violation
* Cap of $25,000 per the calendar year for each provision of the regulations that are violated.

### Wrongful Disclosure of Individually Identifiable Health Information 42 U.S.C. § 1320D-6(a) (Criminal Violations)

Violation of federal law and violations must be committed “knowingly.” A person commits an act “knowingly” when it is done purposefully; that is, the act is a product of a conscious design, intent, or plan that it be done. *Horne v. State of Indiana, 445 N.E.2d 976 (1983)*

The following are the categories of knowingly and in Violation:

* Knowingly and in violation of the regulations using or causing to be used a unique health identifier.
* Knowingly and in violation of the regulations obtaining individually identifiable health information relating to an individual.
* Knowingly and in violation of the regulations disclosing individually identifiable health information to another person.

Criminal Penalties for Violating § 1320d-6:

* Maximum penalties are set forth in §1320d-6(b). Actual sentencing is determined according to the Federal Sentencing Guidelines.
* Maximum Penalties (42 U.S.C. § 1320d-6(b)(1)) for any violation are a $50,000 fine, or one-year imprisonment, or both.
* Maximum Penalties (42 U.S.C. § 1320d-6(b)(2)) If the offense is committed under false pretenses carry a $100,000 fine, or 5-years imprisonment, or both.
* Maximum Penalties (42 U.S.C. § 1320d-6(b)(3)) If the offense is committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm includes a $500,000 fine, or 10-years imprisonment, or both.

Other U.S. Statutes That Could Lead to Further Criminal or Civil Liability for Violating HIPAA

* Wire and Mail Fraud Statues, 18 U.S.C. §§ 1341 & 1343
* False Claims Act, 31 U.S.C. § 3729

If a Workforce Member becomes aware of intentional HIPAA violation(s), they are required to inform the Compliance Officer immediately or the Department of Health and Human Services (contact information located in Section G-100 Emergency Contact Information.

# Quick Information Guide 2.0: HIPAA State Security Laws

### Select State HIPAA Security Laws

Many states have breach reporting requirements that are more stringent than federal laws. The most recent links to state reporting requirements are listed below and are subject to change without notice. Please see state regulatory agencies for specific guidelines.

**Alabama**

[2018 S.B. 318, Act No. 396](http://arc-sos.state.al.us/PAC/SOSACPDF.001/A0012674.PDF)

**Alaska**

[45.48.010](http://www.legis.state.ak.us/basis/folioproxy.asp?url=http://wwwjnu01.legis.state.ak.us/cgi-bin/folioisa.dll/stattx09/query=%5bJUMP:%27AS4548010%27%5d/doc/%7b@1%7d?firsthit)

**Arizona**

Ariz. Rev. Stat. § [18-545](http://www.azleg.gov/viewDocument/?docName=http://www.azleg.gov/ars/18/00545.htm)

**Arkansas**

[Ark. Code](http://www.lexis-nexis.com/hottopics/arcode/) §§ 4-110-101 *et seq.*

**California**

Cal. Civ. Code §§ [1798.29](http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29.), [1798.8*2*](http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82.)

Cal. Penal Code § 471.5: *Alteration or Modification of Medical Record or Creation of False Medical Record with Fraudulent Intent*

Cal. Civ. Code § 56.101: *Storage and Destruction of Records (Pharmaceutical Companies)*

Cal. Civ. Code §56.36: *Violations of Patient Confidentiality of Medical Information*

Cal. Health & Safety Code § 1280.15 - *Reporting of Unlawful or Unauthorized Access or Disclosure of Patient Medical Information*

**Colorado**

[Colo. Rev. Stat.](http://www.lexisnexis.com/hottopics/colorado/) § 6-1-716

**Connecticut**

Conn. Gen Stat. §§ [36a-701b](http://www.cga.ct.gov/current/pub/chap_669.htm#sec_36a-701b), [4e-70](https://www.cga.ct.gov/2016/sup/chap_062a.htm)

**Delaware**

Del. Code [tit. 6, § 12B-101 *et seq.*](http://delcode.delaware.gov/title6/c012b/index.shtml)

**Florida**

Fla. Stat. §§ [501.171](http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0500-0599/0501/Sections/0501.171.html), [282.0041](http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0200-0299/0282/Sections/0282.0041.html), [282.318(2)(i)](http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0200-0299/0282/Sections/0282.318.html)

Florida Statutes § 817.5681: *Protected Health Information Breaches*

**Georgia**

[Ga. Code](http://www.lexis-nexis.com/hottopics/gacode/Default.asp) §§ 10-1-910, -911, -912; § 46-5-214

Georgia Code Title 31 – Health *Chapter 33 – Health Records*

**Hawaii**

Haw. Rev. Stat. §[487N-1 *et seq****.***](http://www.capitol.hawaii.gov/hrscurrent/Vol11_Ch0476-0490/HRS0487N/HRS_0487N-0001.htm)

**Idaho**

Iowa Code §§ [715C.1, 715C.2](https://www.legis.iowa.gov/docs/code/715c.pdf)

**Illinois**

Iowa Code §§ [715C.1, 715C.2](https://www.legis.iowa.gov/docs/code/715c.pdf)

**Indiana**

Ind. Code §§ [4-1-11 *et seq*](http://iga.in.gov/legislative/laws/2016/ic/titles/004/articles/001/chapters/011/)[**.**](http://www.in.gov/legislative/ic/code/title4/ar1/ch11.html), [24-4.9 *et seq.*](http://iga.in.gov/legislative/laws/2016/ic/titles/024/articles/4.9/chapters/001/)

**Iowa**

Iowa Code §§ [715C.1, 715C.2](https://www.legis.iowa.gov/docs/code/715c.pdf)

**Kansas**

Kan. Stat. § [50-7a01 et seq.](http://www.kslegislature.org/li/b2013_14/statute/050_000_0000_chapter/050_007a_0000_article/)

**Kentucky**

KRS § [365.732,](http://www.lrc.ky.gov/Statutes/statute.aspx?id=43326)[KRS](http://www.lrc.ky.gov/Statutes/statute.aspx?id=43575)§§ [61.931 to 61.934](http://www.lrc.ky.gov/Statutes/statute.aspx?id=43575)

**Louisiana**

La. Rev. Stat. §§ [51:3071 *et seq*](http://legis.la.gov/Legis/Law.aspx?d=322027).

**Maine**

Me. Rev. Stat. tit. 10 § [1346 *et seq.*](http://janus.state.me.us/legis/statutes/10/title10ch210-Bsec0.html)

**Maryland**

[Md. Code](http://www.lexisnexis.com/hottopics/mdcode/) Com. Law §§ 14-3501 et seq., Md. State Govt. Code §§ 10-1301 to -1308

**Massachusetts**

Mass. Gen. Laws §[**93H-1 *et seq.***](http://www.mass.gov/legis/laws/mgl/93h-1.htm)

105. Mass. Code Regs. 145.505: *Record Keeping Facilities and Equipment*

105. Mass. Code Regs. 145.545: *Safeguards Against Loss and Use of Medical Records*

105. Mass. Code Regs. 145.555: *Release of Medical Record*

**Michigan**

Mich. Comp. Laws §§ [445.63](http://legislature.mi.gov/doc.aspx?mcl-445-63), [445.72](http://legislature.mi.gov/doc.aspx?mcl-445-72)

Mich. Admin. Code r. 325.3848: *Medical Records Storage*

**Minnesota**

Minn. Stat. §§[**325E.61**](https://www.revisor.mn.gov/statutes/?id=325E.61)**,**[**325E.64**](https://www.revisor.mn.gov/statutes/?id=325E.64)

MN ADC 9505.2197: *Vendor Responsibilities for Electronic Records*

**Missouri**

Mo. Rev. Stat. § [407.1500](http://www.moga.mo.gov/mostatutes/stathtml/40700015001.html)

Mo. Code Regs. Ann. tit. 13, § 70-3.160: *Electronic Submission of HealthNet Claims and Electronic remittance*

**Montana**

Mont. Code §§ [2-6-1501 to -1503,](http://leg.mt.gov/bills/mca_toc/2_6_15.htm)[30-14-1701 *et seq.*](http://leg.mt.gov/bills/mca/30/14/30-14-1704.htm), [33-19-321](http://leg.mt.gov/bills/mca/33/19/33-19-321.htm)

**Nebraska**

Neb. Rev. Stat. §§ [**87-801 *et seq*.**](http://nebraskalegislature.gov/laws/statutes.php?statute=87-801)

**Nevada**

Nev. Rev. Stat. §§[**603A.010 *et seq.***](http://www.leg.state.nv.us/NRS/NRS-603A.html)**,**[**242.183**](http://www.leg.state.nv.us/NRS/NRS-242.html#NRS242Sec183)

**New Hampshire**

New Hampshire Code of Administrative Rules Ph §703.05: *Confidentiality under the Controlled Drug Act*

**New Jersey**

[N.J. Stat. § 56:8-161](https://lis.njleg.state.nj.us/nxt/gateway.dll/statutes%2F1%2F50660%2F51038), [163](https://lis.njleg.state.nj.us/nxt/gateway.dll/statutes%2F1%2F50660%2F51040)

**New Mexico**

[2017 H.B. 15, Chap. 36](https://www.nmlegis.gov/Sessions/17%20Regular/final/HB0015.pdf) (effective 6/16/2017)

N.M. Stat. Ann. §24-14A-6: *Health Information System; Creation and Access*

N.M. Code R. §8.300.11.11B: *Confidentiality of Electronic Data*

N.M. Stat. Ann. §24-14A-10: *Health Information System; Violation and Penalties*

**New York**

[N.Y. Gen. Bus. Law](http://public.leginfo.state.ny.us/lawssrch.cgi?NVLWO:) § 899-AA, [N.Y. State Tech. Law](http://public.leginfo.state.ny.us/lawssrch.cgi?NVLWO:)208

*New York Consolidated Laws, Public Health Law - PBH § 18.*

**North Carolina**

N.C. Gen. Stat §§ [75-61](http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-61.html), [75-65](http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-65.html)

**North Dakota**

N.D. Cent. Code §§ [51-30-01 *et seq*.](http://www.legis.nd.gov/cencode/t51c30.pdf)

**Ohio**

Ohio Rev. Code §§ [1347.12](http://codes.ohio.gov/orc/1347.12), [1349.19](http://codes.ohio.gov/orc/1349.19), [1349.191](http://codes.ohio.gov/orc/1349.191), [1349.192](http://codes.ohio.gov/orc/1349.192)

Ohio Rev. Code Ann. § 3798.03 - *Duty of Covered Entities*

**Oklahoma**

Okla. Stat. §§ [74-3113.1,](http://webserver1.lsb.state.ok.us/OK_Statutes/CompleteTitles/os74.rtf) [24-161 to -166](http://webserver1.lsb.state.ok.us/OK_Statutes/CompleteTitles/os24.rtf)

**Oregon**

Oregon Rev. Stat. §§ [646A.600 to .628](https://www.oregonlegislature.gov/bills_laws/ors/ors646A.html)

Or. Admin. R. 325-015-0055 - *Protection of Patient Safety Data*

Or. Rev. Stat. § 431.970 - *Reports to Health Professional Regulatory Boards (Pharmacist)* Or. Admin. R. 410-121- 4020 - *Information Access (Prescription Drug Monitoring)*

**Pennsylvania**

28 Pa. Code § 115.27: *Confidentiality of Medical Records* 28 Pa. Code § 563.1: *Patient Access to Medical Records* 28 Pa. Code § 115.23: *Preservation of Medical Records*

**Rhode Island**

R.I. Gen. Laws §§ [11-49.3-1 *et seq*.](http://webserver.rilin.state.ri.us/Statutes/TITLE11/11-49.3/INDEX.HTM)

**South Carolina**

S.C. Code § [39-1-90](http://www.scstatehouse.gov/code/t39c001.php)

**South Dakota**

S.D. Cod. Laws §§ [20-40-20 to -46](https://sdlegislature.gov/Statutes/Codified_Laws/DisplayStatute.aspx?Type=Statute&Statute=22-40-20) ([2018 S.B. 62](http://www.sdlegislature.gov/Legislative_Session/Bills/Bill.aspx?Bill=62&Session=2018))

**Tennessee**

[Tenn. Code](http://www.lexisnexis.com/hottopics/tncode/) §§ 47-18-2107; 8-4-119

**Texas**

Tex. Bus. & Com. Code §§ [521.002](http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm#521.002), [521.053](http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm#521.053)

Texas Legislature House Bill 300 (H.B. 300)

**Vermont**

Vt. Stat. [tit. 9 §§ 2430, 2435](http://legislature.vermont.gov/statutes/chapter/09/062)

20-4 Vt. Code R. 1400:10.14: *Security of electronic equipment under the Board of Pharmacy*

**Virginia**

Va. Code §§ [18.2-186.6](http://law.lis.virginia.gov/vacode/title18.2/chapter6/section18.2-186.6/), [32.1-127.1:05](http://law.lis.virginia.gov/vacode/title32.1/chapter5/section32.1-127.1:05/)

**Washington**

Wash. Rev. Code §§ [19.255.010](http://apps.leg.wa.gov/RCW/default.aspx?cite=19.255.010), [42.56.590](http://apps.leg.wa.gov/RCW/default.aspx?cite=42.56.590)

Wash. Admin. Code § 246-455-080: *Security and Release of Reported Hospital Patient Discharge Data*

Wash. Admin. Code § 246-875-070: *Confidentiality & Security of Pharmacy Patient Medication Record Systems*

Wash. Rev. Code § 41.05.039: *Health Information Lead Organization and Secure Access* Wash. Rev. Code § 41.05.042: *Health Information Process Guidelines for Lead Organizations* Wash. Rev. Code § 69.41.055: *Electronic Communication of Prescription Information*

Wash. Rev. Code § 70.02.150: *Healthcare Information Safeguards Provider Requirements*

**West Virginia**

W.V. Code §§ [46A-2A-101 et seq.](http://www.legis.state.wv.us/WVCODE/Code.cfm?chap=46a&art=2A#2A)

**Wisconsin**

Wis. Stat. § [134.98](http://www.legis.state.wi.us/statutes/Stat0134.pdf)

Wis. Stat. Ann. § 252.25 - *Violation of Law Relating to Health*

**Wyoming**

[Wyo. Stat.](http://legisweb.state.wy.us/NXT/gateway.dll?f=templates&fn=default.htm&vid=) §§ 40-12-501 *et seq*

**District of Columbia**

[D.C. Code](http://www.lexisnexis.com/hottopics/dccode/) §§ 28- 3851 *et seq.*

**Guam**

[9 GCA §§ 48-10 et seq.](http://www.guamcourts.org/CompilerofLaws/GCA/09gca/9gc048.pdf)

**Puerto Rico**

10 [Laws of Puerto Rico](http://www.michie.com/puertorico/lpext.dll?f=templates&fn=main-h.htm&cp=prcode) §§ 4051 *et seq.*

**Virgin Islands**

[V.I. Code](http://www.michie.com/virginislands/lpext.dll?f=templates&fn=main-h.htm&cp=vicode) tit. 14, §§ 2208, 2209

If a Workforce Member becomes aware of intentional HIPAA violation(s) they are required to inform the Compliance Officer immediately or the Department of Health and Human Services (contact information located in Section G-100 Emergency Contact Information.

# Quick Information Guide 3.0: HIPAA Definitions

### Definitions

**Access** - The ability or the means necessary to read, write, modify, or communicate data or otherwise use any system that involves Protected Health Information.

**Administrative Safeguards –** Administrative actions and policies and procedures (1) to manage the selection, development, implementation, and maintenance of security measures, and (2) to protect ePHI and to manage the conduct of the Covered Components’ workforce in relation to the protection of ePHI.

**Auditable Event** - Any change to the security state of a system, any attempted or actual violation of the system access control or accountability security policies, or both (e.g., authentication attempts, access of health or financial records, information system start-up or shutdown, use of privileged accounts such as a system admin account).

**Authentication** – The corroboration that a person or entity is the one that it is claimed to be, which requires an individual identification parameter.

**Backup Data** - Retrievable, an exact copy of data to be backed up, including applications, operating systems, database software, and other software supporting packages and tools, as well as the contents of databases and files.

**Breach** – **(1)** The acquisition, access, use, or disclosure of protected health information in a manner not permitted under 45 CFR 164.402, which compromises the security or privacy of the protected health information. **Breach excludes - (i) any unintentional acquisition**, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity (covered or support component) or a business associate, if such acquisition, access, or use was made in good faith and within the course and scope of authority and does not result in further access, use or disclosure in a manner not permitted under 45 CFR 164.402. **(ii) inadvertent disclosure** - by a person who is otherwise authorized to access protected health information at a covered entity (covered or support component) or business associate to another person authorized to access protected health information at the same covered entity (covered or support component) or business associate, or organized health care arrangement in which the covered entity (covered or support component) participates, and the information received as a result of such disclosure is not further accessed, used or disclosed in a manner not permitted under 45 CFR 164.402. **(iii) A disclosure of protected health information** - where a covered entity (covered or support component) or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. **(2) Except as provided in the definition of “Breach,”** an acquisition, access, use, or disclosure of protected health information in a manner not permitted under 45 CFR 164.402 is presumed to be a breach unless the covered entity (covered or support component) or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors: **The nature and extent of the protected health information involved**, including the types of identifiers and the likelihood of re-identification. **The unauthorized person** who used the protected health information or to whom the disclosure was made **whether the protected health information** was actually acquired or viewed; and t**he extent to which the risk** to the protected health information has been mitigated.

**Business Associate (BA)** - A person or organization that creates, receives, maintains, or transmits protected health information in any form or medium, including electronic media, in fulfilling certain functions or activities for a HIPAA covered entity (covered or support component) and that performs a function or activity involving the use or disclosure of protected health information for or on behalf of the covered entity (covered or support component). A person or organization that only assists in the performance of the function or activity are also a business associate. This includes a person or organization that receives PHI from the covered entity (covered or support component), and one who obtains PHI for the covered entity (covered or support component). This includes, for example, data analysis, processing or administration; web site hosting; utilization review; quality assurance; billing; collections; benefit management; practice management; legal services; actuarial services; accounting and auditing; consulting; management and administrative services; accreditation; financial services; or any other service in which the person or organization obtain PHI from or for the covered entity (covered or support component). Members of the workforce are not considered business associates. The exchange of protected health information between providers of health care, for purposes of providing treatment to a patient, does not create a business associate relationship.

**Covered Entity -** Individual, business entity, or group plan that (i) provides or pays the cost of medical care (i.e., a health plan), (ii) processes or facilitates the processing of health information received in a nonstandard format into a standard transaction or a standard transaction into a nonstandard format (i.e., a health care clearinghouse), or (iii) a provider of medical or health services, and any other person or organization that furnishes, bills, or is paid for health care in the normal course of business (i.e., a health care provider).

**De-identified Information** - protected health information from which individually identifiable information has been removed and, when combined with any other information, does not identify the patient. There are only two ways to de-identify health information: a formal determination by a qualified statistician; or the removal of specified identifiers of the patient and of the patient’s relatives, household members, which will be deemed adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the patient.

**Designated Record Set** - a group of records maintained by or for CSM Team that is the covered entity and billing records about a patient maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used in whole or in part by or for the covered entity to make decisions about the patient.

**Disclosure**– The release, transfer, provision of access to, or divulging in any other manner of protected health information outside of the entity holding the information.

**Digital Signature** - Cryptographic code that is attached to a piece of data. This code can be regularly verified to ensure that the data has not been improperly altered.

**Discovered Breach** - A breach is to be treated as discovered by a covered entity (covered or support component) or a business associate if any person, other than the individual committing the breach, which is an employee, officer or another agent of such entity or business associate knows or should reasonably have known of the breach. The time period for notification begins to run when the incident becomes known, not when it is determined that a breach, as defined by the Rule, has occurred.

**Electronic Health Record –** Protected Health Information is maintained in an electronic format.

**Electronic Protected Health Information (ePHI)** is a common reference for PHI in an electronic format**.**

**Electronic Media** - Electronic storage material on which data is or may be recorded electronically, including, for example, memory devices in computers (hard drives) and any removable/transportable digital memory media such as magnetic tape or disk, optical disk, or digital memory card, computers (i.e., servers, desktops, laptops), Storage Area Networks (SANS), floppy diskettes, backup tapes, and cartridges; or transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media.

**Emancipated Minor** – A minor who is to be treated as an adult for purposes of this policy. An emancipation order allows a minor to consent to “medical, dental or psychiatric care, without parental consent, knowledge or liability.” In Connecticut, minors above age sixteen or their parents may petition the Superior Court for Juvenile Matters or the Probate Court for emancipation orders. The court may declare the minor emancipated if (1) the minor has been married, (2) the minor actively serves in the U.S. armed forces, (3) the minor willingly lives away from home and manages his or her own finances, or (4) the court determines “for good cause” that emancipation is in the “best interest” of the minor. A minor may also be considered emancipated under common law under similar circumstances. Check with your state for more information.

**Family Member** – means an individual’s dependent or any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or the individual’s dependent.  Relatives by marriage or adoption are treated the same as relatives who share a common biological ancestor.  First-degree relatives include parents, spouses, siblings, and children.  Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.  Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.  Fourth-degree relatives include great-great-grandparents, great-great-grandchildren, and children of first cousins.

**Genetic Information** – means information about an individual’s genetic tests, the genetic tests of family members of the individual, the manifestation of a disease or disorder in family members of the individual, or any request for or receipt of genetic services including participation in clinical research which includes genetic services by the individual or their family member.  Genetic information includes the genetic information of a pregnant women’s fetus or that of a family member or of any embryo legally held by the individual or family member using an assisted reproductive technology.  Genetic information does not include the sex or age of an individual.

**The Genetic Information Nondiscrimination Act (GINA) -** prohibits discrimination based on genetic information in health coverage.  Title II of GINA prohibits discrimination based on genetic information in employment.

**Health Information** – any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

**HIPAA Compliance Officer** - Individual entrusted with overall responsibility and management of data and information, including electronic data decision-making authority related to the development, implementation, and maintenance of policies and procedures related to University Data and may delegate responsibilities as they deem appropriate in specific functional areas related to Protected Health information privacy and security compliance.

**HIPAA** - The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

**HIPAA Omnibus Rule** - The amendments to the HIPAA Security Regulations published in the Federal Register on January 25, 2013, entitled “Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule.”

**HIPAA Security Regulations -** Regulations published in the Federal Register by the Department of Health and Human Services on February 20, 2003, as the “Health Insurance Reform: Security Standards; Final Rule,” as amended or superseded from time to time. These include the Omnibus Rule amendments, published in the Federal Register on January 25, 2013.

**HITECH** - The Health Information Technology for Economic and Clinical Health Act, enacted under Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5.

**Individually Identifiable Health Information**– a subset of “health information,” including demographic information, (1) that is created or received by a health care provider, health plan, employer, or health care clearinghouse; 2) that relates to the physical or mental health or condition of an individual; the provision of health care to an individual; or the payment for the provision of health care to an individual; and (3) that identifies the individual, or might reasonably be used to identify the individual.

**Information System** - Interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

**Legally Authorized Representative** – A person authorized either by state law or by court appointment to make decisions, including decisions related to health care, on behalf of another person, including someone who is authorized under applicable law to consent on behalf of a prospective subject to the subject’s participation in the procedure involved in the research.

**Limited Data Set**– Protected health information that excludes all of the 16 HIPAA specified direct identifiers of the individual or of relatives, employers, or household members of the individual, but retains geographic subdivisions larger than the postal address and elements of dates. Limited data sets may only be used for research, public health, or for health care operations, and only with a data use agreement that limits the use of the data by the recipient.

**Minimum Necessary**– refers to reasonable efforts made to limit use, disclosure, or requests for PHI to the minimum necessary to accomplish the intended purpose. The “Minimum Necessary Standard” means the standard used to characterize the limited extent to which PHI may be used or disclosed to accomplish an authorized purpose. The standard does not apply to the following: disclosures to or a request by a health care provider for treatment; disclosures to the patient or the patient’s Personal Representative; disclosures made in accordance with an express authorization; disclosures to HHS for complaint investigation, compliance review, or enforcement; or other uses or disclosures required by law.

**OCR** – Office of Civil Rights, the branch of the DHHS that is responsible for federal oversight of the privacy regulations.

**Patient** – a person who is ill or is undergoing treatment for the disease.

**Personal Representative** – Someone with the legal authority to act on behalf of an incompetent adult patient, a minor patient, or a deceased patient or the patient’s estate in making health care decisions or in exercising the patient’s rights related to the individual’s protected health information.

**Physical safeguards** are measures, policies, and procedures to physically protect the Covered Components’ Systems and related buildings and equipment that contain ePHI, from natural and environmental hazards and unauthorized intrusion.

**Privacy Rule** – Provides patients and their authorized representatives, with few exceptions, the right to inspect, review, and receive a copy of medical records and billing records that are held by health plans and health care providers covered by the Privacy Rule.

**Protected Health Information (PHI) -** any type of information that provides a reasonable basis to identify a patient, including, but not limited to, demographic information that relates to the patient’s past, present or future physical or mental health or condition; the provision of health care to the patient; or the past, present, or future payment for the provision of health care to the patient. PHI generally includes many common identifiers: such as name, address, birth date, and social security number. PHI can exist in or on a variety of forms. For example, it can be in “hard copy” or “paper” form, such as a written prescription, or in an “electronic” form such as the data used to adjudicate or reconcile payments received for claims.

**Protected Health Information (PHI)** does not include information found in employment records that a covered entity, such as CSM Team in its capacity as an employer, including worker’s compensation information, education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, or health information that neither identifies nor provides a reasonable basis to identify a patient (De-identified Information) or health information that concerns a patient that has been deceased for more than fifty (50) years.

**Risk Analysis** - A systematic and analytical approach that identifies and assesses risks to the confidentiality, integrity, or availability of a covered entity’s (covered or support component’s) EPHI. Risk analysis considers all relevant losses that would be expected if specific security measures protecting EPHI were not in place. Relevant losses include losses caused by unauthorized use and disclosure of EPHI and loss of data integrity.

**Workforce Member** - Employees, physicians, volunteers, trainees, and persons other than those deemed business associates whose conduct, in the performance of work for a covered entity (covered or support component), is under the direct control of such covered entity (covered or support component), whether or not they are paid by the covered entity (covered or support component), and who have access to PHI. This includes full and part-time employees, volunteers, and third parties other than those deemed business associates who provide service to the covered entity (covered or support component).

**Unemancipated Minor** – A person under 18 years of age and not previously married; not in the Armed Services; not previously emancipated by court proceedings initiated by the parents or the state and in the care and control of the parents. The rights of parents and minors regarding access to PHI varies by state.

# Quick Information Guide 4.0: Privacy Disclosure Guideline Examples

###### Can health care providers engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard?

Answer:

Yes. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requiring covered entities to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that.

providers’ primary consideration is the appropriate treatment of their patients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, and high-quality health care. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.

For example, the following practices are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

* Health care staff may orally coordinate services at hospital nursing stations.
* Nurses or other health care professionals may discuss a patient’s condition over the phone with the patient, a

provider, or a family member.

* A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.
* A physician may discuss a patients’ condition or treatment regimen in the patient’s semi-private room.
* Health care professionals may discuss a patient’s condition during training rounds in an academic or training institution.
* A pharmacist may discuss a prescription with a patient over the pharmacy counter, or with a physician or the patient over the phone.

In these circumstances, reasonable precautions could include using lowered voices or talking apart from others when sharing protected health information. However, in an emergency situation, in a loud emergency room, or where a patient is hearing impaired, such precautions may not be practicable. Covered entities are free to engage in communications as required for quick, effective, and high-quality health care.

###### Does the HIPAA Privacy Rule permit a doctor to discuss a patient’s health status, treatment, or payment arrangements with the patient’s family and friends?

Answer:

Yes. The HIPAA Privacy Rule at 45 CFR 164.510(b) specifically permits covered entities to share information that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient’s care or payment for health care. If the patient is present, or is otherwise available prior to the disclosure, and has the capacity to make health care decisions, the covered entity may discuss this information with the family and these other persons if the patient agrees or, when given the opportunity, does not object. The covered entity may also share relevant information with the family and these other persons if it can reasonably infer, based on professional judgment, that the patient does not object. Under these circumstances, for example:

* A doctor may give information about a patient’s mobility limitations to a friend driving the patient home from the hospital.
* A hospital may discuss a patient’s payment options with her adult daughter.
* A doctor may instruct a patient’s roommate about proper medicine dosage when she comes to pick up her friend from the hospital.
* A physician may discuss a patient’s treatment with the patient in the presence of a friend when the patient brings.

the friend to a medical appointment and asks if the friend can come into the treatment room.

Even when the patient is not present, or it is impracticable because of emergency circumstances or the patient’s incapacity for the covered entity to ask the patient about discussing her care or payment with a family member or other person, a covered entity may share this information with the person when, in exercising professional judgment, it determines that doing so would be in the best interest of the patient. See 45 CFR 164.510(b). Thus, for example:

* A surgeon may, if consistent with such professional judgment, inform a patient’s spouse, who accompanied her husband to the emergency room, that the patient has suffered a heart attack and provide periodic updates on the patient’s progress and prognosis.
* A doctor may if consistent with such professional judgment, discuss an incapacitated patient’s condition with a

family member over the phone.

In addition, the Privacy Rule expressly permits a covered entity to use professional judgment and experience with common practice to make reasonable inferences about the patient’s best interests in allowing another person to act on behalf of the patient to pick up a filled prescription, medical supplies, X-rays, or other similar forms of protected health information. For example, when a person comes to a pharmacy requesting to pick up a prescription on behalf of an individual he identifies by name, a pharmacist, based on professional judgment and experience with common practice, may allow the person to do so.

###### Does the HIPAA Privacy Rule permit a doctor to discuss a patient’s health status, treatment, or payment arrangements with a person who is not married to the patient or is otherwise not recognized as a relative of the patient under applicable law (e.g., state law)?

Yes. The HIPAA Privacy Rule at 45 CFR 164.510(b) permits covered entities to share with an individual’s family member, other relatives, close personal friend, or any other person identified by the individual, the information directly relevant to the involvement of that person in the patient’s care or payment for health care. In addition, HIPAA allows a covered entity to disclose information about a patient as necessary to notify or assist in the notification of (including by helping to identify or locate), such a person of the patient’s location, general condition, or death. In either circumstance, the person can be a patient’s family member, relative, guardian, caregiver, friend, spouse, or partner. The Privacy Rule defers to a covered entity’s professional judgment in these cases and does not require the entity to verify that a person is a family member, friend, or otherwise involved in the patient’s care or payment for care.

HIPAA permits a covered entity to share PHI with anyone from the list of potential recipients, subject to the conditions included at 45 CFR 164.510(b) and described below. Moreover, the list of potential recipients of PHI under 45 CFR 164.510(b) is in no way limited or impacted by the sex or gender identity of either the patient or the potential recipient.

When making disclosures to the persons listed under 45 CFR 164.510(b), a covered entity should get verbal permission from the patient when possible, or otherwise be able to reasonably infer that the patient does not object to the disclosure, before disclosing information to these persons. If the patient is incapacitated or not available, a covered entity may share information when, in its professional judgment, doing so is in the patient’s best interest. Finally, if the individual is deceased, a covered entity may share information with a person who was involved in the individual's care or payment for care prior to the individual's death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

In contrast to the permitted disclosures described above, there are circumstances in which a covered entity is required to disclose information to a family member or other person involved in an individual’s care. Specifically, in some cases, a spouse, partner, or other person involved in a patient’s care will be the patient’s personal representative and thus generally have the authority to exercise the patient’s rights under the HIPAA Privacy Rule on the patient’s behalf, such as the right to access medical and other health records as provided at 45 CFR 164.524(a). A covered entity must treat all personal representatives as the individual for purposes of the Privacy Rule in accordance with 45 CFR 164.502(g). This means a covered entity may not deny a personal representative, as defined in 45 CFR 164.502(g), the rights afforded to the personal representative under 45 CFR 164.502(g) of the Privacy Rule for any reason, including because of the sex or gender identity of the personal representative. For example, if state grants legally married spouses health care decision making authority for each other, such that legally married spouses are personal representatives under 45 CFR 164.502(g), the legally married spouse is the patient’s personal representative, and a covered entity must provide the spouse access to the patient’s records. In this example, a covered entity that does not provide a patient’s lawful spouse with access because of the sex of the spouses would be in violation of the Privacy Rule. Similarly, if a person has been granted a legal health care power of attorney for an individual that grants the person the authority to make health care decisions for the individual in a state, that person satisfies the definition of personal representative and a covered entity in that state that denies the person personal representative status because of the gender identity of the person would be in violation of the Privacy Rule.

For more information about HIPAA and Marriage, see <http://www.hhs.gov/hipaa/for->professionals/special- topics/same-sex-marriage/index.html”. More general information about when HIPAA permits disclosures to family members, friends, and others involved in a patient’s care or payment for care is available at http:/[/www.hhs.gov/hipaa/for-individuals/family-members-friends/index.html](http://www.hhs.gov/hipaa/for-individuals/family-members-friends/index.html) (for individuals) and at <http://www.hhs.gov/sites/default/files/provider_ffg.pdf>

# HIPAA Forms (Fillable PDFs)

The following forms are Fillable PDFs:

1. Business Associate Agreement
2. Certificate of Destruction
3. Authorization for Disclosure of Protected Health Information
4. Request for an Accounting of Protected Health Information Disclosures
5. Request to Amend Protected Health Information
6. Request for Restrictions of Use and Disclosure of Protected Health Information
7. Patient Request for Health Information
8. Revocation of Restrictions of the Use and Disclosure of PHI
9. Personal Representative Request
10. Privacy and Security Audit