HIPAA POLICY

Policy Name	**HIPAA**
Policy Number	**CC – 002**
Version Number	**1.0**
Version Release Date	**9/28/2022**

POLICY SUMMARY

The following Policies and Procedures will govern the use and disclosure of Protected Health Information ("PHI") at Dominion Diagnostics, as well as what steps will be taken in the event unsecured PHI is breached in a manner prohibited under HIPAA. Dominion Diagnostics reserves the right to amend or change these Policies and Procedures at any time (including retroactively). These Policies and Procedures are solely for purposes of ensuring that Dominion Diagnostics employees know what is required by HITECH and HIPAA with respect to the treatment of PHI.

POLICY

Dominion Diagnostics possesses information that is sensitive and valuable (i.e., personal health information, personally identifiable information) as well as proprietary information that is required for business processes. Some information is protected by federal and state laws and/or contractual obligations that prohibit its unauthorized use or disclosure. Access to this information by unauthorized individuals could cause irreparable harm to Dominion Diagnostics or members of the community and could also subject Dominion Diagnostics to fines or other government sanctions. Additionally, if this information were tampered with or made unavailable, it could impair Dominion Diagnostics' ability to do business. Dominion Diagnostics therefore requires all employees and contracted workers to protect information, and the supporting information assets (such as computing devices and storage media) as specified within the associated information security and privacy policies and supporting procedures. All employees are required to know and follow all policies.

Access to PHI – All Dominion Diagnostics employees are authorized to access PHI to the extent the performance of their job functions reasonably requires such access and where access is necessary in furtherance of legitimate, HIPAA-approved purposes of treatment, payment, and health care operations. Employees may not access PHI except in accordance with these Policies and Procedures and only in furtherance of proper business-related activities.

HIPAA "Minimum Necessary" Standard – It is the policy of Dominion Diagnostics that all employees abide by the HIPAA Minimum Necessary Standard, i.e. that the amount and type of PHI requested, accessed, used and/or disclosed shall be limited to the "minimum necessary" information that is needed to accomplish the intended, authorized purpose of the use, disclosure or request. Use and disclosure to other authorized Dominion Diagnostics employees, plan administrators, authorized representatives of the Covered Entity, brokers and/or other business associates will be made in accordance with the Minimum Necessary Standard.

EMPLOYEE RESPONSIBILITIES

All members of Dominion's workforce who use or have access to PHI must comply with all applicable HIPAA privacy and information security policies. If after an investigation you are found to have violated the organization's HIPAA privacy and/or information security policies, then you will be subject to disciplinary action up to termination or legal ramifications if the infraction requires it.

Dominion Diagnostics Compliance Responsibilities (Purpose)

1. Protect information and system resources.
2. Help to ensure the confidentiality, integrity, and availability of information assets.
3. Establish an information security and privacy policy management and governance structure.
4. Create awareness for personnel and other workforce personnel in making information security decisions in accordance with information security and privacy policies.
5. Help protect patient, insured, customer and employee information from unauthorized use, disclosure, modification, or destruction.
6. Clarify management and other workforce personnel responsibilities and duties with respect to the protection of information assets and resources.
7. Establish the basis for internal and external audits, reviews, and assessments.

Scope

1. Dominion's information security and privacy policies define security and privacy requirements for all Dominion personnel and systems that create, maintain, store, access, process or transmits information.
2. Dominion's information security and privacy policies apply to all Dominion personnel including contracted workers, consultants, and others given access to Dominion's applications, systems, and/or information.
3. The policies pertain to all Dominion's systems, applications, and information in all forms in all locations where Dominion's business processes are performed.
4. The policies also apply to information resources owned by others, such as contractors of Dominion, entities in the private sector, in cases where Dominion has a legal, contractual, or fiduciary duty to protect said resources while in Dominion's custody. In the event of conflict, the more restrictive measures apply.
5. The policies cover Dominion's network system which is comprised of various hardware, software, communications equipment and other devices designed to assist Dominion in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connect to any Dominion domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by Dominion at its office locations or at remote locales, and the personally-owned computing devices used for Dominion purposes.
6. The policies will be maintained according to the Employee handbook.
7. The policies will be communicated to all personnel who have any type of access to business information assets.

DEFINITIONS

Common terms and acronyms that may be used throughout Dominion's information security and privacy policies include:

Secured PHI – PHI that has been rendered unusable, unreadable, or indecipherable to unauthorized individuals by either encryption or destruction by a method approved by the National Institute of Standards and Technology.

Unsecured PHI – any PHI that is not secured using one of the HHS-approved technologies or methods (encryption or destruction).

Use – the sharing, employment, application, utilization, examination, or analysis of PHI, in oral, written, electronic or another format.

Disclosure – any release, transfer, provision of access to, or divulging in any other manner of PHI to persons outside of Dominion Diagnostics.

Breach – the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed of the information poses a significant risk of financial, reputational, or other harm to the individual. The term "breach" does not include—

1. any unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate if —

    a. such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and

    b. such information is not further acquired, accessed, used, or disclosed by any person; or

    c. any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at same facility; and

    d. any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

Individual Notice – Notice provided to an individual, with respect to a breach, that is provided promptly and in the following form:

1. Written notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if specified as a preference by the individual, by electronic mail. The notification may be provided in one or more mailings as information is available.

2. In the case in which there is insufficient, or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or, if specified by the individual, electronic) notification to the individual, a substitute

form of notice shall be provided, including, in the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a period determined by the HIPAA Compliance Officer and/or Legal Counsel on the home page of the Web site of the covered entity involved or notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting will include a toll-free phone number where an individual can learn whether or not the individual's unsecured protected health information is possibly included in the breach.

3. In any case determined to require urgency because of possible imminent misuse of unsecured protected health information, in addition to notice described in (#1.), notice may be provided to individuals by telephone or other means, as appropriate.

Individually identifiable health information (IIHI) – This has the same meaning as protected health information (PHI).

Business Associate – An entity that "creates, receives, maintains, or transmits" protected health information (PHI) on behalf of a covered entity as described in § 164.308(b) of the Security Rule and § 164.502(e) of the Privacy Rule.

Electronic PHI ("ePHI") – a subset of PHI that is created, received, maintained, or transmitted in electronic format. All ePHI is Protected Health Information and is subject to the HIPAA privacy, security, and breach notification requirements.

Health Information Technology (HIT) – the term 'health information technology' means hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information.

Protected Health Information ("PHI") – information, in any format, that is created or received by Dominion Diagnostics and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a patient; and that identifies the patient or for which there is a reasonable basis to believe the information can be used to identify the patient.

Protected Health Information (PHI) – protected health information (PHI) means individually identifiable health information:

1. That is:
    a. Transmitted by electronic media;
    b. Maintained in electronic media; or
    c. Transmitted or maintained in any other form or medium.

2. PHI excludes individually identifiable health information in:
    a. Education records covered by the Family Educational Rights and Privacy Act (see definition of Education Records).
    b. Records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice.
    c. Employment records held by a covered entity in its role as employer.
    d. Regarding a person who has been deceased for more than 50 years.

3. PHI is information that is a subset of health information, including demographic information collected from an individual, and:
    a. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
    b. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
        - That identifies the individual;
        - or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

4. The following are the 19 explicitly identified PHI items:
    a. Names
    b. Addresses
    c. Geographic subdivisions smaller than a state
    d. All elements of dates directly related to the individual (Dates of birth, marriage, death, etc.)
    e. Telephone numbers
    f. Facsimile numbers
    g. Driver's license numbers
    h. Electronic mail addresses
    i. Social security numbers
    j. Medical record numbers
    k. Health plan beneficiary numbers
    l. Account numbers, certificate/license numbers
    m. Vehicle identifiers and serial numbers
    n. Device identifiers and serial numbers
    o. Web Universal Resource Locators (URLs)
    p. Internet Protocol (IP) address numbers
    q. Biometric identifiers
    r. Full face photographic images and any comparable images
    s. Genetic data that is individually unique

Additionally, any information that can be linked to a specific individual will also be considered to be PHI.

1. Information security: The preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

2. Media Notice: Notice provided to prominent media outlets serving a state or jurisdiction, following the discovery of a breach, if the unsecured protected health information of more than 500 residents of the State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during the breach.

3. Personally Identifiable Information (PII): Any piece of information, or combination of information items, that can be associated with one individual. PII items are typically considered to be those explicitly specified with any one of a number of data protection and privacy laws.

4. Personal Information: This is information that can be linked to a specific individual, group of individuals, or reveal activities or other types of characteristics of an individual or group. Many types of personal information are not explicitly protected by any law or regulation. PII is a subset of personal information.

5. Qualified Electronic Health Record: The term 'qualified electronic health record' means an electronic record of health-related information on an individual that—
    a. includes patient demographic and clinical health information, such as medical history and problem lists;
    b. and has the capacity—
        1. to provide clinical decision support;
        2. to support physician order entry;
        3. to capture and query information relevant to health care quality; and
        4. to exchange electronic health information with and integrate such information from other sources.

APPLICABLE LAWS/REGULATIONS/LEGAL REQUIREMENTS

1. Dominion must follow all HIPAA and HITECH requirements in addition to all other applicable laws, mandates, regulations and legal requirements.
2. Dominion will identify and document all legal requirements by following the Employee Handbook.

REFERENCES

https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
HIPAA § 164.306 Security standards: General rules
HIPAA § 164.308 Administrative safeguards.(a)(4)(ii)(C)Access establishment and modification
HIPAA § 164.316(a)
HIPAA § 164.316(b)(1) (includes Time Limit, Availability, Updates)
HIPAA § 164.316(b)(2)(iii)
HIPAA NIST SP 800-66 Section 4.21
NIST SP 800-66 Section 4.21
NIST SP 800-53 Security Controls Mapping RA-1, PL-1, PL-2, PL-3, RA-1, RA-3
ISO/IEC 27001: A.5 Security policy
ISO/IEC 27002: 2005 Section 5: Security Policy

VERSION HISTORY

Release Date	Revision Number	Reason for Change	Sections Affected
9/28/2022	1.0	Initial Policy Release	All