Beam Technologies LLC Privacy Policy
September 2022

Table of Contents

Beam Technologies LLC Privacy Policy
September 2022

Introduction

The purpose of this policy manual is to outline the general circumstances under which Beam and/or a Beam workforce member with access to protected health information (PHI) may use or disclose PHI under the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA), as amended, and the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA).

Section 1: Policy Definitions

Applicable Requirements

Applicable requirements mean applicable federal, state, and/or local law, and the terms of the contracts between Beam Technologies Inc. and other persons or entities that conform to federal, state, and/or local law, depending on location.

Breach

Breach is the acquisition, access, use, or disclosure of PHI in an unauthorized manner that compromises the security or privacy of the PHI. The following types of breaches are expressly excluded from this definition:

A. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner prohibited by HIPAA;

B. Any inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI at the same Covered Entity or Business Associate and the information is not further disclosed in a manner prohibited by HIPAA; or

C. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Business Associate

Business Associate means a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. Examples of business associates are set forth more fully in Section 10 of these Policies and 45 CFR §160.103.

Covered Entity

Covered entity means a health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form in connection with a transaction covered by HIPAA rules.

Designated Record Set

Designated record set is a group of records maintained by or for a covered entity that comprises the:

A. Medical records and billing records about individuals maintained by or for a covered health care provider;

B. Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

C. Other records used, in whole or in part, by or for the covered entity to make decisions about individuals.

D. For purposes of this definition, the term "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Disclosure

Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Encryption

Encryption is defined as a method of converting an original message of regular text into encoded text.

The text is encrypted by means of an algorithm (type of formula). If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text.

Firewall

Firewall is a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.

Health Care Clearinghouse

Health Care Clearinghouse is a public or private entity, including a billing service, community health management information system, or community health information system, and "value-added" networks and switches, that do either of the following functions:

A. Processes or facilitates the processing of health information received from another entity in a nonstandard format, or containing nonstandard data content into standard data elements or a standard transaction; or

B. Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health Care Provider

Health care provider means a provider of services, a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health Oversight Agency

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health Plan

Health plan means an individual or group plan that provides or pays the cost of medical care. Health plan includes the following, singly or in combination:

A. The Medicaid program under Title XIX of the Act, 42 U.S.C. § 1396, et seq.;

B. Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care.

HIPAA

HIPAA means the Health Insurance Portability and Accountability Act of 1996, codified at 42 USC §§1320–1320d-8 and 45 CFR Parts 160 and 164.

A. The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions. HIPAA also applies to business associates and their subcontractors. The Rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patient's rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

HITECH

HITECH means the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, and codified at 42 U.S.C. § 300jj et seq.; §§17901 et seq.

Local Area Network (LAN)

LAN is a computer network that covers a small geographic area, i.e. a group of buildings, or an office.

Law Enforcement Official

Law Enforcement Official means an officer or employee of any agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, who is empowered by law to:

A. Investigate or conduct an official inquiry into a potential violation of law; or

B. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Memorandum of Understanding (MOU)

MOU means a formal agreement between two or more parties. The elements of MOUs are more fully explained in Section 10.

Minimum Necessary

Minimum Necessary means to only release a limited data set or the minimum information necessary to accomplish the purpose of the disclosure.

Personal Representative

Personal Representative means a person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent, guardian, or other person acting in loco parentis who is authorized under law to make health care decisions on behalf of an unemancipated minor, except where the minor is authorized by law to consent, on his/her own or via court approval, to a health care service, or where the parent, guardian or person acting in loco parentis has assented to an agreement of confidentiality. A court appointed guardian is a legal representative as well as someone with custody through an order of a court. A health care powers of attorney and some similar designations of a representative under Ohio or local law are legally recognized documents that do not involve any court. These may be sufficient to allow another person to act as a personal representative under HIPAA.

PHI/ePHI

PHI means Protected Health Information, that is, individually identifiable health information relating to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual. PHI does not include individually identifiable health information in any of the following:

A. Education records subject to Family Educational Rights and Privacy Act;

B. Employment records held by a covered entity in its role as employer; or

C. Regarding a person who has been deceased for more than 50 years.

D. For the purposes of this definition, “employer” means the person for whom an individual performs or performed any service, of whatever nature, as the employee of such person.

E. Electronic Protected Health Information (ePHI) means PHI that is in an electronic format. The two are used interchangeably throughout this document.

Public Health Authority

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

TPO

TPO means treatment, payment, or health care operations under HIPAA rules.

A. Treatment means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

B. Payment encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

C. Health care operations are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.

D. The requirements for treatment, payment and healthcare operations are set forth more fully in 45 CFR §164.501.

Unsecured PHI

Unsecured PHI means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued. See 45 CFR §164.402.

A. The regulations require this guidance to be updated annually. PHI that is secured as specified by the guidance will not be subject to notification in the event there is a breach of the secured PHI.

Use

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

User

User is any person authorized to access an information resource.

Vendors/Subcontractors

Vendors/Subcontractors are persons from other organizations providing services to or on behalf of Beam.

Virtual Local Area Network (VLAN)

VLAN is a logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes. It combines user stations and network devices into a single unit regardless of the physical LAN segment they are attached to.

Virus

Virus is a software program capable of replicating itself by modifying other computer programs and inserting its own code. It is usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

Virtual Private Network (VPN)

VPN provides a secure, private network from a public Internet connection.

Wide Area Network (WAN)

WAN is a computer network that enables communication across a broad area, i.e. regional, or national.

Workforce Member

Workforce Member means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such entity, whether or not they are paid by the covered entity or business associate.

Workstation

Workstation is an electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, used to create, receive, maintain, or transmit PHI/ePHI. Workstation devices may include but are not limited to: laptop or desktop computers or monitors, cellphones, tablets, and other handheld devices. For the purposes of this policy, “workstation” also includes the combination of hardware, operating system, application software, and network connection.

Section 2: General Policy

Beam Technologies Inc (Beam) and its workforce members (collectively, Beam) shall conform to all applicable requirements for privacy and confidentiality set forth in HIPAA, HITECH, and other applicable law, as well as the requirements set forth in these policies and accompanying procedures. Beam shall not use or disclose PHI except in accordance with applicable requirements.

TPO

Beam may use PHI for TPO related services without an individual's release or authorization to the extent that such activities occur within Beam. Beam shall obtain a release or authorization from the individual for any disclosure for TPO when such disclosure is to a person or entity that is not otherwise entitled to receive such information under applicable requirements.

Scope of Disclosure: Minimum Necessary Standard

In general, use, disclosure, or requests of records must be limited to the minimum that is reasonably necessary to accomplish the purpose of the use, disclosure, or request. In order to comply with the minimum necessary standard, Beam will adhere to the following policies outlining Beam employee or job position access to PHI and the nature of the PHI to be used or disclosed depending on the purpose of the use, disclosure, or request.

Internal Uses and Disclosures:

A. Electronic role-based access:

All access to sensitive data should be controlled and authorized. Any job functions that require access to sensitive data should be clearly defined. Access rights to privileged user IDs should be restricted to the least privileges necessary to perform job responsibilities (role-based access control). Access to sensitive information such as personal information and business data is restricted to employees that have a legitimate need to view such information. No other employees should have access to this confidential data unless they have a genuine business need.

B. Paper-based access:

Beam will ensure that all hard copies of PHI are stored in a secure, confidential manner and access may only be granted to those employees whose job duties require access. Employees permitted access must avoid reviewing any paper-based PHI outside of the scope of the function being performed. Those employees who do not require access to PHI to perform their job duties will not be permitted to access this information.

C. Department-based access:

The content of the PHI accessible to those departments that need access to PHI to carry out their job function will be limited to only that which is needed.

Routine or Recurring Disclosures:

A. Beam must limit the PHI disclosed or requested to that which is the minimum necessary for that particular type of disclosure or request. For example, for a disclosure made to another health insurance company for coordination of benefits purposes, the dates of service and the effective dates of the policy may be the minimum necessary to satisfy that particular disclosure or request.

Non-Routine Disclosures:

A. Beam will notify legal and legal will evaluate each such non-routine disclosure or request to verify that the PHI disclosed or requested is only that amount which is necessary to accomplish the purpose of the disclosure or request. Examples of non-routine disclosures include, but are not limited to, subpoenas, court orders, or other legal requests.

Reasonable Reliance:

A. In limited circumstances, Beam may, but is not required to, rely on the judgment of the party requesting the disclosure that the PHI requested is the minimum amount needed. Such reliance must be reasonable under the circumstances. Such "reasonable reliance" is permitted only when the request for PHI is made by:

i. A public official or agency who states that the information requested is the minimum necessary for a purpose permitted under 45 CFR 164.512 of the Rule, such as for public health purposes (45 CFR 164.512(b)).

ii. Another covered entity.

iii. A professional who is a workforce member or business associate of the covered entity holding the information and who states that the information requested is the minimum necessary for the stated purpose.

The minimum necessary standard does not apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an individual's authorization.
- Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the Privacy Rule for enforcement purposes.
- Uses or disclosures that are required by other law.

Incidental Uses and Disclosures

Beam may use or disclose PHI incidental to a use or disclosure otherwise permitted or required by applicable requirements:

- An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the Privacy Rule.
- Permissible incidental uses and disclosures are those that occur as a by-product of another permissible or required use or disclosure, as long as Beam has applied reasonable safeguards and implemented the minimum necessary standard **(see Scope of Disclosure: Minimum Necessary Standard on Page 6),** where applicable, with respect to the primary use or disclosure.
- An incidental use or disclosure is not permitted if it is a byproduct of an underlying use or disclosure that violates applicable requirements and Beam policies and procedures.

Changes in Policies and Procedures

Beam shall change its policies and procedures as necessary and appropriate to comply with changes in applicable requirements. The changes shall apply to existing PHI effective on the date of notice of the change. Beam shall document material changes in policies and notices which reflect such changes.Beam shall retain such documentation for seven (7) years or as otherwise mandated by applicable requirements.

Mitigation

Beam shall mitigate, to the extent practicable, any harmful effect that is known to Beam of a use or disclosure of PHI in violation of its policies and procedures or the requirements of applicable requirements by Beam, its business associate, or its vendor/subcontractor.

Beam's duty to mitigate does not alter Beam's duty to report breaches as set forth in Section 8 and as required by law or any contractual obligations.

Prohibition against Retaliation, Intimidation and Waiver of Rights

No investor, officer, partner, vendor, or workforce member of Beam shall intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against

- Any individual for the exercise of their rights or participation in any process relating to HIPAA compliance; or
- Against any person for filing a complaint with the Secretary of the U.S. Department of Health and Human Services, participating in a HIPAA related investigation, compliance review, proceeding or hearing, or engaging in reasonable opposition to any act or practice that the person in good faith believes to be unlawful under HIPAA regulations as long as the action does not involve disclosure of PHI in violation of the regulations.

Further, no investor, officer, partners, or vendors of Beam shall require individuals to waive any of their rights under HIPAA as a condition of treatment, payment, or enrollment in a health plan or eligibility for benefits.

Section 3: Administration

Beam shall designate and document designations of the:

Privacy Officer

The Privacy Officer oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to Beam's policies and procedures covering the privacy of, and access to, individual health information in compliance with federal and state laws, and Beam's information privacy practices.

The current Privacy Officer for Beam is: Devon Bolte, Senior Compliance Manager
Phone: (800) 648-1179
Email: Devon.Bolte@beam.dental

The Privacy Officer's responsibilities include, but are not limited to, the following:

Privacy Risk Assessments and Monitoring:

A. Performs initial and periodic information privacy risk assessments.

B. Conducts ongoing compliance monitoring activities in coordination with the entity's other compliance and operational assessment functions.

Privacy Incident Review and Determination

A. Reviews, assesses and provides determination on company privacy incidents.

B. Reviews and approves all breach notifications including to business partners, business associates, government agencies, and individuals.

Privacy Training

A. Oversees, directs, delivers, or ensures delivery of initial and annual privacy training to all employees, contractors, interns, business associates, and other appropriate third parties.

Protected Health Information/Personal Identifiable Information

A. Establishes with officers and operations a mechanism to track access to PHI, within the purview of Beam and as required by law.

B. Works cooperatively with the applicable Beam units in overseeing individual rights to access, amend, and restrict access to PHI when appropriate.

C. Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning Beam's privacy policies and procedures and, when necessary, legal counsel.

Privacy Liaison

A. Serves as information privacy consultant to Beam for all departments and appropriate entities.

B. Serves as liaison for Federal and state regulators

Beam shall designate and document designations of the:

Security Officer

The current Security Officer for Beam is: Rob Burns, Chief Information Security Officer
Phone: (800) 648-1179
Email: rob.burns@beam.dental

Governance Committee

For purposes of Beam's Privacy Policies, Beam has established a Governance Committee made up of key personnel whose responsibility it is to identify areas of concern within Beam and act as the first line of defense in enhancing the appropriate security posture. Additionally, the Governance Committee will authorize any changes to PHI and documents containing PHI; Retention, Storage, and Destruction policies and procedures; review and approve retention schedules and revisions to current retention schedules; address compliance audit findings; and review and approve control forms relating to business records.

All members identified within this policy are assigned to their positions by the Privacy Officer. The term of each member assigned is at the discretion of the Privacy Officer, but generally it is expected that the term will be one (1) year. Members for each year will be assigned by the Privacy Officer in a new calendar year. This committee will consist of the positions within Beam most responsible for the overall security policy planning of the organization – the Privacy Officer and the Security Officer (where applicable). The current members of the Governance Committee are:

Privacy Officer – Devon Bolte
Security Officer – Rob Burns
HR Director – Emily Linch
Legal Counsel – Steven Heistand

The Governance Committee will meet to discuss security issues, to review concerns that arose during the quarter, and to discuss Retention, Storage, and Destruction of records containing PHI. The Governance Committee will identify areas that should be addressed during annual training and review/update security policies as necessary.

The Governance Committee, in collaboration with Security and any applicable Security committees, will address security issues as they arise and recommend and approve immediate security actions to be undertaken. It is the responsibility of the Governance Committee to identify areas of concern within Beam and act as the first line of defense in enhancing the security posture of Beam.

The Governance Committee, in collaboration with the Security Incident Response Team as identified in the Security Incident Response Policy, are responsible for maintaining a log of security concerns or confidentiality issues. This log must be maintained on a routine basis, and must include the dates of an event, the actions taken to address the event, and recommendations for personnel actions, if appropriate. This log will be reviewed during the quarterly meetings.

Additionally, the Governance Committee maintains responsibility for the following:

- Review, maintain, publish, and distribute retention schedules and records management policies;
- Audit compliance with documents containing PHI management (both electronic and paper) policies and retention schedules;
- Serve as point of contact for any questions pertaining to PHI document Retention, Storage, and Destruction;
- Provide Retention, Storage, and Destruction training for workforce member or business associate that needs assistance;
- Oversee operation of designated offsite record storage center(s) for archival storage of paper PHI or serve as contract administrator for such services, if applicable; and
- Contract for destruction of paper and electronic records and certification thereof.

The Security Officer or other assigned personnel are responsible for maintaining a log of security enhancements and features that have been implemented to further protect all sensitive information and assets held by Beam. This log will also be reviewed during the quarterly meetings.

Contact Person

The following have been designated by Beam as those responsible for receiving complaints relating to PHI and for providing information about Beam's privacy practices. Complaints shall be submitted to compliance@beambenefits.com.

The current contacts for complaints are:
Devon Bolte

Section 4: Authorizations

In compliance with 45 CFR Part 164 and Ohio law, all uses and disclosures of PHI beyond those otherwise permitted or required by law require a signed authorization. An authorization that conforms to procedures adopted by Beam may be used for use or disclosure of PHI in any situation authorization or release of information is required. Please refer to the HIPAA PHI Uses and Disclosures Procedure and the DocuSign Process for HIPAA Authorization and Revocation located on Confluence for additional information on when and how to obtain an authorization.

PHI of deceased individuals is protected to the same extent as that of living individuals. This protection expires 50 years after the death of the individual. In the meantime, PHI may be disclosed to authorized representatives of the decedent, such as an executor or administrator, or to a family member involved in the individual's care or payment for health care prior to the individual's death, if the PHI is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

Beam must also obtain an authorization for any disclosure of PHI that is a sale of PHI. The authorization must state that the disclosure will result in remuneration to the covered entity.

For the purposes of this procedure, a "sale" is defined as a disclosure of PHI by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the PHI, subject to exceptions in HIPAA Rules.

Exceptions for the requirement to obtain an authorization can be found below in Section 5.

Conditioning Services on Authorization

Content Requirements: Each authorization for the use or disclosure of an individual's PHI shall be written in plain language and shall include at least the following information:

- A specific and meaningful description of the information to be used or disclosed;
- The name or identification of the person or class of person(s) authorized to make the use or disclosure;
- The name or identification of the person or class of person(s) to whom the requested use or disclosure may be made;
- Purpose of the disclosure or statement, or that the disclosure is at the request of the individual;
- An expiration date or expiration event that relates to the individual or the purpose of the use or disclosure; the statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of PHI for research, including for the creation and maintenance of a research database or research repository;
- A statement of the individual's right to revoke the authorization in writing, and exceptions to the right to revoke, together with a description of how the individual may revoke the authorization or make reference to conditions for revocation in the notice;
- A statement regarding permissible conditioning of treatment, payment, enrollment or eligibility for benefits on the authorization,;
- A statement that the potential for information disclosed pursuant to the authorization may be subject to re-disclosure by the recipient if the recipient is not subject to federal or state confidentiality restrictions;
- If the authorization is for marketing purposes and Beam will receive either direct or indirect compensation, the authorization must state that Beam will receive remuneration;
- The dated signature of the individual; and
- If the authorization is signed by a personal representative of the individual, a description of the representative's authority to act on behalf of the individual.

Elements for Authorization

- Beam may not condition the provision of TPO to an individual, or eligibility for benefits on the provision of an authorization, except:

    A. Beam may condition enrollment for Beam services or eligibility for Beam services on provision of an authorization requested by Beam prior to an individual's enrollment in the Beam services, if:

        i. The authorization sought is for determining eligibility for Beam services or enrollment determinations relating to the individual.

- Beam may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to such third party.

Combining Authorizations

- An authorization that has been improperly combined with another authorization or document is invalid.
- An authorization can permit disclosure for more than one purpose except that:

  A. An authorization for use or disclosure of PHI for research may only be combined with another authorization for use or disclosure of PHI for research provided there is opportunity to opt out under certain circumstances.

- An authorization that is required as a condition for treatment, payment, enrollment or eligibility for benefits cannot be combined with another authorization.
- An authorization cannot be combined with another document such as a notice or consent for treatment.

Right to Revoke

- An individual may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that:

  A. Beam has taken action in reliance thereon; or

  B. If the authorization was obtained as a condition of obtaining insurance coverage, other laws provide the insurer with the right to contest a claim under the policy or the policy itself.

- An authorization that has been revoked is no longer valid.
- Upon written notice of revocation, further use or disclosure of PHI shall cease immediately except to the extent that the investor, officer, partner, vendor, or workforce member has acted in reliance upon the authorization or to the extent that use or disclosure is otherwise permitted or required by law.

Invalid Authorizations

An authorization is not valid if it has any of the following defects:

- The expiration date or event has passed;
- The authorization was not filled out completely;
- The authorization is revoked;
- The authorization lacks a required element; or
- The authorization violates requirements regarding compound authorizations.

Verification

- Beam must take reasonable steps to verify the identity of a person receiving PHI and the authority of any such person to have access to PHI. For more information, please refer to the HIPAA Verification Requirements found on Confluence.

Document Management

- If the individual who executed the authorization is seeking a copy, a copy of the authorization must be provided to the individual.
- Beam must retain the written or electronic copy of the authorization for a period of seven (7) years from the later of the date of execution or the last effective date.

Section 5: Policy on uses and Disclosures for which no release or authorization is required

Uses and Disclosures

Beam may use or disclose PHI without written release or authorization of the individual as provided for below. Before any information may be used or disclosed as provided for in this section, Beam workforce members must follow the HIPAA PHI Uses and Disclosures Procedure located on Confluence. Failure to follow this policy and the accompanying procedure may result in disciplinary action, up to and including termination.

When required by law:

Beam may use or disclose PHI to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law, including, but not limited to the requirements summarized below in sections 3, 4, and 5.

For Public Health Purposes such as to prevent disease, help with product recalls, and report adverse reactions to medications or specifically to:

A. A public health authority authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury or disability, reporting vital events, conducting public health surveillance, investigations or interventions; or

B. A person who may have been exposed to a communicable disease or may be at risk of contracting or spreading a disease or condition.

For Health Oversight Activities such as investigations, audits, and inspections:

A. PHI may be used or disclosed for activities related to oversight of the healthcare system, government health benefits programs, and entities subject to government regulation, as authorized by law, including activities such as audits, civil and criminal investigations and proceedings, inspections, and licensure and certification actions.

B. Specifically excluded from this category are investigations of an individual that are not related to receipt of health care, or the qualification for, receipt of, or claim for public benefits.

For Judicial and Administrative Proceedings:

A. Beam must always comply with a lawful order, but only in accordance with the express terms of the order.

B. Subpoena, discovery request or other lawful process. Beam may comply with such legal requests only if:

i. Beam receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the PHI that has been requested has been given notice of the request; or

ii. Beam receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order.

C. Beam shall not respond to a subpoena without review by legal to ensure compliance with applicable requirements.

For Law Enforcement Purposes or to a Law Enforcement Official:

A. Pursuant to court order or as otherwise required by law, subject to any exceptions set forth in applicable law.

B. Decedent's PHI may be disclosed to alert law enforcement to the death, if Beam suspects that the death resulted from criminal conduct.

C. Beam may disclose to a law enforcement official PHI that Beam believes in good faith constitutes evidence of criminal conduct that occurred on the premises of Beam.

D. Providing emergency health care in response to a medical emergency, other than such emergency on the premises of Beam, may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

i. The commission and nature of a crime;

ii. The location of such crime or of the victim(s) of such crime; and

iii. The identity, description, and location of the perpetrator of such crime.

E. Compliance/Enforcement of privacy regulations: PHI must be disclosed as requested, to the Secretary of Health and Human Services related to compliance and enforcement efforts.

F. PHI may be disclosed to a correctional institution or a law enforcement official having lawful custody of an inmate if the disclosure of PHI is necessary for:

i. The provision of health care to such individual;

ii. The health and safety of such individual or other inmates;

iii. The health and safety of the officers or employees of or others at the correctional institution;

iv. The health and safety of such individual and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility or setting to another;

v. Law enforcement on the premises of the correctional institution; or

vi. The administration and maintenance of the safety, security, and good order of the correctional institution.

Beam should not respond to a court order, subpoena, or request for information from law enforcement without review by legal to ensure compliance with applicable requirements.

Coroners, Medical Examiners, and Funeral Directors:

PHI may be disclosed to coroners, medical examiners and funeral directors, as necessary for carrying out their duties.

Reduce or Prevent a Serious Threat to Public Health and Safety:

A. PHI may be used or disclosed if the entity believes in good faith:

B. that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to a person or the public, and disclosure is to someone reasonably able to prevent or lessen the threat;

C. Disclosures of admitted participation in a violent crime are limited to the individual's statement of participation and the following PHI:

i. name,
ii. address,
iii. date and place of birth,
iv. social security number,
v. blood type,
vi. type of injury,
vii. date and time of treatment,
viii. date and time of death, if applicable, and
ix. a description of distinguishing physical characteristics.

D. To report suspected abuse, neglect or domestic violence.

Organ and Tissue Donation Requests:

PHI may be disclosed to organ procurement organizations or other entities engaged in the procurement, banking or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

Specialized Government Functions:

A. National Security and Intelligence: PHI may be disclosed to authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other activities authorized by the National Security Act.

B. Protective services: PHI may be disclosed to authorized federal officials for the provision of protective services to the President, foreign heads of state, and others designated by law, and for the conduct of criminal investigations of threats against such persons.

C. Public Benefits: PHI relevant to administration of a government program providing public benefits may be disclosed to another governmental program providing public benefits serving the same or similar populations as necessary to coordinate program functions or improve administration and management of program functions.

D. Military and veterans activities: PHI of individuals who are Armed Forces personnel may be disclosed to assure the proper execution of military missions if the appropriate military authority has published by notice in the Federal Register the following information:

i. Appropriate military command authorities, and

ii. The purposes for which the protected health information may be used or disclosed.

For Workers' Compensation or Other Similar Programs, if applicable:

PHI may be disclosed as authorized and to the extent necessary to comply with laws relating to workers' compensation and other similar programs.

For Disaster Relief Purposes:

An individual has a right and a choice to inform Beam whether or not to share their PHI to assist in disaster relief efforts. However, in the event an individual is unable to communicate their preference, PHI may be disclosed to assist in disaster relief efforts if Beam believes that it is in the best interest of the individual or to lessen a serious and imminent threat to health and safety.

Fundraising:

Beam may use, or disclose to a business associate or to an institutionally related foundation, the following PHI for the purpose of raising funds for its own benefit, without an authorization:

A. Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;

B. Dates of health care provided to an individual;

C. Department of service information;

D. Treating physician;

E. Outcome information; and

F. Health insurance status.

With each fundraising communication made to an individual, Beam shall provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications.

Record of Immunization

Beam may provide proof of immunization without a formal written authorization, but some form of consent, including oral consent, is required.

Limited Data Set

A limited data set is PHI/ePHI that excludes the following identifiers of the individual or of relatives, employers, or household members of the individual:

1. Names;
2. Postal address information, other than town or city, State, and zip code;
3. Telephone numbers;
4. Fax numbers;

5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;
13. URLs;
14. IP address numbers;
15. Biometric identifiers, including finger and voice prints; and
16. Full face photographic images and any comparable images.

Permitted Uses and Disclosures of a Limited Data Set

A limited data set may only be used for purposes of research, public health, or health care operations.

Data Use Agreement

In order to use or disclose a limited data set, Beam must enter into a data use agreement. The data use agreement must:

1. Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with **(see Permitted Uses and Disclosures of Limited Data Set above)** of this policy. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of HIPAA, if done by Beam;

2. Establish who is permitted to use or receive the limited data set; and

3. Provide that the limited data set recipient will:

    A. Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

    B. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

    C. Report to Beam any use or disclosure of the information not provided for by the data use agreement of which it becomes aware;

    D. Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

    E. Not identify the information or contact the individuals.

In instances in which a limited data set may be used or disclosed, Legal must be contacted to determine whether a data use agreement is needed. If it is determined that a data use agreement is needed, Legal will work with the necessary business partners and the recipient of the limited data set to execute a data use agreement. The same process outlined in Section 10: Policy on Business Associates must be followed. See Beam's Business Associate Subcontractor Agreement Procedure for Beam's internal procedure for entering into Business Associate Agreements.

Section 6: Policy on Notices

An individual has a right to adequate notice of the uses and disclosures of the individual's PHI that may be made by or on behalf of Beam, and of the individual's rights and Beam's legal duties with respect to the individual's PHI. Beam shall give adequate notice of the uses and disclosures of PHI that may be made by Beam, and of the individual's rights and Beam's legal duties with respect to PHI.

When Notice Is Required

Beam must provide notice:

1. To individuals enrolled in Beam services;
2. Thereafter, at the time of enrollment, to individuals who are new enrollees;
3. In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation;
4. Within 60 days of a material revision to the notice, to individuals enrolled in Beam services.

Once every two (2) years, Beam shall notify individuals enrolled in Beam services of the availability of the notice and how to obtain the notice.

A Joint Notice of Privacy Practices is available to Beam members on the Lighthouse Portal and is included as part of the Group's Policy Documents. An acknowledgment is not required for:

1. Revised notices; or
2. Periodic notice on availability of notice and how to obtain notice.

Making Notice Available

Beam shall post the notice in a clear and prominent location on Beam's website where it is reasonable to expect individuals seeking service from Beam to be able to read the notice. A Joint Notice of Privacy Practices is available on Beam's website at https://www.beambenefits.com/

Whenever the notice is revised, Beam shall make the notice available upon request on or after the effective date of the revision and shall promptly post to its website as required in this paragraph.

Notice of Revisions

1. When there is a material change to the uses or disclosures, the individual's rights, Beam's legal duties, or other privacy practices described in the notice, Beam shall provide a notice of such change.
2. Notice of material changes shall be made no later than 60 days after the change is effective.
3. The notice shall incorporate all material changes and shall be distributed in accordance with this policy within the time period required in this policy.
4. Except when required by law, a material change to any term may not be implemented prior to the effective date of the notice reflecting the change.
5. Beam is not required to obtain acknowledgment of a revised notice.

Requirements for Electronic Notice

1. The notice must be posted on the website and be made available electronically through the website.
2. Beam may provide the notice required by this section to an individual by email, if the individual agrees to electronic notice and such agreement has not been withdrawn. If Beam knows that the email transmission has failed, a paper copy of the notice must be provided to the individual. Notice that is provided in accordance with this section and in a timely manner is sufficient to meet HIPAA requirements.
3. The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from Beam upon request.

Documentation

Beam shall retain copies of the notices issued by Beam and any written acknowledgements of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment. Copies of such notices shall be retained for a period of at least seven (7) years from the later of the date of creation of the notice or the last effective date of the notice. Acknowledgments or documentation of good faith efforts to obtain acknowledgment shall be retained for a period of at least seven (7) years from the date of receipt.

Section 7: Policy on Individuals' access to PHI

In general, an individual has a right of access to inspect and obtain a copy of PHI about the individual in a designated record set, for as long as the PHI is maintained in the designated record set, subject to any limitations imposed by applicable law.

At the request of an eligible person or the person's guardian or, if the eligible individual is a minor, the individual's parent or guardian, Beam, in collaboration with legal, or a Beam business associate shall provide the person who made the request access to records and reports regarding the eligible individual. On written request, Beam or a Beam business associate shall provide copies of the records and reports to the eligible person, guardian, or parent.

1. Verification

Beam must take reasonable steps to verify the identity of an individual making a request for access. See the HIPAA Identity Verification Requirements on Confluence for more specific information on Beam's internal process.

1.1 Form of Access

Beam shall provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by Beam and the individual.

If an individual requests an electronic copy of PHI that is maintained electronically in one or more designated record sets, Beam shall provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by Beam and the individual, with the expectation that there would be at least a machine readable form of the record. The Department of HHS considers machine readable data to mean digital information stored in a standard format enabling the information to be processed and analyzed by computer. For example, this would include providing the individual with an electronic copy of the PHI in the format of MS Word or Excel, text, HTML, or text-based PDF, among other formats. 78 Fed. Reg. 5631.

A hard copy may be provided if the individual decides not to accept any of the electronic formats offered by Beam.

An individual may instruct Beam to convey electronic versions of PHI to third parties. The request must be made in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the PHI.

Beam may allow the individual to inspect the PHI without copies, if the individual agrees to an inspection only.

1.2 Summary

Beam may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI or may provide an explanation of the PHI to which access has been provided, if both of the following apply:

1. the individual agrees in advance to such a summary or explanation; and
2. the individual agrees in advance to the fees imposed, if any, by Beam for such summary or explanation.

1.3 Fees for Copying

Beam or a Beam business associate may charge a reasonable fee to cover the costs of copying. Beam or a Beam business associate may waive the fee in cases of hardship.

1.4 Denial of Access

If access is denied, Beam must give written notice in plain language and include the following:

1. The basis for the denial;
2. If applicable (i.e. reviewable), the individual's right to have the decision reviewed and how to request such a review;
3. A description of how the individual may complain to Beam or the Secretary of HHS.

Beam must, to the extent possible and within the above timeframes, provide the individual with access to any other PHI requested, after excluding the PHI to which Beam has a ground to deny access as provided for in Section 1.5.

1.5 Review of Denial of Access

Under certain limited circumstances, Beam may deny an individual's request for access to all or a portion of the PHI requested. There are circumstances in which a denial to access may be reviewed and circumstances in which a denial to access may not be reviewed. An individual has a right to have the reviewable ground for denial reviewed by a licensed health care professional designated by the covered entity who did not participate in the original decision to deny.

Unreviewable Grounds for Denial:

A. The request is for psychotherapy notes, or information compiled in reasonable anticipation of, or for use in, a legal proceeding.

B. The requested PHI is in a designated record set that is part of a research study that includes treatment (e.g., clinical trial) and is still in progress, provided the individual agreed to the temporary suspension of access when consenting to participate in the research. The individual's right of access is reinstated upon completion of the research.

C. The requested PHI is in Privacy Act protected records (i.e., certain records under the control of a federal agency, which may be maintained by a federal agency or a contractor to a federal agency), if the denial of access is consistent with the requirements of the Act.

D. The requested PHI was obtained by someone other than a healthcare provider (e.g., a family member of the individual) under a promise of confidentiality, and providing access to the information would be reasonably likely to reveal the source of the information.

Reviewable Grounds for Denial:

A. The access requested is reasonably likely to endanger the life or physical safety of the individual or another person. This ground for denial does not extend to concerns about psychological or emotional harm (e.g., concerns that the individual will not be able to understand the information or may be upset by it).

B. The access requested is reasonably likely to cause substantial harm to a person (other than a healthcare provider) referenced in the PHI.

C. The provision of access to a personal representative of the individual that requests such access is reasonably likely to cause substantial harm to the individual or another person.

If the denial was based on a reviewable ground for denial as provided for above and the individual requests a review, Beam must promptly refer the request to the designated reviewing official. The reviewing official must determine, within a reasonable period of time, whether to reaffirm or reverse the denial. Beam must then promptly provide written notice to the individual of the determination of the reviewing official, as well as take other action as necessary to carry out the determination.

2. Policy On Individuals' Right to Request Restrictions on Disclosure of PHI

Beam may voluntarily agree to restrict the disclosure of information. Beam is not required to agree to such restrictions, unless the disclosure is to a health plan, and involves PHI related to payment or health care operations and pertains to a health care item or service for which the individual has paid out of pocket in full. If there is such an agreement in place regarding an individual's request to restrict the disclosure of PHI, Beam shall abide by the terms of the agreement, unless and until the agreement is rescinded in accordance with Beam procedures.

2.1 Verification

Beam must take reasonable steps to verify the identity of an individual making a request for restrictions on disclosure of PHI.

2.2 Form of request

Any request for restriction shall be in writing. Such request shall be construed as an objection to disclosure when applicable law gives the individual the opportunity to object to disclosure.

2.3 Consideration of request

Beam is not obligated to agree to any requests for restriction except that Beam must agree to a request to restrict disclosure of PHI to a health plan if the disclosure is for payment or health care operations and pertains to a health care item or service for which the individual has paid out of pocket in full.

2.4 Limitations on restrictions

No restriction on use of information shall apply in any of the following circumstances:

1. Emergencies where disclosure is necessary to prevent serious injury to the individual or others.
2. When required for investigations by entities with authority to investigate compliance with applicable requirements.
3. When applicable requirements do not require an authorization or an opportunity to object.

2.5 Confidential communications requests

Beam shall permit individuals to request in writing and must accommodate reasonable requests by individuals to receive communications of PHI from Beam by alternative means or at alternative locations.

Beam may condition the provision of a reasonable accommodation on:

1. When appropriate, information as to how payment, if any, will be handled; and
2. Specification of an alternative address or other method of contact.

2.6 Terminating a restriction

Beam may terminate its agreement to a restriction, if:

1. The individual agrees to or requests the termination in writing;
2. The individual orally agrees to the termination and the oral agreement is documented; or
3. Beam informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after it has informed the individual.

If an agreement to a restriction is terminated, Beam shall document the termination and give notice of such to all workforce members with access to the individual's PHI and to all of Beam's business associates who have access to the individual's PHI. Such notice shall clarify that the termination is effective only with respect to PHI created or received after the individual provided notice of the termination to Beam or after Beam informed the individual of the termination of the agreement to a restriction.

3 Policy On Individuals' Right to Request Amendment of Records of PHI

Subject to the rules set forth in applicable requirements and Beam policies and procedures, an individual has the right to have Beam amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

Beam may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

1. Was not created by Beam or its' carrier partners, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;
2. Is not part of the designated record set;
3. Would not be available for inspection under an individual's right to request access regulations; or
4. Is accurate and complete.

3.1 Verification

Beam must take reasonable steps to verify the identity of an individual making a request for amendment.

3.2 Request for amendment

An individual may request amendment of PHI about the individual held by Beam or a person or entity with which Beam has a business association relationship. Such requests must be in writing.

3.3 Refusal of amendment

1. Notice

If an amendment is denied, Beam must give written notice in plain language which includes the following:

A. The basis for the denial;

B. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

C. A statement that, if the individual does not submit a statement of disagreement, the individual may request that Beam provide the individual's request for amendment and the denial with any future disclosures of PHI that is the subject of the amendment; and

D. A description of how the individual may complain to Beam or the Secretary under the rules. The description must include the name, or title, and telephone number of the contact person or office.

Statement of disagreement or correction

Beam must permit the individual to submit to Beam a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. Beam may reasonably limit the length of a statement of disagreement.

Rebuttal statement

Beam may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, Beam must provide a copy to the individual who submitted the statement of disagreement.

Future disclosures

Future disclosures of covered records must include relevant amendments and rebuttals. Records must allow review of the statements of disagreement and rebuttals.

If an individual has not submitted a statement of disagreement, Beam must include the following with all subsequent disclosures:

A. The individual's request for an amendment; and

B. Beam's notice of denial.

If the disclosure that was the subject of amendment was transmitted using a standard EDI format, and the format does not permit including the amendment or notice of denial, Beam may separately transmit the information to the recipient of the transaction in a standard EDI format.

3.4 Designation and Documentation

The Privacy Officer of Beam, or designated personnel, shall be responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by applicable requirements and Beam procedures.

4. Policy on Accounting of Disclosures of PHI

If Beam discloses an individual's identity or releases a record or report regarding an eligible individual without authorization of the individual, Beam shall maintain a record of when and to whom the disclosure or release was made. Inquiries related to accessing this accounting of disclosures should be directed to Beam's Security Officer.

4.1 General

If Beam discloses an individual's identity or releases a record or report regarding an eligible individual, and there is no authorization for such disclosure, Beam shall maintain a record of when and to whom the disclosure or release was made.

4.2 Verification

Beam must take reasonable steps to verify the identity of an individual making a request for an accounting of disclosures.

4.3 Request for Accounting; Fees

An individual requesting an accounting shall do so in writing. The individual's request must state the period of time desired for the accounting, which must be within the six (6) years prior to the individual's request. The first accounting is free but a fee will apply if more than one request is made in a 12-month period.

4.4 Content of Accounting

The accounting must be in writing and include the following for each disclosure:

1. The date of the disclosure;
2. The name of the entity or person who received the PHI and, if known, the address of such entity or person;
3. A brief description of the PHI disclosed; and

4. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement:

A. A copy of the individual's written authorization under the rules; or

B. A copy of a written request for a disclosure, if any.

4.5 Accounting for Multiple Disclosures to Same Recipient

If, during the period covered by the accounting, Beam has made multiple disclosures of PHI to the same person or entity for monitoring purposes or for disclosures required by law, the accounting may be limited, with respect to such multiple disclosures, and include:

1. The information required by section 4.4 for the first disclosure during the accounting period;
2. The frequency, periodicity, or number of the disclosures made during the accounting period; and
3. The date of the last such disclosure during the accounting period.

4.6 Designation and Documentation

The Privacy Officer of Beam, or designated personnel, shall be the person responsible for receiving and processing requests for accountings by individuals and ensure that Beam retains documentation relating to disclosures for at least six (6) years or as otherwise required by applicable requirements and Beam procedures.

4.7 Exceptions for Accounting Requirement

Beam will not provide accounting for the following disclosures:

1. To carry out treatment, payment and health care operations, except that PHI maintained electronically is subject to accounting for two (2) years prior to the request;
2. To individuals of PHI about them;
3. Incident to a use or disclosure otherwise permitted or required by the HIPAA Privacy Rules;
4. Pursuant to an authorization;
5. For the facility's directory or to persons involved in the individual's care or other notification purposes;
6. For national security or intelligence purposes;
7. To correctional institutions or law enforcement officials;
8. As part of a limited data set; or
9. That occurred prior to the compliance date for Beam.

Section 8: Policy on Notice of Breach

In the event of a breach of unsecured PHI, Beam shall provide notice of breach in accordance with applicable requirements. Notice shall be provided to Beam's insurance carrier partner, the affected individual (if applicable), and the Secretary of HHS (if required). Beam shall take all steps reasonably necessary to ensure that business associates provide notice of such a breach to Beam, as provided for in the terms of any applicable business associate agreement.

1. Presumption of Breach

Any impermissible use or disclosure of PHI is presumed to be a breach unless Beam or the business associate, as applicable, demonstrates by a risk assessment that there is a low probability that the PHI has been compromised. Refer to the HIPAA or Data Privacy Incident Assessment Procedure.

1.1 Risk Assessment

Beam, and/or a business associate of Beam if contractually obligated, shall conduct a risk assessment to determine whether there is a low probability that data has been compromised. A risk assessment shall document that the following areas have been considered:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

1.2 Notice of Breach to Insurance Carrier Partners

Following the discovery of a breach of unsecured PHI, Beam shall notify its insurance carrier partners as provided for pursuant to applicable law and contractual obligations. In notifying Beam's insurance carrier partners, the following information will be provided:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2. A description of the types of unsecured PHI involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. A brief description of what Beam is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
4. Contact procedures for individuals to ask questions or learn additional information.

1.3 Notice of Breach to Individual

Beam, to the extent required by law or by contractual obligation, will notify each individual whose unsecured PHI has been, or is reasonably believed by Beam to have been, inappropriately accessed, acquired, used, or disclosed. The notice must be written in plain language and to the extent possible, must include all of the following:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2. A description of the types of unsecured PHI involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. A brief description of what Beam is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
4. Contact procedures for individuals to ask questions or learn additional information.

1.4 Method of Notice

Beam shall provide notice of breach to an individual, if applicable pursuant to law and/or contractual obligation, in one of the following two formats, depending on the circumstances:

1. Written notice.

    A. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail.

    B. If Beam knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first class mail to either the next of kin or personal representative of the individual.

2. Substitute notice.

    A. In the case that contact information is not available, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in where the individual is deceased;

    B. In the case in which contact information is not available for fewer than ten (10) individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

    C. In the case in which contact information is not available for ten (10) or more individuals, then such substitute notice shall:

        i. Be in the form of either a conspicuous posting for a period of 90 days on the homepage of the website of Beam, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

        ii. Include a toll-free phone number that remains active for at least 90 days that an individual can call to learn whether the individual's unsecured PHI may be included in the breach.

3. Additional Notice In Urgent Situations

In any case deemed by Beam to require urgency because of possible imminent misuse of unsecured PHI, Beam may, in addition to providing written notice, contact individuals by telephone or other means, as appropriate.

1.5 Notice to Secretary of HHS

For a breach of unsecured PHI involving more than 500 residents, Beam shall, if required by applicable law and/or contractual obligation, notify the Secretary of HHS in the manner specified on the HHS website. For breaches of unsecured PHI involving less than 500 individuals, Beam shall maintain a log or other documentation of such breaches and provide the same to its insurance carrier partners. If directed by its insurance carrier partners, Beam shall, not later than 60 days after the end of each calendar year, provide notice to the Secretary of HHS of breaches occurring during the preceding calendar year, in the manner specified on the HHS website.

1.6 Notice to Media

For a breach of unsecured PHI involving more than 500 residents, Beam shall, if required by law or contractual obligation, notify prominent media outlets serving the county. The content of the notice shall be the same as the notice provided to the individual. Before any notice to the media is provided, the notice must be reviewed by Beam's insurance carrier partner, Beam's marketing department, and Beam's legal department.

1.7 Timeliness of Notice

Beam shall provide required notices without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

Beam shall delay providing notice if a law enforcement official states to Beam or its business associate(s) that providing notice would impede a criminal investigation or cause damage to national security. If such a statement is in writing and specifies the time for which a delay is required, Beam or its business associate(s) shall delay such notice for the time period specified by the official. If the statement is made orally, Beam or its business associate(s) shall document the statement, including the identity of the official making the statement, and delay the notice temporarily and no longer than 30 days from the date of the oral statement, unless the law enforcement official submits a written statement during that time.

1.8 Determination of Time of Discovery of Breach

A breach shall be treated as discovered by Beam or its business associate(s) as of the first day on which such breach is known to Beam, or, by exercising reasonable diligence would have been known to Beam. Beam shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent or business associate of Beam.

When a business associate who is not acting as an agent discovers a breach, the date of discovery for Beam is the date when the business associate notifies Beam of the breach.

1.9 Reporting a Potential HIPAA Breach

Beam workforce members are required to submit a Report of Potential HIPAA or other Data/Privacy Incident form immediately upon discovery of a potential HIPAA breach.

Section 9: Policy on Individual Complaints and Grievances

Beam shall permit individuals to make complaints about Beam's HIPAA policies and procedures and/or Beam's compliance with those policies and procedures. Beam shall document all such complaints. Beam employees are expected to follow the Complaints Management Procedure for all such complaints.

Beam employees shall utilize the Complaint Form to permit individuals to make complaints about Beam's policies and procedures of use or disclosure of PHI and/or Beam's compliance with those policies and procedures.

The Privacy Officer and other persons designated to receive such complaints shall be notified of each such complaint and shall participate in the review of such complaints.

Beam shall inform individuals who have made a complaint under this section of their right to file a complaint with the Secretary of Health and Human Services and/or the Ohio Attorney General. Upon request, the Privacy Officer shall assist the individual in filing a complaint with the Secretary of HHS and/or the Ohio Attorney General.

Beam shall document all complaints received and the disposition of each complaint, if any. Documentation shall be maintained in accordance with 45 CFR §164.530(j), or six (6) years.

Section 10: Policy on Business Associates

Beam shall not disclose PHI to any person or entity under contract with Beam or subcontractor of a business associate, without a business associate agreement or Memorandum Of Understanding (MOU) that conforms to requirements applicable to business associate relationships unless such disclosure is otherwise permitted under federal or state law or by a valid authorization. Please see Beam's Business Associate Subcontractor Agreement Procedure for Beam's internal procedure for entering into Business Associate Agreements.

1. Business Associate Agreements

HIPAA requires a business associate agreement with any person or entity that is not a member of Beam's workforce and is receiving or creating PHI on behalf of Beam in order to perform services. Similar agreements are required for subcontractors of a business associate. The business associate agreement must meet the requirements of 45 CFR §164.504(e).

Both HIPAA requirements and Ohio law must be followed, as HIPAA requires business associate agreements, and Ohio law requires contracts and, under some circumstances, authorizations as well for disclosure to business associates.

1.1 Disclosure of PHI to the Business Associate or Subcontractor

Under HIPAA if a business associate agreement is in effect, no authorization is required from the individual whose PHI is being shared with the business associate or subcontractor. The way in which the PHI is shared must conform to the terms of the business associate agreement.

1.2 Identifying Who Is a Business Associate

A business associate is as defined in the Policy Definitions found in Section 1. Additionally, the term is further explained in 45 CFR §160.103.

1. Business associate functions and activities include, but are not limited to:

A. claims processing, billing or administration;

B. data analysis, processing or administration;

C. utilization review;

D. quality assurance; and

E. SSA activities or MUI investigations if not done by Beam workforce members.

2. Business associate services include but are not limited to:

A. Legal;

B. Actuarial;

C. Accounting;

D. Consulting;

E. Data aggregation;

F. Management;

G. Administrative;

H. Accreditation; and

I. Financial.

1.3 Review of existing contracts

Beam shall review all current contracts with any person or entity outside the workforce at least annually to determine whether there is a business associate relationship.

If the relationship meets the requirements for a business associate, Beam shall determine whether the existing contract with the person or entity meets the requirements for a business associate agreement as set forth in these policies and applicable law.

If there has been a change in the relationship and a business associate agreement is required, Beam shall not disclose PHI to such person or entity until the business associate agreement requirements are met through revision to the contract or an addendum.

When a contract extends into multiple years or automatically renews, the contract must be reviewed each year to evaluate compliance with requirements for business associate agreements. If the contract is with a business associate and does not meet business associate requirements the contract shall be amended to conform to business associate requirements or a business associate addendum shall be added.

Beam shall require business associates and subcontractors to demonstrate that any contracts between the business associate or subcontractor and its subcontractors or agents meet requirements of HIPAA rules if the subcontract involves PHI and business associate functions.

1.4 Entering into Business Associate Agreements

1. If Beam is entering into a new relationship with a business associate or subcontractor, Beam personnel shall provide the business associate or subcontractor a copy of Beam's Business Associate Agreement template to be signed by both parties. Before any PHI can be shared with a business associate or subcontractor, an executed business associate agreement must be obtained.

2. If a business associate or subcontractor insists on utilizing a business associate agreement that is not Beam's Business Associate Agreement template, such business associate agreement must be provided to legal for review and approval before execution.

3. If there is an existing contract between a business associate or subcontractor and Beam involving PHI that does not meet the requirements set forth in these policies or applicable law, the Beam employee responsible for the relationship must secure either:

    A. An addendum to the original contract which incorporates business associate agreement elements as provided herein and by applicable law; or

    B. A separately executed business associate agreement that incorporates all of the legally required elements.

4. Only one business associate agreement is required for each business associate, regardless of the number of functions which the business associate performs on behalf of Beam.

1.5 Required Elements for Business Associate Agreements

Those elements that must be included in a business associate agreement can be found in the terms of Beam's Business Associate Agreement template, located on Ironclad found here. Any questions regarding the required elements for a business associate agreement should be directed to legal.

1.6 Violations

If Beam knows of a pattern or practice of the business associate that amounts to a material violation of the agreement, Beam should immediately notify legal. An attempt to cure the breach or end the violation should be made. If such an attempt is unsuccessful, the agreement may need to be terminated, if feasible. If it is not feasible to terminate the agreement, then the problem may need to be reported to the U.S. Secretary of Health and Human Services.

Section 11: E-discovery Policy – Production and Disclosure

It is the policy of Beam to produce and disclose relevant information and records in compliance with applicable laws and court procedures during the litigation process. Please see Beam's Responding to a Subpoena, Lawsuit, or Legal Request Procedure for more information. Any questions or inquiries regarding the production or disclosure of information pursuant to applicable laws or court procedures should be directed to legal.

1. Responsibilities in Responding to a Request to Produce or Disclose:

Upon receipt of a legal request for information, Legal, in collaboration with other relevant business partners, will take the following steps:

- Review the subpoena to determine that all required elements are contained therein, the parties and the purpose are clearly identified, and the scope of information requested is clear.
- Verify appropriate service of the subpoena and that Beam is under legal obligation to comply;
- If the subpoena requests "any and all records," work with the judge and/or the requesting party's attorney to clarify the scope and type of information being requested.

    A. Legal services, such as outside counsel or discovery/litigation consultants, that have access to PHI will need to sign a business associate agreement with Beam. Beam shall execute the business associate agreement as appropriate.

- Legal services will work to identify the potential sources of information which may hold potentially relevant information, such as:

    A. LAN for the office;

    B. Personal shares or personal folders on servers;

    C. Dedicated servers for Beam;

    D. Laptop and/or department computers;

    E. Home computers, cellphones, tablets, etc.;

    F. E-mail, including archived e-mail and sent e-mail;

    G. E-mail trash bin, desktop recycle bin;

    H. Text/instant message archives;

    I. Removable storage media (e.g., CDs, DVDs, memory sticks and thumb drives);

    J. Department/office files such as financial records;

    K. Personal desk files;

    L. Files of administrative personnel in department/office;

    M. Files located in department/office staff home;

    N. Web site archives.

- Based on direction from legal services on the potential locations of relevant information and the information agreed upon in the discovery plan and/or subpoena, establish search parameters (individual identifiers, search terms, key words, etc.) and conduct the search process.
- Maintain a record of the systems searched, search methodology, search parameters (terms), and search results.
- Screen or filter the search results, eliminating inappropriate information (e.g., wrong individual, outside the timeframe, not relevant to the proceeding, etc.).

- Review the content of the data/data sets found to determine relevance to the proceeding and identify information that is considered privileged.
- Determine the final list of relevant data/data sets, location, and search methodology.
- Determine the format in which the information will be disclosed, such as: paper, ASCII, PDF, TIF, screen shot, mirror copy of data file, or review of material on-line.

  A. The format will vary depending on data, source, and agreement made in the business associate agreement or as requested in the subpoena or discovery document.

- Produce the information in the agreed-upon format as outlined in the business associate agreement or as requested in the subpoena or discovery document, if feasible.
- Mask, redact, or retract non-relevant, privileged, or confidential information (such as on a different patient) as appropriate.
- Conduct final review of information before disclosing to the requesting party.
- Retain a duplicate of information disclosed to the requesting party.
- For the information searched and disclosed, calculate the costs for search, retrieval, and disclosure methods using Beam's established formula and state or local governmental formulas for reproduction charges.
- Invoice requesting parties for allowable charges related to the reproduction of health information and records.
- Determine whether other expenses may be charged in accordance with the discovery plan or negotiation with litigants and/or judge.
- Retain information on all searches; including methodology, key words, and systems used in case the methodology has to be recreated for testing purposes and to determine if the sample was statistically valid.
- Assign a monitor for the outside party during their testing protocols.
- Determine the procedures for allowing legal services to review the electronic records and search results on-line. This includes where the review will occur, system access controls, monitoring during the review session, and the charges, if any.
- Prepare for access by identifying the types of information that party is allowed to access. If an authorization has been signed by an individual or legal representative, allow access to legal medical records and/or other information as outlined in the authorization. If other types of information will be reviewed, access is allowed based on the subpoena, court order, state/federal statutes, or agreed-upon discovery plan.
- Legal services will be responsible for managing the process for completion of any interrogatories and will coordinate processes related to depositions and testifying in court.
- Beam, its workforce members, and/or its business associates may be required to provide information for an interrogatory, be deposed, or testify in court. Prior to participating in any of these activities, Legal will consult with and advise the impacted workforce members and/or business associates.

Section 12: Building Security

This policy outlines the procedures for granting, modifying, and terminating physical access to the facilities, workstations, and electronic information systems that may contain PHI/ePHI. Beam has adopted this policy to ensure the confidentiality, integrity, and availability of PHI/ePHI, business, and proprietary information within Beam's information systems and/or applications in accordance to the HIPAA Security Rule 164.310 and its implementation specifications.

Physical access to all of Beam's facilities is limited to only those authorized. In an effort to safeguard PHI/ePHI, the facility(ies), and systems and/or applications from unauthorized access, tampering, and theft, access to designated areas is only permitted to those persons authorized to be in them and with escorts for unauthorized persons.

All workforce members are responsible for reporting an incident of an unauthorized visitor and/or unauthorized access to Beam's facility(ies) to those areas containing PHI/ePHI on information systems and/or applications to the Privacy Officer, Security Officer or Office Manager.

Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment.

1. Facility Security Measures

Areas and facilities containing PHI/ePHI are locked outside of normal business hours. Elevator access before 8:00 am and after 5:00 pm is only available by swipe card. Swipe cards also control access to the stairwells, which have locked doors. The building in which Beam is located is equipped with security cameras to record activities in the parking lot; within the area encompassing the front entrance; and within the area immediately before boarding the elevators. All activities in these areas are recorded on a 24 hour a day 365 day per year basis.

Only authorized workforce members receive a swipe card to access Beam's workspace. Workforce members are required to return their swipe card to HR on their last day of employment or last day of contracted work or services. Workforce members must report a lost and/or stolen swipe card to HR.

All other individuals who exit the elevator who are not a Beam employee must stop at the front desk to check-in.

1.1 Fire Protection

Use of local building codes will be observed. Manufacturer's recommendations on the fire protection of individual hardware will be followed.

1.2 Visitor Policies

Only workforce members are permitted in areas where PHI/ePHI is stored and are provided access as needed to perform their job duties. Visitors to areas of the facility where PHI/ePHI is stored or may be accessed will be expected to sign a non-disclosure agreement at the front desk before accessing any such areas. Visitors to these areas must also be accompanied or escorted by a Beam workforce member who has been granted access to the location. Beam workforce members are expected to shield from view any PHI/ePHI when a visitor is in the area.

Beam employees are responsible for identifying any visitors who are in a restricted area without an escort and are expected to redirect the visitor to the front desk. Any visitor who does not respond appropriately should be immediately reported to the Office Manager. If necessary, the Office Manager may ask the visitor to leave.

Section 13: Policy on Sanctions

Workforce members are subject to disciplinary action for violation of Beam's privacy policies and procedures. Violations that jeopardize the privacy or security of PHI/ePHI are particularly serious. This seriousness will be reflected in the nature of the disciplinary action imposed, up to and including termination of employment.

It is the responsibility of Beam workforce members to report known or suspected privacy or security violations to their direct manager. HR, in collaboration with the Privacy Officer, the employee's direct manager, the Security Officer (if appropriate), and legal (if necessary), are responsible for taking disciplinary action for privacy and security violations.

The Privacy Officer, in collaboration with legal, HR and IT, will investigate and document all alleged violations of Beam's privacy policies and procedures, and their eventual resolution.

Beam will apply and document the application of appropriate sanctions against workforce members who fail to comply with Beam's privacy policies and procedures or applicable requirements.

Beam expressly prohibits any form of retaliation against individuals who: raise issues related to the potential violation of Beam's privacy policies and procedures; file a complaint, participate in an investigation, compliance review or hearing; or oppose any act or practice made unlawful by the HIPAA Privacy or Security Rules. Sanctions may not be applied in a manner which would be reasonably construed as intimidation or retaliation.

Types of Violation

Listed below are the types of violations that require sanctions to be applied. They are stated at levels 1, 2, and 3, depending on the seriousness of the violation. Level 3 represents the most serious violations.

Level 1

- Accessing information that you do not need to know to do your job.
- Sharing computer access codes (user name & password).
- Leaving computer unattended while being able to access sensitive information.
- Disclosing sensitive information with unauthorized persons.
- Copying sensitive information without authorization.
- Changing sensitive information without authorization.
- Discussing sensitive information in a public area or in an area where the public could overhear the conversation.
- Discussing sensitive information with an unauthorized person.
- Failing/refusing to cooperate with the Security Officer, Privacy Officer, and/or authorized designee.

Level 2

- Second occurrence of any Level 1 offense (does not have to be the same offense).
- Unauthorized use or disclosure of sensitive information.
- Using another person's computer access code (user name & password).
- Failing/refusing to comply with a remediation resolution or recommendation.

Level 3

- Third occurrence of any Level 1 offense (does not have to be the same offense).
- Second occurrence of any Level 2 offense (does not have to be the same offense).
- Obtaining sensitive information under false pretenses.
- Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm.

While the ultimate determination on what, if any, disciplinary action will be taken is within the sole discretion of Beam, the Privacy and Security Officers will work with the appropriate Beam officers (HR and legal) to assure the appropriate disciplinary action is taken for known violations.

Section 14: Policy on Document Retention

Beam shall maintain written or electronic copies of all policies and procedures, communications, actions, activities or designations as is required to be documented under HIPAA for a period of seven(7) years from the later of the date of creation or the last effective date or such longer period that may be required under state or other federal law. Information regarding Beam's retention schedule can be found here https://www.beambenefits.com/

1. Changes to Retention Schedule

Proposed changes to the record retention schedule will be submitted to the Governance Committee for review and approval. The Governance Committee will review and research the legal, fiscal, administrative, and historical value of the records to determine the appropriate length of time the records should be maintained.

1.1 Retention of Related Computer Programs

Retention of records implies the inherent ability to retrieve and view a record within a reasonable time. Retained electronic data must have retained with it the programs required to view the data. Where it not economically feasible to pay for maintenance costs on retired or obsolete hardware or software only for the purpose of reading archived or retained data, the data may be converted to a more supportable format, as long as it can be demonstrated that the integrity of the information is not degraded by the conversion.

1.2 Retention of Records in Large Applications

Retention of data for large-scale applications, typically those that reside in the data center and are accessed by a larger audience, shall be the responsibility of the IT department.

1.3 Retention of Records on Individual Workstations

Primary responsibility for retention of data created at the desktop level shall be with the workforce member/author. The workforce member /author will ensure that the documents are properly named and saved to be recognizable by the user in the future, and physically saved to the appropriate drive. By saving a copy in this manner, the IT department will be able to create an archived version of the saved document for seven (7) years after the user deletes the copy from the shared drive. Documents with retention periods in excess of this period will require an alternative means of retention. Users are responsible for the security of any confidential information and/or PHI/ePHI created or maintained on their workstations.

2. Policy on Document Destruction

Beam will dispose of all documents containing PHI that have satisfied their legal, fiscal, administrative, and archival requirements in accordance with federal, state, and/or local law. Records must be destroyed in a manner that ensures the confidentiality of the records and renders the information unrecognizable.

Section 15: Training of Workforce

All current Beam workforce members must be trained on applicable policies and procedures relating to HIPAA and PHI/ePHI as necessary and appropriate for such persons to carry out their functions within Beam. Each new workforce member shall receive the training as described above within a reasonable time after joining Beam. Further, all personnel who work remotely must complete the same annual privacy training as all other employees. Each workforce member whose functions are impacted by a material change in the policies and procedures relating to HIPAA and PHI/ePHI, or by a change in position or job description, must receive the training as described above within a reasonable time after the change becomes effective. Additionally, all workforce members are expected to complete HIPAA and other related training annually.