POLICY & PROCEDURE Data Governance and Data Classification		POLICY #22
SUPERCEDES POLICY:	**EFFECTIVE:**	**LAST REVIEWED:**
Privacy and Security Compliance Program Security Policy 22 v.2 Data Governance and Data Classification	11/13/2020	**5/10/2024**

Purpose

To establish a classification schema to differentiate between various levels of sensitivity and value, to implement suitable procedures for handling different data classifications to ensure the confidentiality, integrity, and availability of the data; and to ensure that users of information systems are notified and made aware when the data they are accessing contains PHI.

To issue and implement guidelines on the ownership, classification, retention, storage, handling, and disposal of all records and information.

Consult with Legal Counsel for any applicable state security or breach laws with respect to matters governed by this policy and procedure to determine any additional requirements. Other federal laws may also apply.

Applicability

All Watershed Workforce members are responsible for awareness of this policy and adherence to the given direction and guidance.

Definitions

For definitions of capitalized terms or phrases, please refer to *Privacy, Security and Breach Notification Glossary*.

Policy

It is the policy of Watershed to (i) implement a classification schema that defines the various levels of data sensitivity; and (ii) to notify users of information systems when the data they are accessing contains PHI.

Procedures

1) Data created or used within Watershed will be identified and classified to belong to one of the following four categories: **Low-Sensitive, Sensitive, Confidential (sensitive information intended for limited business use)**, or **Extremely sensitive**. Definitions of these four categories are found below, and the Data Classification and Handling Checklist can be found on the Staff Website.

   a) Level 1: Low-sensitive information.

(1) Low-sensitive information is data that is not protected from disclosure, that if disclosed will not jeopardize the privacy or security of employees, clients, and partners. This includes information regularly made available to the public via electronic, verbal, or hard copy.

b) Level 2: Sensitive information.

(1) Sensitive information is data that may not be protected from public disclosure but, if made easily and readily available, the organization follows its disclosure policies and procedures before providing this information to external parties.

c) Level 3: Confidential information (sensitive information intended for limited business use).

(1) Confidential information (Sensitive information intended for limited business use) is data that can be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of employees, clients, or partners.

d) Level 4: Extremely sensitive information.

(1) Extremely sensitive information is data that is deemed extremely sensitive and intended for use by named individuals only. This information is typically exempt from public disclosure.

2) General Information and Responsibilities.

a) The Security Officer or designee will be responsible for oversight of this policy and will designate specific Workforce members who will be responsible for implementation and monitoring of compliance for data classifications, technical requirements, and handling of data based on the classifications.

b) The Security Officer or designee will maintain an inventory of where, and in whose custody, the Confidential and Extremely Sensitive Information are stored, to include any hardcopy Confidential or Extremely Sensitive material and records (if available) as part of the risk analysis procedures.

c) All access, physical and remote, to Confidential and Extremely Sensitive data must be reviewed at least annually, and the inventory updated at the end of the review as part of the risk analysis procedures.

d) Department Supervisors/Managers must be aware of all Confidential and Extremely Sensitive data being created, handled, or otherwise in the custody and control of their designated area of responsibility.

e) All Watershed's Workforce members must be familiar with the data classifications covered in this policy. As such, any Workforce member that creates the content must ensure that the content is assigned a suitable classification and that the content is labeled appropriately for the data classification (*See* Data Handling and Labeling section below). Each user that accessing information systems must be notified and made aware when accessing data containing PHI.

f) Workforce members must immediately report any loss, theft, or unauthorized access of Confidential and/or Extremely Sensitive information to their Supervisor and Security Officer or designee..

g) The *Reporting and Assessment Form* will be completed to document any loss, theft, or unauthorized access of Confidential and/or Extremely Sensitive information.

3) Technical and Administrative Requirements. Watershed's information assets must be secured and labeled in a manner appropriate to the assigned classification.

a) Administrative Requirements

i) Low-sensitive information.

(a) Data of this classification requires no special handling requirements.

ii) Sensitive information

(a) This Security Officer or designee shall determine what, if any, special requirements or procedures are required prior to providing data of this classification to external parties.

iii) Confidential information (sensitive information intended for limited business use)

(a) Data of this classification requires special care.
(b) Workforce members must have a business need before any data in the Confidential category can be downloaded or transmitted out of Watershed's environment. Refer to *Security Policy #3, Workforce Security*.
(c) Special labeling requirements. Refer to Section 4 below for examples of special labeling that may be used.
(d) Special copying or printing requirements apply (refer to Section 5 below).
(e) Special procedures related to media handling and destruction – Paper and Electronic Media apply (Refer to Sections 6 and 7 below).

iv) Extremely sensitive information

(a) Data of this classification requires the highest level of special care.

(b) Extremely Sensitive data is prohibited from being downloaded or stored to a Workforce member's workstation; transferred to a removable device (CDs, USB drives etc.); or transmitted out of Watershed's environment without the appropriate level of encryption and proper approval.

(c) Special labeling requirements. Refer to Section 4 below for examples of special labeling that may be used.

(d) Special copying or printing requirements (refer to Section 5 below).

(e) Special procedures related to media handling and destruction – Paper and Electronic Media apply (Refer to Sections 6 and 7 below).

b. Technical Requirements

Refer to *Appendix 2* for specific technical requirements.

4) Additional markings or caveats may be necessary to comply with regulatory or heightened security requirements. Examples include, but are not limited to the following:
   a. CONFIDENTIAL & PROPRIETARY
   b. MAKE NO COPIES
   c. THIRD PARTY MANAGEMENT CONFIDENTIAL
   d. ATTORNEY-CLIENT PRIVILEGED DOCUMENT
   e. DISTRIBUTION LIMITED TO ______
   f. COVERED BY A NON-COMPETE AGREEMENT
   g. This list contains confidential and proprietary information and is the property of Watershed, to which it must be returned. It must not be reproduced or distributed without prior written consent of Watershed.
   h. Property of [Owner]. Must not be disclosed or made available to third parties. Must be returned to [Owner].
5) Special copying and printing.
   a) Watershed Confidential or Extremely Sensitive copying (electronic):
      i. Do not make electronic copies unless specifically permitted by the owner or custodian of the information or in the performance of job functions.
   b) Printing.
      i. Unattended printing is permitted only if physical access controls are used to prevent unauthorized persons from both entering the area around the printer and viewing the material being printed.
      ii. Printers must not be left unattended if the information is being printed or will soon be printed.
6) Special procedures related to data handling and destruction – Paper.
   a) Handling.
      i. Hardcopies of documents classified Confidential and Extremely Sensitive must be physically secured at all times.
      ii. Non-Watershed information will be protected according to the terms of such contracts or agreements (including non-disclosures).

iii. When the media is transported off-premises, it must be approved by the management. Additionally, a mechanism or procedure must exist to verify and record that all media arrived, were received, and stored securely at the receiving location.

b) Destruction.

i. When the hardcopies of documents are no longer required to be retained, the workforce member will be responsible for shredding the documents or disposing of in a HIPAA compliant manner.

7) Procedures related to media handling and destruction – Electronic Media.

a) Destruction.

i. If possible, the media must be physically destroyed by some process such as grinding and crushing or by a chemical process such as burning or acid treatment in accordance with *Security Policy #13, Device and Media Controls*.

ii. Prior to going off-lease, being sold, moved around within the company, or being given away, computer systems', copiers', printers', other devices' hard drives must be processed to overwrite the entire hard drive with random data or a fixed pattern to prevent recovery of the data, in accordance with *Security Policy #13, Device and Media Controls*.

b. Specific authorized methods for electronic media disposal are provided in in accordance with *Security Policy #13, Device and Media Controls*.

Enforcement

Violations of this policy will result in imposition of sanctions in accordance with Watershed sanctions policy. This may include suspension or loss of the violator's use privileges, with respect to Watershed's information systems, termination of employment or volunteer, intern, contractor status with Watershed. Additional civil, criminal and equitable remedies may apply.

Documentation

The Security Officer or designee is responsible for ensuring this version of the policy, together with any forms and other documentation created or obtained in accordance with the policy, will be retained by Watershed for a period of at least 6 years plus the current year from the date of creation or the date when last in effect, whichever is later.

References

Regulatory Authority:

No specific regulatory standard or implementation specification listed in HIPAA.

Internal:

1. Security Policy #3, Workforce Security

2. Security Policy #13, Device and Media Controls

External:

1. Current Administrative Simplification Regulations
2. Refer to NIST Low Sensitive Information Reference Guide for specific guidance

Appendix 1: Data Types and Classifications

Below is a list of data classifications and types of information associated with the classification. This is not an all-inclusive list. System Owners should consult with the Security Officer when associating a data type with a specific classification.

1. **Low Sensitive Information and Sensitive**
   - a. Press releases
   - b. Watershed's commercials
   - c. Advertising and other promotional materials
   - d. Watershed's internet sites (Low Sensitive Information or Sensitive facing) (i.e., www.watershedhealth.com)
   - e. Any other information in the Low Sensitive Information and Sensitive domain and/or not classified as Confidential or Extremely Sensitive
2. **Confidential**
   - a. Data of this classification requires special care (may be less rigorous than for Extremely Sensitive) during its lifecycle (i.e., the methods by which the data is created, received, maintained, transmitted, protected, stored, accessed, and disposed).
   - b. Workforce members must have a clear business need before any data in the Confidential category can be downloaded to one's desktop, laptop, transferred to a removable device or media (CDs, USB drives etc.) or transmitted out of Watershed's environment. The following are the five (5) categories of confidential classification, including specific examples.
     - i. Customer Personally Identifiable Information (PII)
       - (1) Name (first, last, or middle)
       - (2) Address (street, Post Office [PO] Box, city, state, or zip code)
       - (3) Phone number
       - (4) Personal Mobile phone number
       - (5) Customer account number
       - (6) E-mail address
       - (7) Any other personally identifiable information (PII)
     - ii. Employee and Personal Information
       - (1) Employee performance reviews
       - (2) Employee Age
       - (3) Employee timesheets

(4) Internal contact information (including Watershed-provided phone numbers and e-mail addresses)

(5) User ID

(6) Salary

iii. Company Information

(1) Corporate account number

(2) Corporate payments (e.g., checks, etc.)

(3) Watershed’s policies and standards

(4) Watershed’s procedures

(5) Watershed’s Organization Charts

(6) Merger & acquisition documents

(7) Non-Low Sensitive Information or non-Sensitive audit report

(8) Project documentation

(9) Strategic business plans

(10) Tax ID number

iv. Company’s Financial Information

(1) Budgets

(2) Contracts

(3) Gain/Loss data

(4) Invoices

(5) Customer contact information

(6) Staffing plans

(7) Non-Low Sensitive Information or non-Sensitive Financial Statements

v. Any other Company Information expressly labeled as Confidential

3. **Extremely Sensitive**

a. Data of this classification requires special care during its lifecycle (i.e., the methods by which the data is created, received, maintained, transmitted, protected, stored, accessed, and disposed).

b. The following are the five (5) categories of Extremely Sensitive classification, including specific examples.

i. Protected Health Information (PHI) including ePHI - Any PHI that is created, maintained, stored, accessed, transmitted or received electronically. PHI under HIPAA means any information that identifies an individual and relates to at least one of the following:

(1) The individual's past, present or future physical or mental health.

(2) The provision of health care to the individual.

(3) The past, present or future payment for health care.

Information is deemed to identify an individual if it includes any of the following 18 information attributes that could enable someone to determine the individual's identity, as listed below:

(1) Name

(2) Address (all geographic subdivisions smaller than state, including street address, city, county, zip code)

(3) All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death and exact age if over 89)

(4) Telephone numbers

(5) Fax number

(6) Email address

(7) Social Security number

(8) Medical record number

(9) Health plan beneficiary number

(10) Account number

(11) Certificate/license number

(12) Any vehicle or other device serial number

(13) Device identifiers or serial numbers

(14) Web URL

(15) Internet Protocol (IP) address numbers

(16) Finger or voice prints

(17) Photographic images

(18) Any other characteristic that could uniquely identify the individual

ii. Company Information

(1) Intellectual property

(2) Network diagrams that contain any one of these data types:

(a) Hostname

(b) Internet Protocol (IP) address

(c) Hardware manufacturer

(3) Risk assessments

iii. Credit or Debit Card Data

(1) Full Primary Account Number (PAN) (Note: First 6 or last 4 digits may be displayed as required for specific business purposes)

(2) Cardholder name

(3) Expiration date

(4) Service Code

(5) Card validation code (CVC) 1, CVC 2, CVC 3 (Not to be stored after payment authorization)

(6) Personal Identification Number (PIN) (Not to be stored after payment authorization)

(7) Track 1 data, Track 2 data (Not to be stored after payment authorization)

(8) Magnetic stripe data (Not to be stored after payment authorization)

iv. Cryptographic Keys

(1) Application keys

(2) Database keys

(3) Hardware keys

(4) Key components

(5) PIN keys

(6) Secure Sockets Layer (SSL) keys

(7) Software keys

v. Passwords

(1) Passwords

(2) PINs

(3) Passphrases

(4) Verification phrases (for passwords)

vi. Employee Personally Identifiable Information (PII)

(1) Date of birth

(2) National ID number (Social Security Number [SSN] or other)

(3) Passport number

(4) State ID number (Driver’s License)

(5) Background checks

Appendix 2: Technical Requirements of Watershed Devices

Technical Controls				
Systems or applications	**Low Sensitive Information**	**Sensitive**	**Confidential**	**Extremely Sensitive**
Unique user identification				
Assign a unique name and/or number for identifying and tracking user identity			X	X
Automatic Logoff				
Terminate an electronic session after a predetermined time of inactivity (30 minutes)			X	X
To restart session User must re-enter password or other authentication method (biometric/facial recognition			X	X
Encryption and decryption				
Mechanism to encrypt and decrypt electronic information				X
Process for managing the cryptographic keys used to encrypt electronic information on Watershed's information systems				X
Audit controls				
In-house information system activity review				X
Intrusion protection system to monitor, track, and prevent unauthorized access to the network or applications				X
Retention of audit logs with findings				X
Integrity				
Mechanism to protect electronic information from unauthorized alteration or destruction and to authenticate the integrity of electronic information				X
System Security				

Electronic documents				
Do not store on device without password protection		X	X	X
Do not store on device without encryption		X	X	X
End User devices and telecommuting				
Desktops and laptops require a password at least 8 characters in length or biometric			X	X
Terminate an electronic session after a predetermined time of inactivity (30 minutes)			X	X
To restart session User must re-enter password or other authentication method (biometric/facial recognition)			X	X
Encrypt device if it stores this classification			X	X
Devices must have appropriate anti-virus or malware solutions installed			X	X
Devices must have software and patch updates implemented in a timely manner			X	X
Firewall appliance or software deployed for telecommuting			X	X
Utilize HTTPS or Virtual Private Network (VPN) when telecommuting			X	X
Email				
Encrypt message in transit			X	X

Document Control

APPROVED BY:		
Lisa Stanley	5/28/2024	DocuSigned by: Lisa Stanley 9418DCC7CF3D47D...
(Printed Name)	**(Date)**	**(Signature)**

REVISION HISTORY			
Date	**Author**	**Version**	**Comments**
11/13/2020	Scott Snodgrass	1.0	Implemented by Privacy & Security Officer
11/11/2021	Lisa Stanley	1.0	Reviewed
5/20/2022	Lisa Stanley	1.0	Reviewed
5/17/23	Nicole Montagnet	2.0	Reviewed and updated by Privacy & Security Officer
5/10/2024	Nicole Montagnet	3.0	Reviewed and updated by Privacy & Security Officer