Privacy, Security, and Confidentiality Policy

Policy Number: COM.700

Version: 04

Contact: Jodi Shegrud

Original Effective Date: 01.01.1999

Last Reviewed: 07.20.2023

Next Review/Approval Date: 07.31.2024

PRIVACY, SECURITY, AND CONFIDENTIALITY POLICY

POLICY: All Verisys employees and contractors will handle Personal, Confidential, and proprietary information in accordance with all legal, regulatory, and contractual obligations. Personal and Confidential Information is restricted to only those with a business need to know. Employees of Verisys and its associates may not disclose Confidential or Personal information to unauthorized persons or use for their own personal benefit or profit of another. Only information made public by Verisys in publications, brochures and affiliated websites may be released without proper authorization.

SCOPE: This policy applies to all Verisys employees, contractors, and business associates.

GUIDELINES: The purpose of this policy is to establish guidelines for Employees of Verisys Corporation (Verisys) and its associates with respect to the privacy, security, and confidentiality of non-public information.

Verisys is ISO/IEC 27001:2013 certified and uses the standards/controls as guidelines to manage its Information Security Management System (or process). The standards and controls establish general principles for initiating, implementing, maintaining, and improving information security management in our organization.

I. Personal Information

A. Personal Information includes, for the purposes of this Agreement, any consumer or personal information that would be protected under:

- Office of Management and Budget Uniform Administrative Requirements.
    - Protected Personally Identifiable Information (PII).
- the Health Insurance Portability and Accountability Act of 1996 (HIPAA),Public Law No. 104-191;
    - Personal Health Information (PHI).
- the Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA), Public Law No. 106-102;
    - Non-Public Personal Information (NPPI).
- the Fair Credit Reporting Act of 1971 (FCRA), Public Law No. 91-508 and
    - Consumer Reports.
- the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), Public Law No. 108-159.
    - Amended the FCRA and applies to Consumer Reports.

- the California Consumer Privacy Act (CCPA/CPRA), Cal. Civ. Law §1798.100.

II. General Privacy and Information Security Obligations:

A. Verisys will keep confidential all Personal Information contained in any submitted data set that it obtains, creates, or accesses on behalf of, or in connection with any services it provides to or for Client (the "Authorized Services").

B. Verisys will collect, create, use, store, access, disclose and otherwise handle Personal Information only as specifically authorized by, and as necessary to perform services authorized for or on behalf of the Client.

C. Verisys will implement and maintain strict data handling procedures with respect to particularly sensitive Personal Information such as, unique identification numbers,health, and financial information. Verisys does not create PHI in the course of its business. Any PHI received by Verisys is inadvertent and will be handled as described in this Policy.

D. Verisys will use appropriate administrative, technical, and physical safeguards to protect the privacy, security, confidentiality, and integrity of Personal Information in Verisys' custody or control in transit or at rest. Verisys will protect its customers' confidential information from intentional or inadvertent disclosure.

E. Verisys will ensure that all communications containing PII are encrypted and secured, including but not limited to email, fax, and phone communications.

III. Data Collection, Creation, Use and Storage:

A. Verisys will minimize the amount of Personal Information it collects, creates, uses, and stores to that which Verisys genuinely needs to perform the Authorized Services.

B. Verisys will create copies of documents and other media containing Personal Information only as necessary to perform the Authorized Services.

C. No file containing PII shall be downloaded from the Verisys SFTP site to a desktop outside of a secured connection (such as a VPN connection or zero trust network access).

D. Any file containing PII which has been downloaded must be immediately deleted upon completion of file load or file delivery.

E. System access roles and rights must be updated to adhere to the least privilege principle. This means that no individual will have access to all customer data unless it is critical to their job function and they have attested to this policy.

F. All Verisys team members must complete a monthly attestation that all PII they have access to has been deleted and removed from the Trash Bin on their desktops or laptops monthly.

G. Spot audits of download and non-network drives may be completed by the Verisys IT team by remote login to determine if PII has been stored or kept on a desktop or laptop computer.

H. An audit of internal users and levels of access shall be completed annually to ensure the least privilege principle has been maintained.

I. Verisys understands the importance of minimizing the amount of data it maintains and retains Confidential Information only as long as necessary. Verisys maintains organizational record retention procedures, which dictate the length of data retention and data destruction methods for both hard copy and electronic records. Confidential Information may reside in hard copy or electronic records; both forms of PII/NPPI fall within the scope of this policy (See Records Retention Policy).

IV. Data Access and Disclosure

A. Verisys will limit access to Personal Information, and only disclose Personal Information, to Verisys employees who need to know the information to perform the Authorized Services.

B. Verisys will not release provider credentialing data to third parties without provider authorization, unless otherwise permitted or required by law.

C. Verisys will handle requests from individuals for access, correction, portability, and erasure of their records in a timely manner.

D. Except as specified below, Verisys will not disclose Personal Information to any third party without the prior written consent of the Client.

E. Verisys may disclose Personal Information to other Verisys contractors and consultants, but only to the extent such entities or individuals:

- Need to know the information to perform the Authorized Services;
- Agree to disclose the information to need-to-know employees only; and
- Are subject to the Verisys Confidentiality Agreement.

F. Verisys will comply with these requirements in disclosing, transmitting, or providing access to Personal Information to any other person or entity.

G. Verisys will disclose to Client employees who request Personal Information only that information which is minimally necessary to fulfill the request. If the requesting individual is not Verisys' primary Client contact, Verisys will promptly notify such contact of the information request and Verisys' response to the request.

V. Information Security Requirements

A. Verisys asserts it will continually improve, develop, implement, and maintain its comprehensive data privacy and security programs.

B. Verisys asserts its privacy and security programs contain the appropriate administrative, technical, and physical safeguards to protect the privacy, security, confidentiality, and integrity of the Personal Information in Verisys' custody or control.

C. Verisys will regularly test or otherwise monitor the effectiveness of the safeguards' controls, systems, and procedures. Verisys will periodically identify reasonably foreseeable internal and external risks to the privacy, security, confidentiality, and integrity of Personal Information, and ensure that there are safeguards in place to control those risks.

VI. Administrative Obligations

A. In addition to the information security program described in Section V, Verisys will continue to develop, implement, and maintain privacy and security policies and procedures that are designed to enable Verisys to comply with any changes to the law (federal or state) or Client requirements delivered to Verisys in writing by Client.

B. At appropriate intervals or as otherwise requested by Client, Verisys will provide a copy of its written privacy and information security policies and procedures to (i) Client, and (ii) appropriate Employees, Contractors, and consultants of Verisys.

C. Verisys will conduct appropriate background investigations of Employees, Contractors, and consultants, as appropriate. No Employee, contractor or consultant shall be given access to the Personal Information until such investigation is complete and the results are acceptable.

D. Verisys will conduct privacy and information security training, as appropriate, for its employees, contractors, and consultants. The training will be conducted for all new hires and at reasonable intervals (at least annually but may be more frequent if needed) to reinforce

awareness of privacy and information security issues. Employees with ongoing access to such data will sign acknowledgement reminders annually attesting to their understanding of the privacy, security, and confidentiality requirements. This training will also include instruction on where to find this policy.

F. Verisys will require any Employee, Contractor or consultant who handles Personal Information to sign a Confidentiality Agreement.

G. Verisys will monitor all Employees, Contractors, and consultants for compliance with these guidelines. Verisys has delegated the responsibility for maintaining privacy provisions to the departments noted in this policy. Verisys' Compliance Officer shall be the sole entity named to oversee all regulatory reporting compliance issues. If any provision of this policy conflicts with a statutory requirement of international, federal, or state law governing Confidential Information, the policy provision(s) that conflict shall be superseded.

H. Verisys will promptly and thoroughly investigate allegations of any use or disclosure of Personal Information of which Verisys is aware is in violation of these guidelines and will promptly notify Client in writing of any significant violation. Upon becoming aware of a breach of this policy, the discovering employee, subcontractor and/or vendor must immediately report the breach to the Compliance Officer. In accordance with contractual and legal requirements, affected parties will be notified that their Confidential and/or Personal Information may have been compromised, and the notice will be accompanied by a description of action being taken to reconcile any damage as a result of the breach. Notices will be provided as expeditiously as possible. Where PHI is involved, the Compliance Officer will assess the impact and determine if the threshold requires reporting to federal and/or state authorities. The Compliance Officer will handle breach notifications(s) to all governmental agencies to whom such notice must be provided in accordance with time frames specified under these laws. Notices to affected individuals will be communicated by a designee of the Executive Team after consultation with the Compliance Officer and, where appropriate, outside counsel, and within the time frame specified under the appropriate law(s).

I. Verisys will promptly mitigate, to the extent practicable, any harmful effect of which Verisys is aware of any use or disclosure of Personal Information in violation of these guidelines. Infractions of this policy or its procedures will result in disciplinary action under the company's discipline policy and may include suspension or termination. Violations and disciplinary actions are incorporated in the company's onboarding and refresher training.

VII. Data Disposition

A. At appropriate intervals, unless otherwise provided in a written agreement between Verisys and Client, Verisys will (i) return to Client all documents and other media in Verisys' possession or control containing Personal Information, and (ii) purge, delete or destroy, to the extent reasonably practicable, any Personal Information that cannot feasibly be returned to Client. With respect to identical copies of documents or other media whose originals have been returned to Client, Verisys will purge, delete, or destroy such copies.

B. With respect to the disposition of Personal Information, Verisys will follow the instructions provided to it by Client to ensure that the Personal Information is appropriately purged, deleted, or destroyed. Verisys shall provide the Client with an Officer's Certificate to certify its compliance with these procedures.

VIII Social Security Numbers:

A. Verisys recognizes that a social security number (SSN) is an extremely sensitive form of Personal Information and has established the following policies regarding the specific use and handling of this information:

- Documents and/or data containing SSNs will be maintained in a secure environment as described in section 3 of this policy.
- Storage of paper documents will be maintained in locked files with access restricted to authorized personnel.
- SSNs will not be publicly posted or displayed in a manner where the SSN identifies the individual associated with the information.
- SSNs will be electronically transmitted only through encrypted mechanisms.
- Paper and electronic documents containing SSNs will be shredded and disposed of in a secure fashion.

B. SSNs as a specific form of Personal Information will be subject to each of the provisions described in this document.

DEFINITIONS:

Consumer Report: (FCRA 15 U.S.C. §1681a) any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for—

(A)credit or insurance to be used primarily for personal, family, or household purposes;

(B)employment purposes; or

(C)any other purpose authorized under section 1681b of this title.

Non-Public Personal Information (NPPI): (GLBA 15 U.S.C §6809) means personally identifiable financial information—

(i)provided by a consumer to a financial institution;

(ii)resulting from any transaction with the consumer or any service performed for the consumer; or

(iii)otherwise obtained by the financial institution.

Personally Identifiable Information (PII) (2 C.F.R. §200.1) - means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public websites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

Protected Health Information (PHI): (HIPAA 45 C.F.R. § 160.103) is broadly defined as individually identifiable health information, held or maintained by a covered entity or its business associates acting for the covered entity, that is transmitted or maintained in any form or medium. This includes identifiable demographic and other information relating to the past, present, or future physical or mental health or condition of an individual, or the provision or payment of health care to an individual that is created or received by a health care provider, health plan, or health care clearinghouse. No PII/NPPI information can be transmitted to any vendor in any method unless the vendor has been pre-certified for the receipt of such information.

Protected Personally Identifiable Information (PPII): (2 C.F.R. §200.1) means an individual's first name or first initial and last name in combination with any one or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts. This does not include PII

that is required by law to be disclosed. See also the definition of Personally Identifiable Information (PII) in this section.

AFFILIATE PROCESSES/DOCUMENTS:

Access Control Policy
Records Retention Policy
Data Classification Process

REVISIONS LOG

Approval Date	Change Summary	Reason for Change
1/1/1999	New Policy	
10/01/2019	Annual Review	Compliance
12/10/2020	Removed retired documents Added policies regarding the handling of PII and storage on personal devices List of reviewer updated	Annual Review
04/30/2021	Annual Review	N/A
04/20/2022	Annual Review - Template updated, document number changed, ownership changed, ISO 27001 reference added.	Merger
06/15/2022	Ownership change, added Office of Management and Budget Uniform Administrative Requirements under legal requirements, added definitions of protected information, added communication and training statements information from legacy policy IT-002.	Merging legacy policies to reduce duplication.
07/19/2022	Added statements and portions of the Privacy Policy (IT.1200) so specific NCQA and URAC language remains intact.	Merging legacy policies to reduce duplication.
07/20/2023	Annual Review – removed description of ISO/IEC 27002:2013, made VPN reference generic, removed bullet E in Section V as all employees receive the same privacy/security training, added Personally Identifiable Information (PII) definition, added affiliated documents.	Compliance

REFERENCES

Source	Citation

NCQA CVO	3A, 3C
URAC CORE v4.0	13 – Information Management, 15 –Information Confidentiality and Security, 16 - Confidentiality of Individually-Identifiable Health Information
URAC CVO	4 – Confidentiality 9 – Data Integrity
ISO/IEC 27001:2013	A18.1.4 -Privacy and protection of personally identifiable information