Ken Locke and Associates, LLC

PRIVACY & SECURITY POLICY

Oct 1, 2023

Ken Locke and Associates, LLC

PRIVACY & SECURITY POLICY

TABLE OF CONTENTS

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

Ken Locke and Associates, LLC 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.

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 persons 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 the 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 disrupts 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 in order 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
- 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 of the administrative, physical, and technical safeguards in an information system.

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 the 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 persons 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:

- For conducting enrollment
- To allow for and/ or audit claims payments
- 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 contract
- 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 has the opportunity to 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 situation

AUTHORIZED USES AND / OR DISCLOSURES

There are situations which require an individual's authorization prior to the use/ and or 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 with regard to 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 under 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 require 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 a minimum of six (6) 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 event and risk of harm.

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 located in "Procedure Section" of this policy.

ADMINISTRATIVE SAFEGUARDS

Kenneth Locke 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.**
- **All agency associates are required to complete privacy and security training within 30 (thirty) days from hire date.**
- **Our agency conducts privacy and security training on an annual basis.**

- **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.**
- **Our agency revises allowed system access based upon job role changes.**
- **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.**

- **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 of a security incident. Refer to "Reporting a Privacy & Security Breach" procedure located in procedure section.**
- **Our agency requires the prompt reporting of potential privacy and or security breaches**

- **Our agency documents any identified risks and takes appropriate actions to address identified risks.**
- **Our agency has a disaster recovery plan that describes the process for restoring any lost data.**
- **Our agency conducts periodic testing of contingency plans.**
- **Our agency has an emergency mode operation plan that describes process 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 implemented.**
- **Our agency has developed and implemented a privacy web statement.**

PHYSICAL SAFEGUARDS

- **Access to the agency is controlled by door lock and key.**
- **Access to the agency is controlled by building entry key cards.**
- **Visitor access to the agency is controlled by a requirement that all visitors be accompanied by an employed agency associate.**
- **All protected health information must be stored in a locked file cabinet overnight.**
- **All protected health information must be stored in a locked desk overnight.**
- **All protected health information must be stored in a locked office overnight.**
- **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 outgoing agency mail in a window envelope must be reviewed to verify that only name and address are displayed in window.**
- **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 reviews physical layout of associate workstation screens and display monitors to safeguard protected health information from individuals not authorized.**
- **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.**
- **All requests for agency system demonstrations by an external organization or individual requires the review of the Privacy Officer.**
- **All agency associates must invoke software closure on equipment if not in use within five minutes.**

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 outgoing emails containing protected health information must be sent securely with encryption.**
- **Protected health information cannot be sent to an external email address using a multifunction device (a device that consolidates the functionality of a printer, copier, scanner and/or fax into one machine).**
- **All documents containing protected health information must be shredded after meeting retention requirements.**
- **This agency prohibits the use of any mobile device (laptops, hand held 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.**
- **All computer workstations are automatically locked down by systems when associate is away from workstation for more than five minutes.**

- **Password protection screen savers are applied to disable computers when inactive.**

- **Our agency maintains a unique name and/ or number for the identification and tracking of system user identity.**

- **Our agency has implemented technical procedures that verify the person or entity seeking access or protected health information.**

- **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.**