Advocate Health Advisors

PRIVACY & SECURITY POLICY

Reviewed Annually

Privacy Official/Officer: Joshua Houchens,
Joshua.houchens@advocatehealthllc.com

Compliance Officer: Alissa Morris,
compliance@advocatehealthllc.com

ADVOCATE HEALTH ADVISORS

PRIVACY & SECURITY POLICY

TABLE OF CONTENTS

- Confidentiality/Non-disclosure Agreement
- Business Associate Agreement

Individual Privacy Right

Privacy & Security Procedures & Guidelines

- Reporting a Privacy & Security Breach
- Return / Destruction of Information
- HIPAA Privacy & Security Training Program
- Performing Authentication
- Minimum Necessary Guidelines
- Responding to Individual Privacy Rights

Regulatory Reference

PRIVACY & SECURITY POLICY SCOPE & FOCUS

Advocate Health Advisors adopts the following privacy and security policy. This document is the formal written policy regarding the protection and security of information as required by federal and state laws, rules and regulations. All associates of this agency are required to follow the guidance provided in this policy. This policy also applies to any temporary associates, all contractors, vendors and any others who are provided access to this agency's data and systems. Associates who violate or fail to comply with this policy are subject to disciplinary actions and may also be subject to civil penalties.

This policy applies to oral, written and electronic individually-identifiable health information, and non-public personal information. The information protected applies to individuals, members, clients, agents, brokers, employer groups, providers, and vendors including person(s) who are deceased. The scope of protected information by this policy includes all requirements as indicated in agreements with covered entities. The terms of this policy will continue to apply in the event the agency no longer does business.

This agency will follow all Federal and state laws and regulations. In the event of conflicting regulations, this agency will follow the most stringent requirement or seek assistance from legal counsel.

The contents of the following privacy and security policy include: definitions of terms used frequently in the privacy and security regulations, information on how our agency uses and discloses protected health information, provides information on the various safeguards in place to protect information, agreements between the agency and its employees, the agency and its vendors and sub-contractors, and the agency and the covered entity, definitions of individual privacy rights, and privacy and security procedures and guidelines.

DEFINITIONS

The following are terms commonly used within the Federal HIPAA Privacy and Security rules. Familiarity with these terms will assist in your overall understanding of the Privacy rule and Business Associate requirements.

Access - means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Administrative Safeguards - this term is used to define the administrative actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect information.

• The agency performs a documented, organization-wide risk analysis and risk management process at least annually and upon significant changes, aligned to NIST SP 800-66 Rev. 2 guidance.

• Annual phishing-resistant security awareness training is required for all workforce members, with additional role-based training for administrators and personnel handling ePHI or nonpublic financial information.

• Incident response and disaster recovery plans are tested (e.g., tabletop exercises) at least annually; lessons learned are tracked to closure.

• Recognized Security Practices: The agency documents and maintains recognized security practices for at least the preceding 12 months pursuant to the HITECH Act; OCR may consider these during enforcement.

American Recovery & Reinvestment Act of 2009 - ARRA, commonly referred to as the **Stimulus** or **The Recovery Act** is an economic stimulus package enacted by the 111th U S Congress in February 2009. The act included specific healthcare incentives.

Authentication - process used to verify the identity of a person whose protected health information is being requested, and the authority of the requester to access that person's protected health information.

Authorization - document that gives Covered Entities the permission to use or disclose Protected Health Information for specific purposes, typically for reasons other than treatment, payment or health care operations.

Breach - the unintentional or unauthorized release of Protected Health Information.

Business Associate - a person or organization that performs certain functions or activities that involve the use or disclosure of Protected Health Information on behalf of a Covered Entity.

Business Associate Agreement - an agreement mandated by the Privacy rule between a Covered Entity and a business associate providing services involving Protected Health Information.

Complaint - any concern or expression of dissatisfaction regarding privacy issues of protected information.

Confidentiality - means the property that data or information is not made available or disclosed to unauthorized people or processes.

Confidentiality Agreement (Non-disclosure Agreement) - executed contract which requires a third party to safeguard protected health information.

Covered Entity - as defined by federal Privacy regulation:

- Health Care clearing houses – public or private organizations that process or facilitate the processing of data elements of health information received from other covered entities, including billing services.
- Health Plans – individual or group plans that provide, or pay the cost of, medical care, including group health plans, HMOs, etc.
- Health Care Providers – physicians or other health care providers, licensed, accredited, or certified to perform specific health care services.

De-identification - is the process of removing key identifiers from an individual's protected health information so that the remaining information no longer identifies the individual, and the information cannot be re-identified to the individual.

Disclosure - is the act of releasing, transferring, divulging, or providing access to protected health information to an organization other than the Covered Entity maintaining the information.

Electronic Health Record - EHR is a systematic collection of electronic health information about individual patients.

Encryption - means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Financial Information - as defined in Gramm-Leach-Bliley regulations, term pertains to elements such as bank account numbers, routing numbers and loan numbers.

Gramm-Leach-Bliley Act (GLBA) - federal law passed in 1999 that includes provisions to protect consumer's personal financial information and governs the collection and disclosure of their financial information.

Health Insurance Portability and Accountability Act (HIPAA) Title II - Administrative Simplification – federal law containing administrative provisions for health plans, providers,

and health care clearinghouses. The privacy portion of the law, designed to ensure the privacy of protected health information became effective April 14, 2003.

HITECH Act - part of **ARRA. ARRA** contains specific healthcare incentives including information on enforcement of privacy and security, breach notification requirements, electronic health record access and additional impacts to Business Associate agreements.

Incidental Disclosure - secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a by-product of an otherwise permitted use and disclosure.

Individual - Individual means the person who is the subject of Protected Health Information.

Individually Identifiable Health Information - any information that may identify an individual and relates to the past, present, or future mental or physical condition of the individual. For example, a name, address, telephone number, birth date, or Social Security number in combination with a diagnosis or other health-related information.

Individual Privacy Rights - according to HIPAA Title II regulations, individuals are entitled to individual privacy rights that include the following items:

- Right to Notice of Privacy Practices
- Right to Restrictions on Use and Disclosure of Protected Health Information
- Right to Alternate Communications
- Right of Access to Protected Health Information
- Right to Amend Protected Health Information
- Right to an Accounting of Disclosures of Protected Health Information
- Right to file a privacy complaint

Information system - means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity - means the property that data or information have not been altered or destroyed in an unauthorized manner.

Malicious software - means software, for example, a virus, designed to damage or disrupt a system.

Minimum Necessary Standard - is the practice of limiting the amount of information to the minimum amount of Protected Health Information necessary to accomplish the intended purpose of the Use or Disclosure.

Nonpublic Personal Information - "personally identifiable information" is information about a consumer which is provided by the individual to obtain a product or service.

Non-Routine Disclosure - disclosure of protected health information is a disclosure that does not ordinarily happen in routine operations or on a recurring basis.

Notice of Privacy Practices - a document required by the HIPAA Privacy rule that health care providers and health plan operations must provide individuals to inform the individual of their privacy rights and explains how their organization uses & discloses their Protected Health Information.

Password - means confidential authentication information composed of a string of characters.

Privacy Officer- the person designated to develop, implement, and oversee the entity's compliance with the HIPAA Privacy Rule.

Physical safeguards - are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Protected Health Information (PHI) - as defined by federal privacy regulation is information that:

- Contains data elements or combinations of data elements that could identify a person or provides a reasonable basis to believe someone could be identified.
- Contains health-related information about that person; and
- It is maintained or transmitted in any form (electronic, written, or oral).

Routine Disclosures - is a disclosure of protected health information that ordinarily happens in payment and health plan operations, or on a recurring basis.

Safeguards - processes and procedures to provide protection of PHI using administrative, physical and technical methods.

Sanction - penalty for non-compliance.

Security or Security measures - encompass all the administrative, physical, and technical safeguards in an information system.

• Phishing-resistant multi-factor authentication (MFA) is required for all remote access, email, and administrator/privileged accounts. (Essential HPH CPGs).

• Strong encryption (in transit and at rest) is required for systems storing or transmitting ePHI or nonpublic financial information; encryption keys must be protected and stored separately.

• Endpoint Detection & Response (EDR)/anti-malware protections are deployed to all workstations and servers handling agency data; alerts are centrally monitored.

• Centralized log collection and retention is implemented for security-relevant systems to support incident detection and investigation (Enhanced HPH CPGs).

• Network segmentation is implemented to limit lateral movement and to isolate sensitive systems.

• Zero Trust principles are progressively adopted (least privilege, continuous verification, and segmentation) for user, device, and application access.

• Use of generative AI or automated tools with PHI or nonpublic personal information is prohibited unless expressly approved by the Privacy & Security Official and protected by a signed BAA with technical safeguards (no public/consumer AI tools).

• All third-party connections handling PHI or nonpublic personal information must meet vendor/supplier cybersecurity requirements, including MFA, encryption, and incident reporting obligations per executed agreements.

Security Incident - means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Technical Safeguards - security controls, safeguards and counter measures applied to an information system.

TPO - term that stands for treatment, payment and health care/plan operations.

Transaction - means the transmission of information between two parties to carry out financial or administrative activities related to health care.

Treatment - means the provision, coordination, or management of health care or health care related services by one or more health care providers.

US Department of Health and Human Services - The Department of HHS responsible for the enforcement and administration of HIPAA law.

Use - is the sharing, Use, examining, or analysis of Protected Health Information within a Covered Entity that maintains that information.

User - means a person or entity with authorized access.

Workforce - term for employees, volunteers, trainees, and other people who perform work for a Covered Entity.

Workstation - means an electronic computing device, for example, a lap or desk computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

USES AND DISCLOSURES OF INFORMATION

This agency may use and disclose protected health information (referred to in this policy as PHI) as described in the Federal HIPAA Privacy regulation, 45 C.F. R. §164.501 and as outlined in this Policy.

Permitted & Required Uses and Disclosures – This agency is allowed to use and disclose any protected health information for the following purposes. Refer to the Privacy Officer or obtain assistance from legal counsel for other allowed uses and disclosures.

Provide and conduct administrative functions related to payment and health care operations for and on behalf of a covered entity that include the following:

- To allow for and/ or audit claims payments
- For conducting enrollment
- To allow for quoting
- For underwriting activities
- To allow for case issuance
- Use of eligibility information for commissions and bonus processing and inquiries.
- For conducting Customer service activities
- To assist with request for identification cards
- To assist with requested demographic changes
- Use of financial information for the sole purpose of processing insurance premiums

- To respond to the Secretary of the Department of Health and Human Services to determine compliance with regulations
- For compliance programs and oversight audit functions
- To report privacy violations to the appropriate Federal and State authorities consistent with the HIPAA Privacy regulations
- For data aggregation to permit data analysis for contracted covered entities
- To public health and safety authorities
- To report abuse, neglect or domestic violence
- To law enforcement officials under certain circumstances
- For judicial and administrative proceedings
- To fulfill any obligations under workers' compensation laws or contracts
- To assist with the procurement, banking, or transplantation of organs, eyes or tissues
- To an individual upon request to provide access to his or her own protected health information
- To an individual to provide an accounting of disclosures of protected health information
- To request proposals for services to be provided to or on behalf of a covered entity
- To investigate fraud

The following are situations of additional uses and /or disclosures of protected health information where the individual can agree, object or restrict the use or disclosure:

- To assist in disaster relief efforts
- To another individual to assist with care or payment
- In an emergency

AUTHORIZED USES AND / OR DISCLSOURES

There are situations which require an individual's authorization prior to the use/ and disclosure of their protected health information.

- Marketing - this agency will ensure that an authorization has been completed prior to the marketing of any non-health care product.
- Psychotherapy notes - this agency will obtain a written authorization from the individual to use and/or disclose psychotherapy notes of any client for any activities outside of treatment, payment or health plan operations.
- Fund-raising - this agency will discuss any proposed fund-raising activities with the Privacy Officer to ensure covered entity obligations are met.

DISCLOSURES BY WHISTLEBLOWERS

Agency associates may disclose protected health information if they believe that agency has been unlawful or committed professional violations of privacy. These types of disclosures can be made to:

- A health oversight agency or public health authority authorized by law to investigate professional agency standards.
- An attorney retained by or on behalf of the agency associate for the purpose of determining the legal options of the associate regarding the conduct.

SALE OF PROTECTED INFORMATION

- This agency prohibits the selling for profit of protected information or data.

AVAILABILITY OF INFORMATION

This agency shall prepare, maintain and retain records relating to the use and disclosure of PHI in such form and for such time periods as required by applicable state and federal laws, rules and regulations. Upon reasonable request, covered entities may obtain copy and have access to any medical, administrative or financial record of the agency related to the use and disclosure of PHI. Review executed business associate agreement with covered entity to determine any appropriate charges for copies of the records. The agency shall make available information to covered entities to fulfill obligations to provide access to, provide a copy of and account for disclosures with respect to PHI pursuant to HIPAA and the HIPAA Regulations.

AUDITS, INSPECTIONS and ENFORCEMENT

This agency upon reasonable notice and determination will comply with legal obligations of HIPAA relating to audits, inspections and enforcement**.**

LITIGATION or ADMINISTRATIVE PROCEEDINGS

This agency shall make itself, and any contractors, employees or agents assisting the Agency in the performance of its obligations with covered entities to be available to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against a covered entity, based upon claimed violation of HIPAA, the HIPAA Regulations or other laws relating to security and privacy except where the Agency or its contractor, employee or agent is a named adverse party.

MINIMUM NECESSARY

The privacy regulation describes minimum necessary as limiting the use, disclosure, or request of protected health information to the least amount required to accomplish the intended purpose.

Limiting access to protected health information to those associates who have a "need to know" work function associated with their specific role at the agency also falls below minimum necessary.

This agency will apply minimum necessary guidelines to include written and oral communications. Engaging in casual conversation regarding protected health information is prohibited.

This agency makes reasonable efforts to limit the use and disclosure of protected health information to the least amount required to accomplish the task, and applies the minimum necessary standards when requesting, using, or disclosing protected health information.

DE-IDENTIFICATION

De-identification is a formal process of removing key identifiers (name, address, SSN, etc.) from an individual's protected health information so that the remaining information no longer identifies the individual, and the information cannot be re-identified to the individual. De-identified data requires no individual privacy protection and is not covered by the Privacy regulations. Refer to the Privacy & Security Official for further assistance regarding de-identification of data.

INFORMATION GUIDANCE

DOCUMENT RETENTION

Agency will maintain documents containing protected health information as required by state and/or federal laws, rules, standards and regulations. All documents containing protected health information will be maintained for a minimum of ten (10) years in accordance with the Federal HIPAA privacy regulation.

ASSOCIATE SANCTIONS

Failure to comply with agency privacy and security policy and procedures will result in appropriate sanctions with the associate. Sanction will be determined by severity of events and risk of harm.

In the following section, you will need to review carefully and adopt or delete statements that apply to implemented safeguards at your agency.

SAFEGUARDS

In accordance with the Federal HIPAA privacy regulations, this agency maintains reasonable administrative, physical and technical safeguards to assist with the protection of personal information. The safeguards below were implemented by this agency with consideration for our organization size and available technology. Additional details regarding specific procedures are in "Procedure Section" of this policy.

ADMINISTRATIVE SAFEGUARDS

Alissa Morris has been designated as the Privacy & Security Official for this agency. The acceptance of this designation includes the responsibility to administer the agency's privacy and security policy.

- **Our agency developed a privacy and security training program that includes contents of this policy.**
- **Our agency conducts privacy and security training upon employment with the agency.**
- **Our agency conducts privacy and security refresher training as needed.**

- **Our agency promptly removes system access upon associate termination.**

- **Disciplinary actions will be imposed on associates that fail to comply with the agency's privacy & security policy and procedures up to and including potential termination. Sanctions are determined by the severity and circumstance of the violation.**
- **All associates are required to sign a confidentiality agreement upon employment. Refer to "Agreement Section" for sample template.**

- **Agency will never delegate any work performed on behalf of a covered entity to an offshore vendor.**
- **Our agency associates perform an authentication process prior to the release of protected health information.**
- **Our agency follows the "minimum necessary" guidelines. Refer to "Minimum Necessary procedure".**
- **Agency will follow specific instructions provided by a covered entity on the return or destruction of data if contract is terminated. Upon termination of contract with covered entity, review executed Business Associate Agreement for instructions. Contact covered entity to verify instructions.**
- **Our agency has a documented procedure for handling security incidents. Refer to "Reporting a Privacy & Security Breach" procedure located in procedure section.**

- **Our agency requires prompt reporting of potential privacy and security breaches**

- **Our agency documents any identified risks and takes appropriate actions to address identified risks.**
- **Our agency will maintain system tracking logs of access and use of data and periodically review the information for potential breaches of our privacy and security policy**
- **Our agency has a data backup plan that describes process of creating and maintains retrievable exact copies of electronic protected health information.**
- **Our agency has a disaster recovery plan that describes process for restoring any lost data.**
- **Our agency has an emergency mode operation plan that describes processes to enable continuation of critical business processes while operating in an emergency mode.**
- **Our agency conducts periodic technical and nontechnical evaluations to ensure that appropriate security has been provided.**
- **Our agency has developed and provides a Notice of Privacy Practices that describes the allowed uses and disclosures of protected health information.**
- **Our agency has developed and implemented a privacy web statement.**

PHYSICAL SAFEGUARDS

- **Access to the agency is controlled by door lock and key.**

- **Visitor access to the agency is controlled by visitor sign in log.**
- **Visitor access to the agency is controlled by requirement that all visitors be accompanied by employed agency associate.**
- **All protected health information must be secured when not in use for more than 30 minutes. Documents must be placed in desk drawer, file cabinet, or folder to protect unauthorized access of protected health information.**
- **In situations where mail may be handled by various agency associates, mail should be forwarded to the address unopened. For mail that is not addressed to a specific individual, if the opened mail contains protected information, it should be placed in a folder or larger envelope for routing to the correct area.**

- **All documents containing protected information should be appropriately destroyed after meeting retention guidelines. Destruction of documents will occur by on-site shredding.**

- **All documents are to be retrieved from printers, copiers, and facsimile machines as promptly as possible.**
- **All documents that contain personal information requiring transport must be placed in a sealed envelope, sealing briefcase, locking box or other sealed container prior to the transport of the information.**
- **All agency mobile devices (such as cell phones, smartphones, BlackBerry devices or laptops, must be stored out of sight in a locked desk, locked office, or locked cabinet overnight.**
- **All workstation screens and display monitors that contain protected health information are visibly blocked to agency visitors.**
- **Agency requires all associates utilizing "agency systems" when working from a remote location to follow security measures implemented for remote access.**
- **Agency follows security processes such as degaussing, data wiping and physical destruction to ensure that protected health information is no longer accessible prior to the disposal or re-use of equipment.**

TECHNICAL SAFEGUARDS

- **System access is restricted to only those associates that have a need-to-know information to perform their job role at the agency.**
- **System access is reviewed and changed as needed due to change in job role.**
- **System access is promptly terminated upon associate termination or resignation.**
- **All outgoing faxes containing protected health information require a fax cover sheet.**
- **All fax cover sheets include a privacy disclaimer of:**
  The information transmitted is intended only for the person or entity to which it is addressed and may contain CONFIDENTIAL material. If you receive this material/information in error, please contact the sender and delete or destroy the material/information.

- **All documents containing protected health information must be shredded after meeting retention requirements.**

- **This agency prohibits the use of any mobile device (laptops, handheld devices, BlackBerry's, etc.) if they do not allow for secure access or transmission of protected health information.**
- **All agency associates must log off/shut down computers at the end of the business day.**
- **Password protection screen savers are applied to disable computers when inactive.**
- **System password changes are required every 90 days**

- **Our agency has a disaster recovery plan to obtain access to critical data.**
- **Our agency has a business continuity plan to obtain access to critical data.**
- **Our agency has a procedure to allow data access in emergency situations.**

AGREEMENTS

Our agency requires various agreements with our associates, vendors, and contractors to maintain the confidentiality of information and meet requirements with federal privacy regulations. A brief description of the various agreements and sample templates follow.

Associate Confidentiality Agreement:

The Associate Confidentiality Agreement is signed by every associate of our agency. The intent of this document is to obtain confirmation that associates understand that all information is the property of the agency and should only be used in the performance of the job with the agency. It further indicates that agreement remains in place upon termination.

Confidentiality Agreement/ Non-disclosure Agreement:

The Confidentiality/Non-disclosure Agreement is required by this agency for any contractors, including subcontractors and independent contractors to whom we provide any protected health information of a contracted covered entity.

Business Associate Agreement

A Business Associate Agreement is a document typically executed between a covered entity and an organization performing services (such as an independent broker/agency) involving the use and/or disclosure of Protected Health Information on behalf of the covered entity.

The Business Associate rule within the federal HIPAA privacy regulation seeks to ensure that as a business partner, the Business Associate adheres to the essential privacy protections required by the covered entity and that there is no degradation of privacy safeguards when data is shared with the Business Associate. As a Business Associate, the agency has accepted the responsibility to follow through on certain compliance requirements.

INDIVIDUAL PRIVACY RIGHTS

Privacy laws, rules, and regulations provide individuals with various options that are called individual rights. Individual privacy rights may be invoked by the individual or, if appropriate information is provided, by an authorized personal representative(s). The following are brief descriptions of the various individual rights.

Privacy Notice

Update (2026): The Notice of Privacy Practices (NPP) must incorporate the remaining modifications required by HHS with a compliance date of February 16, 2026. Portions of the April 26, 2024 Final Rule related to reproductive health care privacy were vacated on June 18, 2025; remaining NPP modifications are undisturbed pending further HHS guidance.

The Federal HIPAA Privacy regulation requires that covered entities provide a **Notice of Privacy Practices.** This notice describes the permitted and required uses and disclosures of protected information, provides an explanation of individual privacy rights, and outlines how to file a privacy complaint. Individuals have the right to request and receive Notice of Privacy Practices.

Access

The right to request access to protected health information allows individuals the opportunity to review and/or obtain a photocopy (or other such format) of their information. Upon receipt of a written request, a response must be provided within thirty (30) days unless an extension is needed.

Accounting

The right to an accounting allows individuals to request a list of disclosures of their protected health information made for purposes other than treatment, payment, health plan operations, and other activities in the past six years. Some activities to account for include, but are not limited to, audits by health oversight agencies for audit, investigations, licensure, for judicial and administrative proceedings (court order, subpoena, discovery, etc.), and for research purposes.

Restriction

The right to restrict allows individuals to request a limit or restriction on the use and disclosure of their protected health information. The regulation does not require agreement to the restriction if it is determined that the restriction may interfere with treatment, payment or operations.

Restriction Termination

The right to remove a restriction allows individuals the ability to request or agree to the removal of a previously requested restriction**.**

Alternate Communications

The right for an individual to request that health information is sent to a different address or by a different communication method due to potential abuse.

Amendment

The right to amend allows individuals the right to request a correction of their protected health information created and maintained by a covered entity that is inaccurate and/or incomplete.

Regulations require a response to this request within sixty (60) days of receipt, unless an extension is needed**.**

File a Complaint

The right to file a privacy complaint allows individuals the opportunity to express to the covered entity or the Secretary of the Department of Health and Human Services, any concerns of dissatisfaction regarding privacy issues**.**

In the event our agency receives any Individual Privacy Rights or a privacy concern about a covered entity, the request should be forwarded to our agency Privacy & Security Officer as quickly as possible to coordinate the request with the specific covered entity.

PRIVACY & SECURITY PROCEDURES & GUIDELINES

1) **Reporting a Privacy & Security Breach**
2) **Return / Destruction of Information**
3) **HIPAA Privacy & Security Training Program**
4) **Performing Authentication**
5) **Minimum Necessary Guidelines**
6) **Responding to Individual Privacy Rights**

REPORTING A PRIVACY AND OR SECURITY BREACH

• If an incident involves unauthorized acquisition of unencrypted customer information regulated by the FTC's GLBA Safeguards Rule and affects 500 or more consumers, notify the FTC as soon as possible and no later than 30 days after discovery (16 CFR Part 314).

Purpose

This procedure establishes the required reporting of alleged or actual privacy and/or security breaches. As a contracted Business Associate of covered entities, we are required to report breaches of unsecured protected health information in accordance with privacy and security regulations. Additionally, many states have data breach notification laws that require covered entities to report incidents and notify affected individuals.

Scope

The scope of this procedure is applicable for all incidents of alleged or actual privacy and / or security breaches.

Definitions

Protected Health Information *as defined by the federal privacy regulation is information that:*

- *Contains data elements or combinations of data elements that could identify a person or provide a reasonable basis to believe someone could be identified.*
- *Contains health-related information about that person; and*
- *Is it maintained or transmitted in any form (electronic, written, or oral)*

Breach – *the unintentional or unauthorized release of Protected Health Information.*

Policy

Our agency requires all associates and subcontractors to report any suspected breach of protected health information in accordance with legal and contractual requirements. All suspected breaches of protected health information will be reported immediately to our designated Privacy & Security Official for investigation. Report to Joshua Houchens, Joshua.houchens@advocatehealthllc.com.

The Privacy & Security Official will quickly analyse the report of suspected or actual breach information to assess for potential risks and to determine whether a breach of unsecured protected health information has occurred. The assessment will also include a review on the level of risk and potential harm to the individual(s).

Our Privacy & Security Official will notify the Privacy Office of the covered entity of any incident without unreasonable delay and in any event no later than timeframe documented in the business associate agreement.

Our Privacy & Security Official and the designated contact from the covered entity Privacy Office will jointly discuss and determine notification requirements to be compliant with state and federal laws.

Procedure

1. An actual or suspected breach of protected health information should be reported to the Privacy & Security Official as quickly as situation is determined.
2. Provide all information regarding the suspected incident to the Privacy & Security Official or complete an incident notification form if available. At a minimum the information provided should include names, dates, nature of the protected health information, the manner of the unauthorized use or disclosure and any written or electronic documentation concerning the incident.
3. Upon receipt of potential breach incident, the Privacy & Security Official will promptly investigate and assess risk of incident.
4. Privacy & Security Official will review contractual agreements with impacted covered entities to obtain reporting information, process and contact.
5. The Privacy & Security Official will report the privacy incident to the covered entity's Privacy office as quickly as discovery of the breach but not later than timeframes indicated within covered entity Business Associate agreement.
6. The Privacy & Security Official will provide the covered entity the following information regarding the suspected / alleged privacy and/or security breach: identification of each individual whose unsecured protected health information has alleged to have been accessed, acquired or disclosed, a description of the event, date of potential breach, type of protected health information involved in incident, any preliminary steps that have been taken to mitigate the damage and description of investigatory steps taken to date or complete an incident notification form provided by a covered entity.
7. The Privacy & Security Official will cooperate and assist the covered entity's Privacy Office with mitigation of risk of harm, required notifications, implementation of any corrective actions, & retraining of associates. Review of the executed Business Associate Agreement will also assist with responsibilities and obligations regarding notification methods and contents.
8. The Privacy & Security Official will document all actions of every incident in detail and retain documentation for a period of at least six years or follow agency retention requirements.

Return / Destruction of Protected Health Information upon Contract Termination

Purpose

This procedure is to provide guidelines on the required return or destruction of protected health information upon termination of contract with a covered entity in accordance with contractual agreements.

Scope

The scope of this procedure is applicable for our agency and any subcontractors having access to protected health information of our covered entity(ies).

Definitions

Protected Health Information *as defined by the federal privacy regulation is information that:*

- *Contains data elements or combinations of data elements that could identify a person or provide a reasonable basis to believe someone could be identified.*
- *Contains health-related information about that person; and*
- *Is it maintained or transmitted in any form (electronic, written, or oral)*

Policy

In accordance with the requirements of our executed Business Associate Agreements with covered entities, our agency is required to return or destroy protected health information of the covered entity upon contract termination. Our agency will contact the covered entity to discuss the best method of returning or destroying protected health information that was received, created or retrieved by our agency on behalf of the covered entity.

If immediate contact can't be made, our agency will continue to protect and safeguard the protected health information and limit further use or disclosure of such information until return / destruction has occurred.

Procedure

1. Upon notification or decision that contract between our agency and covered entity has been terminated or will be terminated, agency Privacy and Security Official shall contact the covered entity to discuss most appropriate method for return or destruction of protected health information.

2. Privacy Official will follow directions provided by the covered entity regarding the return or destruction of data and verify that all actions are complete.

3. Privacy Official will document completed actions.

Purpose

This procedure provides the general guidelines on the required privacy and security training of agency associates.

Scope

The scope of this procedure is applicable for all agency associates and any subcontracted associates as determined by the Privacy & Security Officer.

Definitions

Health Insurance Portability and Accountability Act (HIPAA) Title II – Administrative Simplification – the federal law containing administrative provisions for health plans, providers, and health care clearinghouses. The privacy portion of the law, designed to ensure the privacy of protected health information became effective April 14, 2003.

Policy

Our agency requires all associates to complete a HIPAA privacy and security training. Any subcontractor that has access to or uses any protected health information of a covered entity will also be required to complete our HIPAA privacy and security training. The agency Privacy & Security Officer will make determinations on requirements for subcontractors.

All new associates of our agency will complete the HIPAA privacy and security training within at least ninety (90) days of employment. Any identified remedial training is conducted at the discretion of the Privacy & Security Officer.

The Privacy & Security Officer will maintain all formal recording of training and completion dates.

The Privacy & Security Officer will determine contents of privacy and security training, implementation methods to meet the needs of the organization and need for any assessment of the training. The Privacy & Security Officer will revise privacy and security training to include new rules or regulations impacting privacy and or security.

Procedure

1. Agency will develop or purchase a HIPAA privacy & security training program.
2. Agency will review required audience to determine appropriate method of training delivery for associates.
3. Agency will determine timeframe for required completion of training.

4. Prior to planned training, Privacy & Security Officer will review existing training for any needed revisions. Review regulations for any revisions that need to be included.
5. Prior to training, Privacy & Security Officer will review pattern of privacy and /or security incidents to determine if any topic or safeguard needs to be stressed in training.
6. Privacy & Security Officer will coordinate any required review of proposed training program if applicable.
7. Obtain documentation indicating completion of training for all associates.
8. Privacy & Security Officer will maintain copy of training program and completion of training proof.

PERFORMING AUTHENTICATION

Purpose

This procedure establishes the required process of authentication prior to the release of protected health information.

Scope

The scope of this procedure is applicable for all requests for release of protected health information.

Definitions

Authentication – process used to verify the identity of a person whose protected health information is being requested, and the authority of the requester to access that person's protected health information.

Policy

Our agency requires all associates and subcontractors to conduct authentication prior to the release of any requested protected health information. The agency requires verification of the identity of a person whose protected information is being requested prior to disclosing the information. Our process also includes verification of the authority of the person to have access to the requested protected health information. Both elements of identity and authority are required by this agency for valid authentication.

Procedure

1. Receive a request that involves the release of protected health information.

2. Ask a series of questions that require the requestor to provide information that allows the agency to validate the identity of the individual whose information is being requested. If

the requestor is not the owner of the protected health information, determine what provides the authority for the requested protected health information (power of attorney, official title, etc.).

3. If assistance is needed concerning the allowed release, contact the Privacy & Security Officer.

MINIMUM NECESSARY GUIDELINES

Purpose

This procedure establishes the required process of using the minimum necessary protected health information to fulfil a request or perform a required task.

Scope

This agency will make reasonable efforts to limit the use and disclosure of protected health information to the least amount required to accomplish the task, and applies the minimum necessary standards when requesting, using, or disclosing protected health information.

Definitions

Minimum Necessary - *is defined as limiting the use, disclosure, or request of protected health information to the least amount required to accomplish the intended purpose.*

Policy

Our agency requests all associates and subcontractors to follow minimum necessary guidelines for all forms of communications of protected health information.

Procedure

1. Receive a request or identify a required action that involves the use or release of protected health information.

2. Review information to be provided to determine the minimal amount of information that will fulfill the request yet accomplish the intended purpose.

3. Provide response or conduct action using the minimal amount of protected information.

4. The minimum necessary requirement does NOT apply to:

- Uses or disclosures made to the individual who is the subject of the protected health information
- Uses or disclosures made pursuant to an individual's authorization
- Uses or disclosures required for compliance with HIPAA Administrative Simplification Rules
- Disclosures to a health care provider for treatment purposes
- Disclosures made to the Secretary of Health and Human Services when disclosure is required for enforcement purposes of the HIPAA Privacy regulations; or
- Uses or disclosures required by law.

An agency associate may presume that a request for information from public officials, or covered entities (such as providers or hospitals) is for minimum necessary information.

RESPONDING TO RECEIVED INDIVIDUAL PRIVACY RIGHTS

Purpose

This procedure establishes the required process of responding to the receipt of any individual privacy rights request or complaints received on behalf of a covered entity.

Scope

The scope of this procedure is applicable for all received individual privacy rights requests and privacy complaints intended for a covered entity.

Definitions

Individual Privacy Rights - are defined by the federal privacy regulation as various options allowed to individuals regarding their privacy. The Individual Rights include right to access, right to amend, right to an accounting, right to restriction, right to complain, right to confidential communications and the right to a Notice of Privacy Practice.

Policy

Upon receipt of any individual privacy right or privacy complaint received for a covered entity, our agency will promptly contact and provide the covered entity with the individual privacy right or privacy complaint.

Procedure

1. Receive an Individual Privacy Rights request or privacy complaint on behalf of a covered entity. *Note – some covered entities have forms to request these rights.

2. Document all information pertaining to the individual privacy request or complaint and promptly provide the information or form to the agency Privacy & Security Officer.

3. Upon receipt of individual privacy rights request or privacy complaint on behalf of a covered entity, identify Privacy & Security contact information for the covered entity and make contact as quickly as possible to allow covered entity to meet required response timeframes.

4. Follow instructions provided by covered entity and forward information and/or forms to the covered entity.

5. Document actions performed to forward information to covered entity.

Regulatory Resources

The following are sources may be beneficial in providing the specific regulations and frequently asked questions and answer documents regarding the regulations.

AGENCY	URL LOCATION	REGULATORY ENTITY
Office for Civil Rights	www.hhs.gov/ocr/	HHS Office for Civil Rights
HIPAA Privacy Rule	www.hhs.gov/ocr/privacy	HHS Office for Civil Rights
HiTech (ARRA of 2009)	www.hhs.gov/ocr/privacy/hipaa/	HHS Office for Civil Rights
HIPAA Security Rule	www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html	HHS Office for Civil Rights
Gramm-Leach Bliley Act	www.ftc.gov/privacy/glbact	Federal Trade Commission
Federal Trade Act	www.ftc.gov	Federal Trade Commission

HIPAA Security Rule (Summary)	https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html	HHS Office for Civil Rights
Breach Notification Rule	https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html	HHS Office for Civil Rights
NIST SP 800-66 Rev. 2	https://csrc.nist.gov/pubs/sp/800/66/r2/final	NIST
HPH Cybersecurity Performance Goals	https://hhscyber.hhs.gov/performance-goals.html	HHS
FTC GLBA Safeguards Rule (16 CFR Part 314)	https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314	Federal Trade Commission

DISCLAIMER: THIS DOCUMENT IS MEANT ONLY AS A GUIDE AND IS NOT A DEFINITIVE LEGAL INTERPRETATION.