INFORMATION SECURITY AND PRIVACY:

HIPAA Privacy Policy

Version:	10.0
Approval Date:	April 08, 2024
Approval Authorities:	PSEC

For any comments or feedback related to this Policy, please email PandSCompliance@veradigm.com.

Summary of Changes

Date	Version	Summary of Changes	Author
18-Apr-13	1.0	CPC Draft	Wright
25-Jul-14	2.0	Legal Privacy Draft	Wright/Ross
27-Oct-15	3.0	New Section 12.2 and editorial changes	Wright/Ross/Carter
7-Apr-17	4.0	Annual Review	P&S Team
12-Jun-18	5.0	Annual Review	P&S Team
29-Jul-19	6.0	Annual Review, revisions to align with other Veradigm Policies, removed redundant verbiage	P&S Team
28-Jul-20	7.0	Annual review, clarification and alignment of responsibilities, removed duplicative information and requirements covered in other Policies	P&S Team
08-Jul-21	8.0	Annual review, minor edits for clarity	P&S Team
10-Jul-22	9.0	Annual Review	P&S Team
02-Jan-23	9.1	Changed name to Veradigm, revised template	P&S Team
14-Mar-24	10.0	Annual Review, updated responsibilities, removed irrelevant requirements, updated section references	P&S Team

Approval Log

Date	Version	Approval Authority
3-May-13	1.0	PSEC
7-Aug-14	2.0	PSEC
27-Oct-15	3.0	PSEC
7-Apr-17	4.0	PSEC
12-Jun-18	5.0	PSEC
29-Jul-19	6.0	PSEC
12-Aug-20	7.0	PSEC
02-Aug-21	8.0	PSEC
29-Aug-22	9.0	PSEC
02-Jan-23	9.1	CSO & CPSC
08-Apr-24	10.0	PSEC

1.0 Contents

2.0 Purpose and Scope

2.1 Purpose

- The Veradigm HIPAA Privacy Policy implements the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, 45 CFR Parts 160 and 164, in the context of Veradigm overall business activities and obligations (both under law and contract) as a Covered Entity and a Business Associate. This Policy defines the procedures and protocols for management and Workforce members who have access to Protected Health Information (PHI) and are subject to HIPAA.
- The HIPAA Privacy Rule contains privacy and breach notification requirements that apply to PHI created, received, maintained, or transmitted by health care providers who engage in certain electronic transactions, health transactions, health plans, health care clearinghouses, and their business associates.
- The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is the Departmental component responsible for implementing and enforcing the HIPAA Rules.

2.2 Scope

- All Workforce members are required to comply with this Policy. Individuals who violate these requirements are subject to disciplinary action, up to and including termination or dismissal in accordance with the Progressive Disciplinary Action for Compliance Violations Policy.

2.3 Responsibilities

Chief Privacy & Security Counsel (CPSC):

- Ensures that requirements in this Policy are maintained in accordance with HIPAA, 45 CFR Parts 160 and 164 and any amendments and rules.

- Provides advice and consultation to Workforce members regarding the requirements in this Policy.

- Makes a determination of, including but not limited to:

    - Whether a use or disclosure of PHI is permitted and/or required by law.
    - What constitutes the minimum amount of information necessary to accomplish the intended purpose of the use, disclosure, or request.
    - Whether a Business Associate Agreement ("BAA") is required.
    - Whether a breach by a Business Associate was material, such that additional action is required.

  - Whether a requested disclosure of PHI is limited to a Limited Data Set of PHI and ensures that a valid Data Use Agreement is in place before Veradigm provides a Limited Data Set to another entity.
  - What action to take to remedy the violation of a Data Use Agreement, including the possibility of discontinuing disclosure of PHI to the recipient and/or reporting the recipient to the Secretary of the Department of Health and Human Services.

- Provides guidance on written notification to Covered Entity client when a request for access, amendment, restriction, or accounting has been received from an individual.

- Authorizes Veradigm to make requested amendments to PHI in a Covered Entity client's Designated Record Set (DRS), so long as the Covered Entity client has provided written authorization. Advises Veradigm as to the documentation required from Covered Entity clients to request amendments to PHI.

- Advises Workforce members when assistance is requested by vendors who access PHI.

- Upon receiving notice of a material breach of the obligations of the Business Associate Agreement, if a Business Associate cannot or will not take action to cure the breach and/or end the violation in a timely manner, reviews if termination of the contract is feasible and/or appropriate and makes recommendations to the General Counsel or her designee.

- Leads investigations to determine whether a privacy incident has occurred.

- Advises the company regarding appropriate action to mitigate, to the extent practicable, harmful effects that are known to Veradigm stemming from a use or disclosure of PHI in violation of this Policy and other relevant Veradigm requirements.

- Ensures that record retention and destruction information is included in the Veradigm Record Management Policy and Retention Schedule for certain documentation as required by HIPAA.

- Prior to making a disclosure pursuant to any request under HIPAA, the CPSC or his/her designee will ensure that any such disclosure meets the requirements of this Policy, verifies the terms of the BAA with the specific Covered Entity client and the identity and authority of the requestor who seeks access to the PHI.

- Directs the investigation of privacy-related complaints and ensures appropriate retention of records related to the investigation.

- Conduct a review of this HIPAA Privacy Policy and related corporate policies, standards, and procedures annually or each time there is a significant and material change in laws or regulations regarding the privacy of Sensitive Information.

- In collaboration with Human Resources, designs and ensures the provision of adequate training to all Workforce members, including to every new hire as a part of the on-boarding process, on this Policy and related policies and procedures. Ensures that the proper documentation exists to verify completion of such training by Workforce members.

- Recommends disciplinary action for any Workforce member who fails to comply with Veradigm privacy and security policies.

- May designate another individual to function in his/her capacity with regard to the requirements set forth in this Policy.

Veradigm Workforce:

- Ensures that PHI is only accessed, used, and disclosed in accordance with the Minimum Necessary requirements of applicable law and this Policy. This includes appropriate de-identification of PHI, which must be done in accordance with the Veradigm PHI Use and De-Identification Policy and Procedure.

- Consults the CPSC or other Veradigm Privacy counsel for any questions about this Policy, how to comply with this Policy, or other privacy matters.

- Reports any privacy or security incident that might constitute a violation of a Business Associate Agreement (BAA) to the CPSC, CSO, Ethics & Compliance hotline and/or Redball Incident Management Tool.

- May not use or disclose PHI other than as provided in this Policy.

- Verifies the identity and authority of persons requesting PHI from a Covered Entity client or Vendor.

3.0 Reasonable Safeguards to Protect the Confidentiality of Protected Health Information

- Veradigm provides reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy, confidentiality, integrity and availability of PHI.

- Veradigm must obtain reasonable written assurances that its Business Associates will appropriately use and disclose PHI by requiring appropriate safeguards including policies, procedures and practices.

- If Veradigm provides a Limited Data Set to another entity pursuant to a Data Use Agreement, the recipient of the Limited Data Set is required to use appropriate safeguards to prevent the use or disclosure of information in a manner other than as allowed by the Data Use Agreement.

4.0 When Business Associate Agreements are Necessary

4.1 Business Associate

- A Business Associate is a person or entity that accesses, creates, receives, maintains, or transmits PHI, or performs certain functions or activities for or on behalf of Veradigm, including, but not limited to the following:

    - Claims processing or administration
    - Data center hosting
    - Product development
    - Data analysis, processing or administration
    - Billing
    - Benefits management

- A Business Associate may also include those providing the following services to Veradigm:

    - Legal
    - Auditing
    - Actuarial
    - Accounting
    - Consulting
    - Data aggregation
    - Management
    - Administrative, accreditation or financial services

- Other types of Business Associates may include the following:

    - Health Information Organizations
    - E-prescribe gateways
    - One that offers Personal Health Records to individuals on behalf of a Covered Entity
    - Patient Safety Organizations
    - Subcontractors
    - Others that provide data transmission services and that require access to PHI on a routine basis

4.2 Use and Requirements of Business Associate Agreements

- When Veradigm requires the services of a third party, the following actions are taken:

  - Business Unit determines if the third-party will perform a function, activity or service for which the third party may have access to PHI.
  - Business Unit consults with the CPSC or Veradigm Legal counsel.
  - CPSC/Legal counsel determines whether a BAA is necessary.
  - CPSC ensures that Veradigm executes a BAA with the Business Associate and that the BAA is appropriately retained.

- BAAs must satisfy the following requirements:
  - When Veradigm contracts with a Business Associate, Veradigm must ensure that the terms meet or exceed the applicable requirements that clients have required of Veradigm.
  - Contents of the BAA are to be dictated by regulation and client contractual requirements.
  - All BAAs must have an Effective Date from at least March 23, 2013. If not, a new BAA is required.
  - All BAAs must be reviewed and approved by Privacy counsel.

4.3 Violation of Business Associate Agreement

- In the event any Workforce member becomes aware of any issue with a Business Associate that may constitute a violation or breach of the Business Associate's obligations under its contract or HIPAA, the Workforce member must report the matter as required by the Veradigm Privacy and Security Incident Response Policy.

- Veradigm shall take reasonable steps to cure the breach or to end the violation, as described below.

5.0 Disclosure and Review of Privacy Violations Committed by Veradigm or by a Veradigm Business Associate

The following actions will be taken when there is a potential violation of a BAA by Veradigm when acting as a Business Associate or by a Veradigm Business Associate:

- Upon discovery of a potential violation of a BAA, including suspected or confirmed unauthorized access, use or disclosure of PHI, the individual who discovered the potential violation (Workforce member, vendor, etc.) reports as required by the Veradigm Privacy and Security Incident Management Policy.

- CPSC investigates to determine the scope of the suspected or confirmed unauthorized access, use or disclosure and whether additional action is necessary.

- If the CPSC determines that the unauthorized access, use or disclosure was material, CPSC works with the applicable Business Unit to cure the violation and prepare any required notifications.

- If a Veradigm Business Associate fails to cure a violation or continues to violate the requirements of the BAA, the CPSC, in consultation with the General Counsel, or her designee, and other appropriate resources, may recommend contract termination or take other appropriate steps to meet Veradigm compliance obligations and appropriately protect PHI.

6.0 De-Identification of Protected Health Information

- In some circumstances, PHI can be de-identified by removing certain individual identifiers in accordance with HIPAA and can be used and disclosed without authorization.

- PHI received, maintained, created, transmitted or held on behalf of Covered Entity clients may not be de-identified without prior written authorization from the Covered Entity client.

- Business Units seeking to de-identify Covered Entity client data for internal or external purposes shall first submit a written request in accordance with the Veradigm PHI Use and De-identification Policy and Procedure.

7.0 Permitted Uses and Disclosures of Protected Health Information

- Workforce members may use or disclose PHI to support the treatment, payment or healthcare operations of Covered Entity clients, as directed by Covered Entity clients, as consistent with any applicable Business Associate Agreement, and in accordance with the provisions of this Policy or incident to such use or disclosure.

- Subject to the Minimum Necessary requirement described in this Policy, Workforce members may use and disclose PHI as follows:

    - For Veradigm quality assurance activities, so long as a client has not prohibited Veradigm from doing so;
    - As necessary for legal or financial review of Veradigm operations; and,
    - For internal administrative activities.

8.0 Disclosure of Protected Health Information as Required by Law

8.1 Requirements

- Veradigm is permitted to make disclosures of PHI without an authorization pursuant to the applicable requirements of 45 C.F.R. §164.512 including, but not limited to:

    - Disclosures about victims of abuse, neglect, or domestic violence
    - Disclosures for judicial and administrative proceedings

- Disclosure to comply with State laws requiring disclosure of PHI, as applicable

- Workforce members shall direct these requests to the General Counsel, or her designee, who determines whether the PHI may be released without an authorization.

8.2 Judicial and Administrative Proceedings / Pursuant to Process

If a requestor seeks PHI in the course of a judicial or administrative proceeding and/or pursuant to process, Workforce members shall:

- Follow Section 11.0 of this Policy, Disclosure of Protected Health Information Pursuant to Judicial or Administrative Proceedings, if the request is made by a non-governmental official.

- Follow Section 12.0 of this document, Disclosure of Protected Health Information for Law Enforcement Purposes, if the request is made by a governmental official or a person acting on behalf of a governmental official.

9.0 Disclosure of Protected Health Information for Certain Public Health Activities

- Generally, Workforce members may use or disclose PHI only in accordance with Section 7.0 of this Policy, Permitted Uses and Disclosures of Protected Health Information.

- Workforce members may disclose PHI to the following entities, without obtaining authorization from the Covered Entity client or patient:

  - A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions, or
  - At the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority.

- Such requests shall be reviewed and approved by the General Counsel, or her designee, before any PHI is shared.

10.0 Disclosures of Protected Health Information for Certain Health Oversight Activities

- As a general rule, Workforce members may not disseminate PHI other than as provided in Section 7.0 of this Policy, Permitted Uses and Disclosures of Protected Health Information, without authorization from the Covered Entity client or the patient.
- In addition, Workforce members may, with advance written authorization from Veradigm Legal Counsel as specified below, disclose PHI to a health oversight agency for oversight activities authorized by law. Health oversight agencies include agencies or authorities of the United States, a State or territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting on behalf of such public agency, that is authorized by law to oversee the healthcare system (whether public or private). Health oversight activities include, but are not limited to: audits; civil, administrative or criminal investigations; inspections; and licensure or disciplinary actions.

- All requests to Disclose PHI for Health oversight activities shall be directed to the General Counsel, or her designee, for review and response.

- Disclosures made during routine inspections for health oversight and/or accreditation purposes are included in a log of disclosures.

10.1 Compliance with Legal and Professional Standards

- Workforce members shall report conduct that may be unlawful or otherwise violates professional standards to the Chief Compliance Counsel or Ethics & Compliance hotline.

- If a Workforce member desires to report unlawful or substandard conduct to a third-party investigator or enforcement agency, such disclosure of PHI made in the context of reporting unlawful or substandard conduct does not result in violation of the requirements of this Policy, provided that:

    - The Workforce member believes in good faith that Veradigm or a Workforce member has engaged in conduct that is unlawful or otherwise violates professional standards, or that the services, or conditions provided by Veradigm or a Workforce member potentially endanger one or more patients, Workforce members, or the public, and

    - The disclosure is to:
        - A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of Veradigm,
        - An appropriate healthcare accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by Veradigm or

- An attorney retained by or on behalf of the Workforce member for the purpose of determining the legal options of the Workforce members with regard to the conduct described previously.

11.0 Disclosure of Protected Health Information Pursuant to Judicial or Administrative Proceedings

If a Workforce member receives a request for disclosure of PHI in the context of a judicial or administrative proceeding, the following actions shall be taken:

- Forward the request to the General Counsel, or her designee. Note: All such requests must be in writing.
- Counsel will determine whether Veradigm may disclose PHI without obtaining an authorization from the Covered Entity client and/or patient.

12.0 Disclosure of Protected Health Information for Law Enforcement Purposes

12.1 Law Enforcement Officials

- Law enforcement officials include officers or employees of an agency or authority of the United States, a State or a territory, a political subdivision of a State or territory, or an Indian tribe who is empowered to investigate or conduct an official inquiry into a potential violation of law, or prosecute or otherwise conduct a criminal, civil or administrative proceeding arising from an alleged violation of law.

- Requests for PHI including, but not limited to, court orders, subpoenas, search warrants, etc., from law enforcement officials shall be directed to the General Counsel, or her designee, to evaluate the request for compliance with applicable law, and respond to the request.

12.2 Law Enforcement Delay

- If a law enforcement official notifies Veradigm that an action otherwise required under HIPAA would impede a criminal investigation or cause damage to national security, the General Counsel, or her designee, shall:

    - Delay such action for the time period specified by the law enforcement official, or
    - If the statement is made verbally, the General Counsel, or her designee, shall document the statement, including the identity of the law enforcement official making the statement, and delay the notification temporarily and no longer than 30 days from the date of the verbal statement, unless a written statement as described above is submitted during that time.

13.0 Disclosure of Protected Health Information for Military or National Security Purposes

Workforce members may not disseminate PHI except as provided in Section 7.0 of this Policy, Permitted Uses and Disclosures of Protected Health Information. If Workforce members receive a request for disclosure of PHI for a military or national security purpose, such Workforce members shall direct the request to the General Counsel, or her designee, who determines whether to disclose PHI in response to the request.

14.0 Disclosure of Protected Health Information in Situations Presenting a Serious Threat to Health and Safety

In the event Workforce members receive a request for disclosure of PHI for one of the reasons below, such Workforce members shall direct the request to the General Counsel, or her designee, who determines whether to disclose PHI in response to the request.

- Abuse, neglect, or domestic violence
- Serious threat to the health or safety of the public
- Identification and location purposes (e.g., disclosure of PHI in response to a request by law enforcement for purposes of locating a missing person or a material witness)
- A crime other than abuse, neglect, or domestic violence
- Criminal conduct is suspected in the death of an individual
- A crime has taken place on Veradigm premises

15.0 Disclosure of Protected Health Information as Necessary to Comply with Workers' Compensation Laws

- When a request from State agencies or similarly situated entities pertaining to PHI purportedly necessary to resolve workers' compensation claims is received, Human Resources, in consultation with the CPSC or Employment Counsel, reviews and responds to the request.

- Workforce members may only use or disclose PHI as authorized by, and to the extent necessary to comply with, laws relating to workers' compensation or other similar programs established by law, if authorized by Human Resources.

16.0 Use of Limited Data Sets

- A Limited Data Set (LDS) is PHI that excludes the direct identifiers of the individual or of relatives, employers, or household members of the individual.

- Generally, Veradigm does not maintain LDS on behalf of its Covered Entity clients. If Veradigm does maintain a Covered Entity client's LDS, Veradigm shall agree to terms and conditions regarding maintenance of such LDS, in consultation with and with approval of the General Counsel, or her designee, in a written agreement signed by both the Covered Entity client and Veradigm.

17.0 Right to Request Additional Restrictions on the Use or Disclosure of Protected Health Information

Patients requesting restrictions on uses and disclosures of their PHI are informed that such requests must be made directly to their providers. Written requests from patients for restrictions on uses and disclosures of their PHI shall be promptly forwarded to the patient's healthcare provider. The provider is responsible for reviewing and responding to the patient's request.

18.0 Uses and Disclosures of Protected Health Information for which an Authorization is Required

- Veradigm may only use or disclose PHI about a patient if the disclosure is authorized by the Covered Entity client or, in special cases, the patient or the patient's personal representative, pursuant to an authorization form which complies with the requirements of this Policy or is otherwise permitted or required by another Veradigm procedure. Veradigm Privacy counsel must be consulted before Veradigm initiates a use or disclosure requiring the patient's authorization.
- A patient's (or personal representative's) request to access his or her own PHI is subject to Section 25.0 of this Policy, Right to Access Records, rather than the procedure outlined below.

18.1 Elements of Patient Authorization

If a use or disclosure of PHI requires a patient's authorization, Veradigm may only make the use or disclosure pursuant to an authorization written in plain language and containing the following elements:

- The authorization contains a description of the information to be used or disclosed that identifies the information in a specific and meaningful way. If Veradigm intends to use or disclose substance abuse treatment program records, information about mental health or developmental disability services, HIV/AIDS test results or other highly confidential information, the patient specifically authorizes the use or disclosure of each type of highly confidential information (e.g., by checking or initialing the appropriate box on the authorization form).

- The authorization contains the name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

- The authorization contains the name or other specific identification of the person(s), or class of persons, to whom Veradigm may make the requested use or disclosure.

- The authorization contains a description of each purpose for which PHI is to be used or disclosed. This description must be specific enough to provide a patient with the facts that he/she needs to make an informed decision whether to allow release of the PHI. The statement "at the request of the individual" is a sufficient description of the purpose only when an individual initiates the authorization and does not (or elects not to) provide a statement of the purpose.

- The authorization contains an expiration date or an expiration event that relates to the patient or purpose of the use or disclosure.

- The authorization contains a statement of the patient's right to revoke the authorization in writing and either:

    - A statement of the exceptions to the patient's right to revoke an authorization and a description of how the patient may revoke the authorization; or
    - A reference to Veradigm Notice of Privacy Practices, if the Notice of Privacy Practices describes the exceptions to the patient's right to revoke an authorization and the authorization revocation process.

- While state and federal law prohibits the re-disclosure of certain records and information, the authorization contains a statement that PHI used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and may no longer be protected by the HIPAA privacy standards.

- If the authorization is for a marketing activity and if Veradigm has received or will receive financial remuneration above its costs incurred in connection with such marketing activity, the authorization states that Veradigm is receiving financial remuneration in connection with such marketing activity.

- The authorization contains a signature of the patient or the patient's authorized personal representative and the date of the signature.

- If the authorization is signed by a personal representative of the patient, a description of such personal representative's authority to act for the patient is to be included.

- Veradigm may not disclose PHI pursuant to an authorization without first verifying the validity of the authorization form under state and federal law by consulting with Veradigm Privacy counsel.

18.2 Revocation of Authorization

A patient may revoke an authorization at any time. To revoke an authorization, the patient submits the revocation in a writing that specifies the authorization to be revoked. A revocation is effective immediately unless the patient specifies a future date in his or her written revocation. The revocation is not valid where Veradigm has already relied upon the authorization.

18.3 Documentation Requirements

The Business Unit that receives the request shall retain the original authorization from the patient or patient's representative.

18.4 Historical Patient Information

Notwithstanding the foregoing, if approved by Veradigm Privacy counsel and in accordance with contractual requirements, Veradigm may use or disclose PHI that it created or received prior to April 14, 2003 pursuant to an authorization or other express legal permission obtained from a patient prior to April 14, 2003 if:

- The authorization or other express legal permission specifically permits such use or disclosure, and
- There is no agreed upon restriction in accordance with Section 17.0 of this Policy, Right to Request Additional Restrictions on Use or Disclosure of Protected Health Information.

19.0 Uses and Disclosures of Protected Health Information for Marketing Purposes

Veradigm does not use or disclose a patient's PHI for marketing Veradigm or a third party's products or services, except in certain circumstances permissible by law. Questions regarding this section or requests for exceptions shall be directed to the CPSC.

20.0 Limitations on the Sale of Protected Health Information

Veradigm does not directly or indirectly receive remuneration in exchange for PHI from a third-party unless in accordance with this Policy.

20.1 Patient Authorization

If Veradigm wishes to enter into a relationship with a third party by which it receives remuneration in exchange for an individual's PHI, Veradigm Privacy counsel determines whether an exception set forth in the section below applies or whether an authorization from the Covered Entity client

and the patient is required. If Privacy counsel determines that an exception does not apply, Veradigm must obtain an authorization from the Covered Entity client and an authorization from the patient that permits Veradigm to receive remuneration in exchange for the patient's PHI in accordance with Section 18 of this Policy, Uses and Disclosures of Protected Health Information for which an Authorization is Required, before providing the PHI to the third party.

20.2 Exceptions Not Requiring an Authorization

- Veradigm may directly or indirectly receive remuneration in exchange for an individual's PHI without first obtaining the patient's authorization if the purpose of the exchange is one or more of the following:

    - For public health activities, as described in 45 CFR 164.512(b),
    - For research and the price charged reflects the costs of preparation and transmittal of the data for such purpose,
    - For the sale, transfer, merger, or consolidation of all or part of the Covered Entity or Veradigm with another Covered Entity, or
    - For remuneration that is provided by a Covered Entity to a Business Associate for activities involving the exchange of PHI that the Business Associate undertakes on behalf of and at the specific request of the Covered Entity pursuant to a BAA.

21.0 Minimum Necessary Protected Health Information for Routine Disclosure

21.1 Minimum Necessary Requirements

- Except as described in the next Section, Workforce members shall use or disclose only the minimum amount of information necessary to perform the payment and healthcare operations activities on behalf of Covered Entity clients or Veradigm Covered Entity activities permitted under Section 7.0 of this Policy, Permitted Uses and Disclosures of Protected Health Information.

- In determining whether the amount of PHI requested is the minimum necessary for a specific payment or healthcare operation purpose, Workforce members may rely, if reasonable under the circumstances, on statements by public officials, other Covered Entities or their Business Associates that they are requesting the minimum PHI necessary to achieve the stated purpose of the request. Workforce members also may rely on the statements of Veradigm own Business Associates or certain professionals within its Workforce (such as IT security professionals, attorneys, or internal auditors) that the information requested to provide professional services to Veradigm is the minimum necessary for such purposes.

- Workforce members may disclose the following PHI in each of the contexts described herein:

- Workforce members may disclose such information to its Business Associates as contractually agreed to between Veradigm and each Business Associate.
- In performing the following activities, also known as "standard transactions," Workforce members may disclose information contained in the standard Centers for Medicare and Medicaid Services (CMS) billing form and in mandatory or situational fields of HIPAA-required electronic transaction format (current version of National Council for Prescription Drug Programs), as may be amended from time to time:
    - Healthcare claims or equivalent encounter information
    - Healthcare payment and remittance advice
    - Coordination of benefits
    - Healthcare claim status
    - Eligibility
    - Referral certification or authorization
    - Health claims attachments

21.2 Exceptions to Minimum Necessary Requirement

The minimum necessary standard does not apply in the following circumstances:

- Disclosures to a Covered Entity client regarding the Covered Entity client's patients to the extent necessary for services and support
- Uses or disclosures made pursuant to an authorization
- Uses or disclosures made in mandatory or situational fields of a HIPAA transactions standard (e.g., those elements set forth by the National Council for Prescription Drug Programs)
- Disclosures to the Department of Health and Human Services (HHS) when required by HHS for compliance and enforcement purposes
- Uses or disclosures that are required by law

21.3 Entire Medical Record

As a general rule, Veradigm may not use, disclose or request an entire medical record of a patient unless the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

21.4 Department of Health and Human Services (HHS) Guidance

To the extent practicable, Veradigm abides by HHS guidance on what constitutes "minimum necessary" amount of PHI for a purpose once issued. Such guidance is required by the Health Information Technology and Economic and Clinical Health (HITECH) Act.

22.0 Non-Routine Disclosures of Protected Health Information

In making a determination as to whether a non-routine disclosure of PHI should be made, Veradigm Privacy counsel assesses the request based on criteria that includes the following:

- Determines who is receiving the information and the purpose for the proposed disclosure.
- Confirms that the applicable documents, including contracts, permit the requested use and/or disclosure.
- Verifies the identity or authority of the Requestor, as required by Section 29 of this Policy, Verification of Identity or Authority.
- Determines whether HHS has issued a minimum necessary guidance that is relevant to the proposed disclosure and follows the guidance, if practicable.
- Determines the minimum necessary PHI to accomplish the requested purpose under the following criteria:
    - The purpose of the request or disclosure,
    - The nature and extent of PHI requested or to be disclosed,
    - The trustworthiness of the person who receives the PHI,
    - Whether the disclosure presents a risk of financial or other harm to the patient,
    - The extent to which requested PHI can be extracted from the rest of the record without undue burden and without viewing unnecessary parts of the record, and
    - The immediacy or urgency of the need for the PHI.

In making this determination, Veradigm Privacy counsel may rely on statements, if reasonable under the circumstances:

- By public officials, other Covered Entities or their Business Associates, that they are requesting the minimum PHI necessary to achieve the stated purpose of the request
- Of Veradigm's own Business Associates or certain professionals within its Workforce that the information requested to provide professional services to Veradigm represents the minimum necessary for such purposes

23.0 Minimum Necessary Access to Protected Health Information by Job Description

- Workforce members may only access PHI that they need to perform their job functions. To the extent technically feasible, Veradigm implements technical controls and other safeguards to assure that Workforce members only access the PHI necessary for their job functions.

- Veradigm grants User IDs for accounts capable of accessing PHI only to those Workforce members who need such information to perform their job duties.

- When granting new access to PHI, Veradigm determines the proper scope of access to PHI.

24.0 Dissemination of Notice Privacy Practices

As a healthcare clearinghouse and Business Associate, Veradigm is not required by the HIPAA Privacy Rule to maintain and disseminate a Notice of Privacy Practices (see 45 CFR 164.520).

25.0 Right to Access Records

- Patients have the right, at their own expense, to receive a copy of the PHI that Veradigm maintains in a Designated Record Set (DRS), for as long as Veradigm maintains the DRS.

- Generally, Veradigm does not maintain DRS for its Covered Entity clients. All requests from patients for access to records held by Veradigm shall be forwarded directly to the Covered Entity client to respond or the patient shall be advised to contact their healthcare provider.

25.1 Granting Access to Protected Health Information

The following actions will be taken when a Covered Entity client directs Veradigm to provide access to a DRS, in whole or in part.

- Client requests Veradigm, in writing, to copy a patient's DRS.
- Client may request a copy of the DRS in electronic format and may direct Veradigm to transmit the copy to an entity or person designated by the Covered Entity client (based on the patient's request, provided that the choice is clear, conspicuous, and specific). Veradigm may impose a reasonable fee for providing a copy of the DRS.
- Veradigm provides the electronic copy of the DRS in a secure manner, via traceable means (e.g., FedEx, secure VPN with audit trail, in person with signed receipt) as the Covered Entity client has directed.

25.2 Denial of Access to Protected Health Information

The Covered Entity client determines whether a request for access from a patient will be denied. The Covered Entity client is responsible for notifying the patient if his/her request is denied. If a patient requests a review of a denial, such request for review of denial shall be promptly forwarded to the appropriate Covered Entity client for review and response.

26.0 Accounting of Disclosures

Upon request, Workforce members, in consultation with the CPSC, shall provide Covered Entity clients with a written accounting of uses and disclosures of an

individual patient's PHI made by Veradigm as required by law. However, such accounting is not required to include the following disclosures of PHI by Veradigm, if such disclosures are known to Veradigm:

- Made for treatment, payment, or healthcare operations purposes
- Made to the individual
- Made to caregivers of the individual
- Incident to a use or disclosure otherwise permitted or required by this Policy
- Pursuant to a valid authorization
- For national security or intelligence purposes
- To correctional institutions or law enforcement officials
- As part of a Limited Data Set

26.1 Logging of Disclosures

- A log of required disclosures shall be maintained. These may include disclosures made pursuant to the following sections of this Policy:
    - Section 5.0 Disclosure and Review of Privacy Violations Committed by Veradigm or a Veradigm Business Associate
    - Section 8.0 Disclosure of Protected Health Information as Required by Law
    - Section 9.0 Disclosure of Protected Health Information for Certain Public Health Activities
    - Section 10.0 Disclosure of Protected Health Information for Certain Health Oversight Activities
    - Section 11.0 Disclosure of Protected Health Information Pursuant to Judicial or Administrative Proceedings
    - Section 12.0 Disclosure of Protected Health Information for Law Enforcement Purposes
    - Section 14.0 Disclosure of Protected Health Information in Situations Presenting a Serious Threat to Health or Safety
    - Section 15.0 Disclosure of Protected Health Information as Necessary to Comply with Workers' Compensation Laws

- Such log contains information that is disclosed in an accounting, which includes the following:
    - The date of the disclosure,
    - The name of the entity or person who received the PHI and, if known, the address of such entity or person,
    - A brief description of the PHI disclosed, and
    - A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or, in lieu of such statement, a copy of a written request for disclosure, if any.

26.2 Timing of Requests

- The Workforce member who receives a request from a Covered Entity client for an accounting for a specific individual shall act on such a request no later than 30 days after receipt or as otherwise agreed to with the Covered Entity client in writing.

- Within the required time, the recipient shall provide the Covered Entity client with the accounting requested; or, if he/she is unable to provide the accounting within the time period, he/she may extend the time to provide the accounting by up to 30 days, provided that the following occur:

    - The recipient, within the time, provides the Covered Entity client with a written statement of the reasons for the delay and the date by which he/she will provide the accounting; and,
    - The recipient uses only one such extension of time for action on a request for an accounting.

26.3 Process

The Workforce member who receives a request for an accounting shall take the following actions:

- If the request is from a patient or patient's representative, the Workforce member shall direct the individual to make the request to the patient's healthcare provider.

- The recipient works with the Covered Entity client and other appropriate Workforce members to accommodate the request for an accounting in accordance with this Policy and the BAA with the Covered Entity client.

Exception: Veradigm will temporarily suspend an individual's right to receive an accounting of disclosures for the time specified by a health oversight agency or law enforcement official, if such agency or official provides Veradigm with a written statement that such an accounting would be reasonably likely to impede the agency's activities and specifies the time for which such a suspension is required. If a verbal statement is received from an agency or official, Veradigm shall: (a) document the statement, including the identity of the agency or official making the statement; (b) promptly inform the General Counsel, or her designee, of the statement; (c) temporarily suspend the right to an accounting of disclosures subject to the statement; and, (d) limit the temporary suspension to no longer than 30 days from the date of the verbal statement, unless a written statement is submitted during that time.

26.4 Content of the Accounting

- If Veradigm makes multiple disclosures during the period covered by the accounting, Veradigm provides a summary accounting to the Covered Entity client requesting the accounting on behalf of an individual.

- Multiple disclosures include the following:

    - For a single purpose to the Department of Health and Human Services for the purpose of ascertaining Veradigm compliance with the rules; or,

    - To the same person or entity for a single "national priority purpose," defined as:

        - Disclosures required by law
        - Disclosures for certain public health activities
        - Disclosures for certain health oversight activities
        - Disclosures made pursuant to judicial or administrative proceedings
        - Disclosures for law enforcement purposes
        - Disclosures for military or national security purposes
        - Disclosures deemed necessary to comply with laws governing workers' compensation, and
        - Disclosures made in situations presenting a serious threat to health or safety.

    - When a summary accounting is provided, it contains the following information:

        - The information required for the first disclosure during the accounting period,
        - The frequency, periodicity, or number of the disclosures made during the accounting period, and
        - The date of the last such disclosure during the accounting period.

26.5 Charges and Fees

Veradigm may impose a reasonable fee for each request for an accounting by a Covered Entity client.

27.0 Right to Request Amendment of Protected Health Information

If Veradigm maintains the Designated Record Set (DRS) for a Covered Entity client, Veradigm shall amend information collected and maintained about Covered Entity clients' patients in the DRS for as long as the PHI is maintained by Veradigm. Veradigm requires Covered Entity clients seeking amendment of PHI to make a

request to amend in writing and to provide reasoning to support the request. Workforce members shall, without delay, direct patients who request an amendment to either contact their healthcare provider directly or refer such requests to the Covered Entity client.

27.1 Granting an Amendment Request

The following steps will be taken when an amendment request is granted:

- Covered Entity client, in writing, submits or approves a requested amendment, in whole or in part.
- CPSC, Chief Compliance Counsel, or his/her designee directs Workforce members to make the appropriate amendment to the PHI that is the subject of the request.
- Veradigm amends the PHI or record by identifying the records in the DRS that are affected by the amendment and appends or otherwise provides directions to the location of the amendment.
- CPSC, Chief Compliance Counsel, or his/her designee directs appropriate Workforce members to inform the Covered Entity client of the completed amendment in a timely manner.

27.2 Another's Granting of an Amendment

Workforce members shall direct third party requests for an amendment of a DRS held by Veradigm to the applicable Covered Entity client. If the Covered Entity client approves an amendment to the DRS, follow process in 26.1 of this Policy.

27.3 Denying an Amendment Request

Denial of an amendment request is the responsibility of the Covered Entity and not Veradigm.

28.0 Right to Request Alternative Communications

Workforce members shall refer requests made by patients to receive disclosures of PHI by Veradigm by alternative means or at alternative locations to a patient's healthcare provider or direct the patient to submit such request directly to his/her healthcare provider.

29.0 Verification of Identity or Authority

29.1 Identity and Authority of a Public Official

29.1.1 In-Person Contact

When a public official requests PHI in person on a visit to/inspection of Veradigm, Workforce members shall require such official to present his/her agency identification in the form of a badge, other official credentials, or other proof of government status.

29.1.2 Written Statement

For requests made in writing by a public official, Veradigm shall require a written statement on appropriate government letterhead that the person requesting the PHI is acting under the government's authority. Workforce members who receive such a written statement shall forward it to the General Counsel, or her designee, without delay.

29.2 Requests Connected to a Judicial or Administrative Proceeding

Requests made pursuant to warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority and Workforce members shall process such requests in accordance with Section 11.0, Disclosure of Protected Health Information Pursuant to Judicial or Administrative Proceedings (if no State action is involved) or Section 12.0, Disclosure of Protected Health Information for Law Enforcement Purposes (if State action is involved).

29.3 Disclosures under Technical HIPAA Policy Exceptions

Workforce members shall process requests for disclosure under the following technical HIPAA exceptions in accordance with the relevant sections of this Policy or referred to Veradigm Privacy counsel for approval prior to the disclosure:

- Disclosures required by law
- Disclosures for public health activities
- Disclosures for health oversight activities
- Disclosures to law enforcement officials
- Disclosures for health or safety
- Disclosures for specialized government functions (such as military and veteran's activities, for national security and intelligence activities and for protective services for the president and others)
- Disclosures to comply with workers' compensation programs

- Disclosures to report victims of abuse, neglect or domestic violence
- Disclosures about decedents
- Disclosures to facilitate organ and tissue procurement, or
- Disclosures to correctional institutions about inmates or other individuals.

30.0 Internal Enforcement of Privacy and Security Requirements

The following describes the actions taken when a possible violation of this Policy or the Veradigm Code of Conduct has occurred:

- CPSC, CSO, or Veradigm Compliance receives a report of possible privacy and/or security violations by a Workforce member.

- CPSC, CSO and/or Veradigm Compliance shall investigate the complaint.

- Upon determination that an employee has committed a privacy and/or security violation, the CPSC, in consultation with CSO, Chief Compliance Counsel, business manager, and/or Human Resources, shall consider relevant evidence in considering what constitutes appropriate disciplinary action, including the following:

    - The work history of the employee
    - The severity of the violation
    - Veradigm general disciplinary practices

- Human Resources shall take appropriate disciplinary action in accordance with the Veradigm Progressive Disciplinary Action for Compliance Violations Policy. Employee sanctions may include, but are not limited to, the following:

    - Informal counseling
    - Verbal warning
    - Written warning
    - Suspension
    - Termination

- CPSC shall direct appropriate action to mitigate, to the extent practicable, harmful effects that are known to Veradigm officials stemming from a use or disclosure of PHI in violation of the BAA, HIPAA/HITECH, this Policy and other Veradigm requirements.

31.0 Handling Privacy-Related Complaints

- If a Covered Entity client or patient alleges that Veradigm has violated its obligations to a Covered Entity client under contract, BAA, the HIPAA Privacy Rule, or other state or federal law dealing with privacy or confidentiality of health information, Workforce members shall instruct the individual to file a

complaint with the Veradigm Chief Compliance Counsel via the Ethics & Compliance hotline from the US and Canada at 866-206-1906 or from any location using the webform at https://ethcomp.com/Veradigm.

- Upon receiving a privacy-related complaint, the CPSC, in consultation with the CSO, and/or Chief Compliance Counsel, shall undertake an investigation to determine whether a breach of privacy has occurred.

- If an unauthorized disclosure has been confirmed, CPSC, in consultation with CSO, Chief Compliance Counsel, and Human Resources shall determine appropriate disciplinary action to recommend, or other appropriate steps to mitigate any harm or otherwise remedy any issues.

- Workforce members found to be in violation of these requirements or who breach the confidentiality of a patient's PHI are subject to disciplinary action, up to and including termination or dismissal.

32.0 Training on HIPAA-Related Standard Operating Procedures

- Workforce members shall complete applicable education, training, and/or courses as defined and required by Veradigm. Any Workforce member who is required or likely to access PHI as a part of his/her job duties must complete all required HIPAA training prior to accessing PHI. The CPSC, in collaboration with Human Resources, shall direct all Workforce members to receive such training within 30 days of joining Veradigm workforce. Veradigm management shall train department Workforce members on requirements applicable to job duties.

- Managers of any Workforce member who cannot complete assigned training within the first 30 days of employment must request an exception in writing from the Chief Compliance Counsel.

33.0 Maintenance of HIPAA-Required Documentation

Veradigm shall maintain records as required by HIPAA for six (6) years. Refer to Veradigm Records Management Policy and Retention Schedule for further retention requirements.

34.0 Titles of Persons Responsible

Veradigm hereby documents the following titles of persons responsible for certain HIPAA compliance activities, as required by the Privacy Rule.

- Chief Privacy & Security Counsel
- Chief Security Officer
- Chief Compliance Counsel

35.0 Regulatory References

- 45 CFR Parts 160, 162 and 164 - Health Insurance Portability and Accountability Act ("HIPAA")
- Pub. L. No. 111-5, Title XIII - Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009 ("HITECH")
- 45 CFR Parts 160 and 164 – Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under HITECH and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule.

36.0 Definitions

For the purposes of this Policy, Veradigm adopts the definitions in 45 CFR §160.103 and 45 CFR §164.103, the HIPAA Privacy and Security Rules. In the event a definition in this Policy is in conflict with the HIPAA Privacy and Security Rules, the Rules shall take precedence.

"Business Unit" is a formally defined area of Veradigm representing a specific business function (such as Finance, Solutions Development, Sales, Support, etc.). This could be a department or subset of a department.

"Chief Privacy & Security Counsel" (CPSC) is also the Chief Privacy Officer.

"Chief Security Officer" (CSO) is the individual designated in writing to act on behalf of Veradigm for all administrative, physical, and technical security issues as defined in 45 CFR §164.308(a)(2).

"**Designated Record Set" (DRS)** is defined in 45 CFR 164.501.

"Individually Identifiable Health Information" means information, including demographic information, related to:

- an individual's past, present or future physical or mental health condition;
- the provision of health care to an individual; or,
- the past, present, or future payment for provision of health care to an individual that identifies an individual or for which there is a reasonable basis to believe that it can be used to identify an individual. Individually Identifiable Health Information includes common patient identifiers.

"Privacy Policy" refers to the Veradigm Privacy Policy that provides the framework for safeguarding and protecting Sensitive Information, including PHI for the Company.

"Protected Health Information" (PHI) means Individually Identifiable Health Information held or transmitted by a Covered Entity or its business associate, in any form or media, whether it is electronic, paper or oral.

"Sensitive Information" is a class of data, that relates to an identified or identifiable individual or entity that is sensitive, confidential, or proprietary to such person or entity and may potentially cause harm to such person or entity if lost or accessed, or used or disclosed by unauthorized persons, either internal or external to Veradigm. "Sensitive Information" includes, but is not limited to, Protected Health Information, Personal Information, Personal Health Information, Personal Data, and Personally Identifiable Information (as those terms are defined in applicable law).

"Workforce" and/or "**Workforce member"** means full-time or temporary Veradigm employees, contractors, third party users, volunteers, interns, trainees, agents, and other persons whose conduct, in the performance of work for Veradigm, is under the direct control of Veradigm, whether they are on-site or off-site, and whether or not they are paid by Veradigm.