INFORMATION SECURITY AND PRIVACY:

Privacy Policy

Version:	11.0
Approval Date:	February 18, 2025
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
7-Aug-14	2.0	Revision of entire policy to encompass international business requirements.	Ross/Wright/Carter
27-Oct-15	3.0	Technical and editorial modifications to the policy.	Ross/Wright/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	P&S Team
29-Jul-20	7.0	Annual Review, minor clarifications, updated references and regulations	P&S Team
06-Jul-21	8.0	Annual Review, clarified definition of Sensitive Information	P&S Team
28-Jul-22	9.0	Annual Review	P&S Team
02-Jan-23	9.1	Changed name to Veradigm, revised template	P&S Team
16-Oct-23	10.0	Annual review, updated relevant regulations	P&S Team
10-Jan-25	11.0	Annual Review	P&S Team

Approval Log

Date	Version	Approval Authority
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
14-Nov-23	10.0	PSEC
18-Feb-25	11.0	PSEC

1.0 Contents

2.0 Purpose and Scope

- The Veradigm Privacy Policy defines the requirements for the Veradigm Workforce to protect Sensitive Information as required under applicable laws as defined in Appendix A.

- It is the policy of Veradigm to comply with all applicable laws and regulatory requirements for the use, access and disclosure of Sensitive Information, to protect Sensitive Information, and to prevent and mitigate privacy incidents.

- All members of the Workforce shall be required to comply with this Policy, and it is applicable to Veradigm's global operations.

3.0 Exceptions

Exceptions to this Privacy Policy may be granted by the Chief Privacy & Security Counsel ("CPSC") or their designee.

4.0 Privacy Principles

Veradigm has implemented the following fair information privacy principles that support individual rights and set guidelines for the protection of Sensitive Information:

- Notice. Veradigm shall provide notice regarding its privacy policies and procedures and include the purposes for which Sensitive Information is accessed, collected, used, retained, and disclosed. Notice may occur in a variety of formats, including publication on Veradigm internal and external websites and specified in internal and external contracts and agreements.

- Choice and Consent. Where practical or required by law or contract, Veradigm shall provide individuals with opportunity to consent to or authorize Veradigm's access, collection, use, retention, and disclosure of Sensitive Information. Consent or authorization may be explicit or implicit depending upon the specific circumstances, and the CPSC shall advise the Business Units as to appropriate means of obtaining consent or authorization.

- Limited Collection. Veradigm shall collect Sensitive Information only for the purposes identified in the notice.

- Limited Use and Disclosure. Veradigm shall use and/or disclose Sensitive Information to third parties only for the purposes identified in the notice.

- Limited Retention. Veradigm shall retain Sensitive Information only as long as necessary, including, but not limited to, as may be required by law or contract, or to fulfill a valid business purpose.

- Integrity. Veradigm shall maintain the integrity of the Sensitive Information under its care.

- Right to Inspect/Correction. Individuals may request access to their Sensitive Information and request amendment to that Sensitive Information if such information is believed to be inaccurate. Veradigm shall review and respond to requests for access and amendment in a timely manner. The CPSC shall provide guidance to Business Units regarding individual rights to access and/or amend Sensitive Information upon request by the Business Unit.
- Disposal. Veradigm shall dispose of Sensitive Information at the end of the applicable retention period in a manner that prevents any likelihood of restoration of the Sensitive Information or in a manner required by law or contract.
- Training. Veradigm shall provide training to Workforce members on this Privacy Policy.
- Breach Notification. Veradigm Workforce members shall immediately report any actual or suspected breaches of Sensitive Information in accordance with the Privacy and Security Incident Reporting Policy to enable Veradigm to comply with applicable laws and to meet its contractual obligations.
- Accountability. Veradigm shall impose discipline, up to and including termination, for violations of this Privacy Policy in accordance with Veradigm Progressive Disciplinary Actions for Compliance Violations Policy.

5.0 Privacy Policy Requirements

5.1 Policy Availability

This Privacy Policy shall be made available to the Workforce through Veradigm management, the intranet, formal training programs, and other appropriate mechanisms.

5.2 Review Cycle

- The CPSC shall review the privacy requirements for the organization. The CPSC shall be responsible for conducting an annual review of this Privacy Policy and related corporate policies, standards, and procedures. The CPSC may grant an exception for an annual review of Veradigm Privacy and Security policies. A review shall also occur each time there is a significant and material change in laws or regulations regarding the privacy of Sensitive Information. The CPSC shall submit material changes or modifications to this Policy for review and approval by the Privacy and Security Executive Council (PSEC).
- Requests for changes or modifications to this Privacy Policy may be submitted by a Workforce member in writing to the CPSC. The CPSC shall determine whether the requested change or modification should be included in the Privacy Policy.

5.3 Policy Retention

- This Privacy Policy, as well as any procedures supporting this Privacy Policy, and all previous versions shall be maintained as required by the Records Management Policy and Retention Schedule.

6.0 Privacy Requirements

6.1 Executive Commitment

Veradigm executive leadership agrees that maintaining the privacy and security of Sensitive Information is essential to Veradigm business and reputation and to operating in a responsible, compliant manner. Accordingly, the Privacy and Security Executive Council approves and supports this Privacy Policy, including the designation of a Privacy Officer.

6.2 Workforce Responsibilities

Each Veradigm Workforce member is responsible for the privacy and security of Sensitive Information in his or her workspace. Workforce members shall take reasonable and appropriate precautions to safeguard Sensitive Information in accordance with Veradigm security policies, procedures and guidance.

Each Workforce member shall be responsible for:

- Reading and understanding the contents of this Privacy Policy and its related policies and procedures;
- Ensuring that his or her actions comply with the requirements of this Privacy Policy and its related policies and procedures;
- Demonstrating his or her understanding of and compliance with this Privacy Policy and its related policies and procedures through the completion of annual training and certification or through other means used by Veradigm;
- Collaborating with all levels of the Veradigm organization to ensure that an effective Privacy Program is implemented and maintained;
- Seeking assistance if uncertain how to comply with the requirements of this Privacy Policy and its related policies and procedures;
- Complying with security policies and procedures and implementing and maintaining the security program;
- Reporting any violations of this Privacy Policy, related policies or procedures or the law or regulations to one or more of the following:
    - The CPSC;
    - CSO;
    - Chief Compliance Officer;
    - Human Resources representative;
    - Veradigm management;
    - The incident reporting process as defined in the Privacy & Security Incident Response Policy; and/or
    - The Speak Freely Ethics & Compliance hotline from the US and Canada at 866-206-1906 or from any location using the webform at https://ethcomp.com/Veradigm.

6.3 Manager's Responsibility

In addition to responsibilities as a member of the Workforce, each Veradigm manager shall also be responsible for:

- Ensuring that all members of the Workforce reporting directly or indirectly to such manager have read, understand, been trained on, and comply with this Privacy Policy and its related policies and procedures;
- Ensuring all members of the Workforce who report directly or indirectly to such manager have completed the required privacy training;
- Ensuring that this Privacy Policy, and its related policies and procedures, are fully implemented in his or her functional area of responsibility; and
- Requesting guidance from Human Resources or the CPSC on implementing this Privacy Policy as a manager if needed.

6.4 Business Units and Functional Areas

In addition to responsibilities as a Workforce member, each Business Unit or functional area leader shall also be responsible for:

- Identifying any privacy-related contractual requirements mandated or requested by external clients or third-party vendors and obtaining approval for such requests from privacy counsel prior to contract execution;
- Identifying where Sensitive Information is located, and providing such information to the CPSC and/or CSO upon request;
- Approving, documenting and periodically reviewing Workforce member access to Sensitive Information and ensuring access is consistent with Workforce members' duties and responsibilities; and
- Documenting and maintaining procedures to implement this Privacy Policy within its own Business Unit.

6.5 Chief Privacy and Security Counsel

The Chief Privacy and Security Counsel shall be responsible for:

- Developing, implementing and maintaining this Privacy Policy and related policies and procedures;
- Coordinating with the CSO in the development and maintenance of security policies and programs to ensure that appropriate physical, administrative and technical safeguards are in place to protect the privacy and security of Sensitive Information;
- Upon request, providing guidance in the development of Standard Operating Procedures (SOPs) for Business Units and functions, relating to Sensitive

Information, and responding to questions regarding requirements for handling Sensitive Information;

- In collaboration with Human Resources, designing and ensuring the provision of adequate training to all Workforce members, including to every new hire as a part of the on-boarding process, on this Privacy Policy, related policies and procedures, and the privacy and security laws and regulations of applicable jurisdictions;
- Receiving and reviewing complaints related to this Privacy Policy and related procedures including documenting the complaint and disposition thereof;
- Recommending disciplinary action for any Workforce member who fails to comply with Veradigm privacy and security policies;
- Collaborating with Litigation Counsel to review and respond to requests from law enforcement and regulatory agencies related to Sensitive Information;
- Ensuring that the Veradigm Workforce has information necessary to enable compliance with applicable privacy laws, regulations, and contractual privacy requirements; and
- May designate another individual to function in their capacity with regards to the requirements set forth in this Privacy Policy.

6.6 Human Resources

Human Resources shall be responsible for:

- Together with the CPSC, designing, documenting, and enforcing a progressive disciplinary policy for non-compliance with, or violation of, this Privacy Policy and related policies and procedures;
- Ensuring that Workforce members who report violations of this Privacy Policy, related policies or procedures or the law are protected from retaliation;
- Collaborating with hiring managers to ensure privacy and security obligations are specified in Veradigm job descriptions; and
- Communicating job status changes, including termination of Workforce members, to IT Operations, so that access to systems with Sensitive Information is appropriately modified.

7.0 Permitted Uses and Disclosures of Sensitive Information

7.1 Consent and Authorization to Use Sensitive Information

- Limited Collection. Workforce members shall only collect, request, or access the minimum amount of Sensitive Information necessary to serve a valid business purpose and in accordance with the requirements of this Privacy Policy, other

applicable policies and procedures, relevant contractual requirements, and as required by law.

- Limited Use. Workforce members shall only access, use, and disclose Sensitive Information in accordance with:
    - the requirements of the consent or authorization provided by the subject or owner of the Sensitive Information;
    - the requirements of this Privacy Policy, or other applicable policies and procedures;
    - relevant contractual requirements; and
    - as required by law.

- Workforce members shall limit access, use and disclosure of Sensitive information to the minimum amount of Sensitive Information necessary to accomplish a valid business purpose.

- Workforce members shall direct requests to limit or cease using Sensitive Information to the CPSC for review.

7.2 De-Identified Sensitive Information

- In certain cases, Veradigm may receive consent or authorization to de-identify Sensitive Information for a specific purpose. In these cases, once the Sensitive Information has been de-identified, Workforce members shall use and disclose the de-identified Sensitive Information only in accordance with the consent or authorization.

- Workforce members seeking to de-identify data for internal or external purposes shall first submit a written request in accordance with the Veradigm PHI Use and De-identification Policy in order to evaluate the scope and purpose of the request and means of de-identification to ensure that applicable legal and contractual requirements are met.

7.3 Disclosures Required by Law

Veradigm may use or disclose Sensitive Information as required by law.

8.0 Privacy Risk Assessment

Veradigm shall assess Privacy Risk annually pursuant to the Veradigm Risk Management Policy.

9.0 Reporting and Managing of Privacy Complaints and Incidents

Workforce members shall follow Veradigm Privacy and Security Incident Response Policy in reporting and managing privacy complaints and incidents.

10.0 Disposal of Sensitive Information

Workforce members shall retain and properly dispose of electronic media and paper copies containing Sensitive Information in accordance with the Veradigm Records Management Policy and Retention Schedule and the Veradigm Information Classification and Handling Policy. Workforce members shall return to the client or destroy all media containing client PHI in accordance with the contractual agreement with the client.

11.0 Human Resources Privacy Requirements

- Human Resources shall ensure that Sensitive Information of Workforce members is appropriately classified and protected in accordance with this Privacy Policy, Veradigm Information Classification and Handling Policy, applicable laws, regulations, and contractual requirements.
- Veradigm operates a self-funded employee health plan for United States employees. It has contracted with one or more third-party administrators to administer this benefit plan. The employee health plan is a covered entity under HIPAA and shall comply with the requirements of the Veradigm HIPAA Privacy Policy.
- Veradigm shall provide a privacy notice to all U.S. employees who participate in the self-funded health plan and shall provide authorization and release forms to employees for the use and disclosure of Sensitive Information, including PHI.
- For countries other than the United States, Veradigm Human Resources shall protect any health-related Sensitive Information obtained as a result of providing health-related benefits to employees in accordance with this Privacy Policy, applicable laws, regulations, and contractual requirements.

12.0 Definitions

"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.

"CPSC" means the Chief Privacy and Security Counsel who is also the Chief Privacy Officer.

"CSO" means the Chief Security Officer.

"Privacy Policy" refers to this formal statement by Veradigm executive management outlining the overall intention and direction of the safeguarding and protection of PHI and other Sensitive Information for Veradigm, including, but not limited to, affiliates of Veradigm. It is not intended to be detailed, but rather to serve as a capstone principle supported by subordinate documents (including, but not limited to, privacy procedures and standards).

"Sensitive Information" is a class of regulated data that relates to an identified or identifiable individual that may potentially cause harm to such person if accessed, used or

disclosed by unauthorized persons, either internal or external to Veradigm. Sensitive Information includes, but is not limited to, Protected Health Information (PHI), Personal Information (PI), Personal Health Information, Personal Data (PD), employee data and Personally Identifiable Information (PII) (as those terms are defined in applicable law).

"Workforce" means full-time or temporary 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.

Appendix A – Applicable Regulatory Standards

Laws and regulations relevant to this Policy include, but are not limited to, the following:

- Health Insurance Portability and Accountability Act of 1996 (US)
- Health Information Technology for Economic and Clinical Health Act of 2009 (US)
- Federal Trade Commission Act (US)
- Children's Online Privacy Protection Act of 1998 (US)
- Privacy Act of 1983 (Canada)
- Personal Information Protection and Electronic Documents Act (Canada)
- Personal Information Protection Act (Alberta, Canada)
- Health Information Act (Alberta, Canada)
- Personal Information Protection Act (British Columbia, Canada)
- E-Health (Personal Health Information Access and Protection of Privacy) Act, (British Columbia, Canada)
- Personal Health Information Act (Nova Scotia, Canada)
- Personal Information International Disclosure Protection Act, SNS 2006 c.3 (Nova Scotia, Canada)
- Freedom of Information and Protection of Privacy Act (Manitoba, Canada)
- Personal Health Information Act (Manitoba, Canada)
- Personal Health Information Protection Act (Ontario, Canada)
- Health and Information Protection Act (Saskatchewan, Canada)
- Information Technology Act of 2008 (India)
- Digital Personal Data Protection Act, 2023 (India)*
- Data Privacy Act of 2012 (Philippines)
- Applicable state data protection laws (US)

*effective date still to be determined