

DEPARTMENT: Information Protection and Security	POLICY DESCRIPTION: Virginia – Breach of Personal and/or Medical Information Notification
PAGE: 1 of 7	REPLACES POLICY DATED:
EFFECTIVE DATE: May 1, 2021	REFERENCE NUMBER: IP.DP.VA.010
APPROVED BY: Ethics and Compliance Policy Committee	

<p>SCOPE: All Company-affiliated facilities in the state of Virginia, including, but not limited to, hospitals, ambulatory surgery centers, imaging and oncology centers, physician practices, shared services centers and corporate departments, Groups, Divisions and Markets (collectively Virginia Affiliates).</p>
<p>PURPOSE: To provide guidance regarding workforce members' responsibility related to breach notification of personal and/or medical information and to establish the requirements for each Company-affiliated facility in Virginia of the breach notification laws as required by the Code of Virginia, Section 18.2-186.6 Breach of Personal Information Notification and Section 32.1-127.1:05 Breach of Medical Information Notification.</p>
<p>POLICY: Virginia law contains two separate breach notification laws: one for Personal Information and one for Medical Information. In the event of a Breach, all Company-affiliated facilities will comply with the requirements of these laws.</p> <p>The analysis of a potential Breach and whether notifications must be provided should be done in coordination with other breach notification laws, including the HIPAA breach notification requirements addressed at the Protected Health Information Breach Risk Assessment and Notification policy, IP.PRI.011. Both statutes provide that compliance with notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by an entity's primary or functional state or federal regulator result in compliance with Virginia law. Further, the Breach of Medical Information Notification statute provides that the law does not apply to (i) a person or entity who is a "covered entity" or "business associate" under HIPAA and is subject to requirements for notification in the case of a breach of protected health information (42 USC 17932 et seq.) or (ii) a person or entity who is a non-HIPAA-covered subject to the Health Breach Notification Rule promulgated by the Federal Trade Commission pursuant to 42 USC § 17937 et seq.</p> <p>Breach of Personal Information Notification § 18.2-186.6</p> <p>If unencrypted or un-redacted Personal Information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the Individual or Entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an Individual or Entity that owns or licenses computerized data that includes Personal Information shall disclose any Breach of the Security of the System following discovery or notification of the Breach of the Security of the System to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay.</p> <p>Notice required by the Personal Information Notification Statute may be reasonably delayed to allow the Individual or Entity to determine the scope of the Breach of the Security of the System and restore the reasonable integrity of the system. Notice required by this the Personal Information Notification Statute may be delayed if, after the Individual or Entity notifies a law enforcement agency, the law enforcement agency determines and advises the Individual or Entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without</p>

DEPARTMENT: Information Protection and Security	POLICY DESCRIPTION: Virginia – Breach of Personal and/or Medical Information Notification
PAGE: 2 of 7	REPLACES POLICY DATED:
EFFECTIVE DATE: May 1, 2021	REFERENCE NUMBER: IP.DP.VA.010
APPROVED BY: Ethics and Compliance Policy Committee	

unreasonable delay after the law enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

An Individual or Entity shall disclose the Breach of the Security of the System if Encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the Individual or Entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.

An Individual or Entity that maintains computerized data that includes Personal Information that the Individual or Entity does not own or license shall notify the owner or licensee of the information of any Breach of the Security of the System without unreasonable delay following discovery of the Breach of the Security of the System, if the Personal Information was accessed and acquired by an unauthorized person or the Individual or Entity reasonably believes the Personal Information was accessed and acquired by an unauthorized person.

An Entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of Personal Information that are consistent with the timing requirements of the Personal Information Notification Statute shall be deemed to be in compliance with the notification requirements of the Personal Information Notification Statute if it notifies residents of the Commonwealth in accordance with its procedures in the event of a Breach of the Security of the System.

An Entity that is subject to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) and maintains procedures for notification of a Breach of the Security of the System in accordance with the provision of that Act and any rules, regulations, or guidelines promulgated thereto shall be deemed to be in compliance with the Personal Information Notification Statute.

An Entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the Entity's primary or functional state or federal regulator shall be in compliance with the Personal Information Notification Statute.

The provisions of the Personal Information Notification Statute shall not apply to criminal intelligence systems subject to the restrictions of 28 C.F.R. Part 23 that are maintained by law-enforcement agencies of the Commonwealth and the organized Criminal Gang File of the Virginia Criminal Information Network (VCIN), established pursuant to Chapter 2 (§ [52-12](#) et seq.) of Title 52.

Pursuant to the enforcement duties and powers of the Office of the Attorney General, the Attorney General may bring an action to address violations of Breach of Personal Information Notification § 18.2-186.6. The Office of the Attorney General may impose a civil penalty not to exceed one hundred fifty thousand dollars (\$150,000) per Breach of the Security of the System or a series of breaches of a similar nature that are discovered in a single investigation. Nothing in the Personal Information Notification Statute shall limit an Individual from recovering direct economic damages from a violation of the Personal Information Notification Statute.

DEPARTMENT: Information Protection and Security	POLICY DESCRIPTION: Virginia – Breach of Personal and/or Medical Information Notification
PAGE: 3 of 7	REPLACES POLICY DATED:
EFFECTIVE DATE: May 1, 2021	REFERENCE NUMBER: IP.DP.VA.010
APPROVED BY: Ethics and Compliance Policy Committee	

DEFINITIONS

"Breach of the Security of the System" means the unauthorized access and acquisition of unencrypted and un-redacted computerized data that compromises the security or confidentiality, of Personal Information maintained by an Individual or Entity as part of a database of Personal Information regarding multiple Individuals and that causes, or the Individual or Entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth. Good faith acquisition of Personal Information by an employee or agent of an Individual or Entity for the purposes of the Individual or Entity is not a Breach of the Security of the System, provided that the Personal Information is not used for a purpose other than a lawful purpose of the Individual or Entity or subject to further unauthorized disclosure.

"Encrypted" means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable.

"Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities or any other legal Entity, whether for profit or not for profit.

"Financial institution" has the meaning given that term in 15 U.S.C. § 6809(3).

"Individual" means a natural person.

"Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither Encrypted nor redacted:

1. Social security number;
2. Driver's license number or state identification card number issued in lieu of a driver's license number;
3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts;
4. Passport number; or
5. Military identification number.

The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

DEPARTMENT: Information Protection and Security	POLICY DESCRIPTION: Virginia – Breach of Personal and/or Medical Information Notification
PAGE: 4 of 7	REPLACES POLICY DATED:
EFFECTIVE DATE: May 1, 2021	REFERENCE NUMBER: IP.DP.VA.010
APPROVED BY: Ethics and Compliance Policy Committee	

"Redact" means alteration or truncation of data such that no more than the following are accessible as part of the Personal Information:

1. Five digits of a social security number; or
2. The last four digits of a driver's license number, state identification card number, or account number.

Breach of Medical Information Notification § 32.1-127.1:05

If unencrypted or unredacted Medical Information was or is reasonably believed to have been accessed and acquired by an unauthorized person, an Entity that owns or licenses computerized data that includes Medical Information shall disclose any Breach of the Security of the System following discovery or notification of the Breach of the Security of the System to the Office of the Attorney General, the Commissioner of Health, the subject of the Medical Information, and any affected resident of the Commonwealth without unreasonable delay. Notice required by the Breach of Medical Information Notification Statute may be reasonably delayed to allow the Entity to determine the scope of the Breach of the Security of the System and restore the reasonable integrity of the system. Notice required by this the Breach of Medical Information Notification Statute may be delayed if, after the Entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the Entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

An Entity shall disclose the Breach of the Security of the System if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key.

An Entity that maintains computerized data that includes Medical Information that the Entity does not own or license shall notify the owner or licensee of the information of any Breach of the Security of the System without unreasonable delay following discovery of the Breach of the Security of the System, if the Medical Information was accessed and acquired by an unauthorized person or the Entity reasonably believes the Medical Information was accessed and acquired by an unauthorized person.

The Breach of Medical Information Notification Statute shall not apply to (i) a person or Entity who is a "covered entity" or "business associate" under the Health Insurance Portability and Accountability Act of 1996 (42 USC § 1320d et seq.) and is subject to requirements for notification in the case of a breach of protected health information (42 USC 17932 et seq.) or (ii) a person or Entity who is a non-HIPAA-covered entity subject to the Health Breach Notification Rule promulgated by the Federal Trade Commission pursuant to 42 USC § 17937 et seq.

An Entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the Entity's primary or functional state or federal regulator shall be in compliance with the Breach of Medical Information Notification Statute.

DEPARTMENT: Information Protection and Security	POLICY DESCRIPTION: Virginia – Breach of Personal and/or Medical Information Notification
PAGE: 5 of 7	REPLACES POLICY DATED:
EFFECTIVE DATE: May 1, 2021	REFERENCE NUMBER: IP.DP.VA.010
APPROVED BY: Ethics and Compliance Policy Committee	

DEFINITIONS

“Breach of the Security of the System” means unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of Medical Information maintained by an Entity.

Good faith acquisition of Medical Information by an employee or agent of an Individual or Entity for the purposes of the Entity is not a Breach of the Security of the System, provided that the Medical Information is not used for a purpose other than a lawful purpose of the Entity or subject to further unauthorized disclosure.

“Encrypted” means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable.

“Entity” means any authority, board, bureau, commission, district or agency of the Commonwealth or of any political subdivision of the Commonwealth, including cities, towns and counties, municipal councils, governing bodies of counties, school boards and planning commissions; boards of visitors of public institutions of higher education; and other organizations, corporations, or agencies in the Commonwealth supported wholly or principally by public funds.

“Medical Information” means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither Encrypted nor redacted:

1. Any information regarding an Individual’s medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
2. An Individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the Individual, or any information in an Individual’s application and claims history, including any appeals records.

The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

“Redact” means alteration or truncation of data such that no information regarding an Individual's medical history, mental or physical condition, or medical treatment or diagnosis or no more than four digits of a health insurance policy number, subscriber number, or other unique identifier are accessible as part of the Medical Information.

DEPARTMENT: Information Protection and Security	POLICY DESCRIPTION: Virginia – Breach of Personal and/or Medical Information Notification
PAGE: 6 of 7	REPLACES POLICY DATED:
EFFECTIVE DATE: May 1, 2021	REFERENCE NUMBER: IP.DP.VA.010
APPROVED BY: Ethics and Compliance Policy Committee	

PROCEDURE:

Notification

Notice can be a:

1. Written notice to the last known postal address in the records of the Individual or Entity;
2. Telephone notice; or an
3. Electronic notice

Notice required by this policy shall include a description of the following:

1. The incident in general terms;
2. The type of Personal Information or Medical Information that was subject to the unauthorized access and acquisition;
3. The general acts of the Individual or Entity to protect the Personal Information or Medical Information from further unauthorized access;
4. A telephone number that the person may call for further information and assistance, if one exists; and
5. If the notice is pursuant to Breach of Personal Information Notification § 18.2-186.6, advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

Substitute Notice

Substitute notice is permitted, instead of the notice described above, if the Individual or the Entity required to provide notice demonstrates that the cost of providing notice will exceed fifty thousand dollars (\$50,000), the affected class of Virginia residents to be notified exceeds one hundred thousand (100,000) residents, or the Individual or the Entity does not have sufficient contact information or consent to provide the notice described above.

Substitute notice shall consist of all of the following:

1. E-mail notice if the Individual or the Entity has e-mail addresses for the members of the affected class of residents;
2. Conspicuous posting of the notice on the website of the Individual or the Entity if the Individual or the Entity maintains a website; and
3. Notice to major statewide media.

Other Notification Requirements

In the event an Individual or Entity provides notice to more than one thousand (1,000) persons at one time pursuant to this policy, the Individual or Entity shall notify, without unreasonable delay, the Office of the Attorney General and (1) if a breach of Personal Information, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a

DEPARTMENT: Information Protection and Security	POLICY DESCRIPTION: Virginia – Breach of Personal and/or Medical Information Notification
PAGE: 7 of 7	REPLACES POLICY DATED:
EFFECTIVE DATE: May 1, 2021	REFERENCE NUMBER: IP.DP.VA.010
APPROVED BY: Ethics and Compliance Policy Committee	

(p), and (2) if a breach of Medical Information, the Commissioner of Health, of the timing, distribution, and content of the notice.

In addition, for Breach of Personal Information Notification § 18.2-186.6, any employer or payroll service provider that owns or licenses computerized data relating to income tax withheld pursuant to Article 16 (§ [58.1-460](#) et seq.) of Chapter 3 of Title 58.1 shall notify the Office of the Attorney General without unreasonable delay after the discovery or notification of unauthorized access and acquisition of unencrypted and un-redacted computerized data containing a taxpayer identification number in combination with the income tax withheld for that taxpayer that compromises the confidentiality of such data and that creates a reasonable belief that an unencrypted and un-redacted version of such information was accessed and acquired by an unauthorized person, and causes, or the employer or payroll provider reasonably believes has caused or will cause, identity theft or other fraud. With respect to employers, this subsection applies only to information regarding the employer's employees, and does not apply to information regarding the employer's customers or other non-employees.

Such employer or payroll service provider shall provide the Office of the Attorney General with the name and federal employer identification number of the employer as defined in § [58.1-460](#) that may be affected by the compromise in confidentiality. Upon receipt of such notice, the Office of the Attorney General shall notify the Department of Taxation of the compromise in confidentiality. The notification required under this subsection that does not otherwise require notification under the Breach of Personal Information Notification Statute shall not be subject to any other notification, requirement, exemption, or penalty contained in the Breach of Personal Information Notification Statute.

REFERENCES:

1. VA. Code section 18.2-186.6 Breach of Personal Information Notification
2. VA. Code section 32.1-127.1:05 Breach of Medical Information Notification
3. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Standards for Notification in the Case of Breach of Unsecured Protected Health Information, 45 CFR Parts 160 and 164
4. Protected Health Information Breach Risk Assessment and Notification, [IP.PRI.011](#)