Policy:
HIPAA Policies and Procedures Manual - US

LifeWorks

Table of Contents

1. Introduction

1.1. Purpose and Application

LifeWorks (US) Ltd. ("LifeWorks" or "Company") is committed to maintaining the privacy and confidentiality of Protected Health Information (PHI) in compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended, and the regulations promulgated pursuant thereto (hereinafter referred to as the "the Privacy Rule"), as well as other federal, state and local laws, rules and regulations related to the collection, use and disclosure of PHI.

LifeWorks performs services as both a Covered Entity, as well as a Business Associate for certain of its clients who are themselves Covered Entities, or even in some cases, for clients who are themselves Business Associates of a Covered Entity. This HIPAA Privacy Policy (the "Policy") sets forth the privacy policies and procedures applicable to LifeWorks to the extent that it provides services involving the collection, use and disclosure of PHI. Modifications to the Privacy Rule are expected from time to time, some of which may require amendment of this Policy. If any provision of this Policy is inconsistent with HIPAA or a more restrictive applicable state privacy law (to the extent not preempted), the Policy will be interpreted to comply with such law.

1.2. Scope

LifeWorks is committed to safeguarding and keeping confidential the PHI it uses, discloses, receives or maintains. Consistent with the requirements of the Privacy Rule, any PHI received or created by a LifeWorks line of business that may qualify as Covered Entities and/or Business Associates, may be used or disclosed solely in accordance with this Policy.

All employees, volunteers, contractors, and agents whose conduct, in the performance of work for Company, or are under the direct control of HIPAA-covered lines of business (the "Workforce") are expected to comply with the policies and procedures set forth herein. Workforce members may include individuals who act as independent contractors of the Company when performing work for the Company if designated as such by the Company. Questions about this Policy, including its applicability to independent contractors and other affiliates, should be directed to the Company's HIPAA Privacy Officer who may involve Responsible Persons (as that term is defined herein).
.

1.3. Maintenance and Amendment

This Policy is the responsibility of the HIPAA Privacy Officer. The HIPAA Privacy Officer may amend this Policy as they deem necessary or appropriate to ensure continued compliance with HIPAA, subject to the approval of the Company.

1.4. Other Company Policies

This Policy should be read in conjunction with the Company's Security Policy and other administrative policies that may affect the use and disclosure of PHI and remedial action to be taken in the event of policy violations. The HIPAA Privacy Officer is responsible for resolving any conflicts between the terms of this Policy and any other Company policy as they apply to PHI.

1.5. Policy Effective Date

This Policy is effective as of January 1, 2015 as amended from time to time. For any services provided by LifeWorks after that date, the effective date is the date on which LifeWorks first performed the services in the US.

2. Definitions

Authorization. An Individual's specific written permission, meeting the content requirements of the Privacy Rule, allowing LifeWorks to use and disclose PHI for purposes other than those described in Article 5. 45 CFR §164.508

Breach. The acquisition, access, use, or disclosure of an Individual's PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI. 45 CFR § 164.402

Business Associate. A person or entity who creates, receives, maintains, or transmits PHI for a Covered Entity or for another Business Associate. For purposes of this Policy, Business Associate shall include subcontractors that create, receive, maintain, or transmit PHI on behalf of the Company.45 CFR §160.103

Covered Entity. A health plan, a health care clearinghouse, or a health care provider that transmits health information in electronic form in connection with a transaction covered under HIPAA. 45 CFR §160.103

De-identified Information. A record in which all items of identifying information enumerated in the Privacy Rule have been removed to render the information not subject to the Privacy Rule. Even if these identifiers are removed, the Privacy Rule states that information will still be considered identifiable if the Covered Entity has a means by which to re-identify the data. (45 CFR 164.514)

Designated Record Set. A group of records that include PHI maintained by or for a Covered Entity that pertain to medical records and billing records about Individuals maintained by a health care provider; enrollment, payment, claims adjudication, medical or case management record systems maintained by a health plan; and other information used by or for the Covered Entity to make health-related decisions about Individuals. 45 CFR § 164.501

Electronic Transmissions. Includes transactions using all forms of electronic media. Such transactions include the transfer of information over the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, magnetic tape, disk, or compact disc media. 45 CFR § 160.103

Genetic Information. With respect to any Individual, information about such Individual's genetic tests; the genetic tests of family members of such Individual; the manifestation of a disease or disorder in family members of such Individual (i.e., family health history) that could be detected in a genetic test; or any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the Individual or any family member of the Individual. 45 CFR § 160.103

Health Care Operations. Certain administrative, financial, legal and quality improvement activities that are necessary to run LifeWorks business and to support the core functions of treatment and payment. 45 CFR § 164.501

HHS. The United States Department of Health and Human Services, the agency charged with interpreting and enforcing the Privacy Rule.

HIPAA. The Health Insurance Portability and Accountability Act of 1996 (as amended), and the regulations promulgated thereunder (such regulations also are known as the Privacy Rule).

HIPAA Privacy Officer. The LifeWorks employee or partner responsible for implementing and updating this Policy and for carrying out the duties assigned to them under this Policy. (See Article 3). Reference to the HIPAA Privacy Officer includes any Responsible Persons to whom the HIPAA Privacy Officer has delegated duties assigned to the HIPAA Privacy Officer.

Individual. A person (alive or deceased) who is the subject of the PHI.

Limited Data Set. Is PHI that excludes the following direct identifiers of the Individual or of relatives, employers, or household members of the Individual: names; postal address information, other than town or city, State, and zip code; telephone numbers; fax numbers; electronic mail addresses; social security numbers; medical record numbers; Health Plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; biometric identifiers, including finger and voice prints; and full face photographic images and any comparable images.

Marketing. Making a communication about a product or service that encourages recipients to purchase or use the product or service.

Minimum Necessary. The standard described in Article 4 of this Policy to limit PHI that is accessed, requested, used, disclosed, created, or transmitted in accomplishing Payment, Health Care Operations, and other functions of a Covered Entity.

Payment. Activities undertaken by a Covered Entity health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits, and by a Covered Entity health care provider or health plan to obtain or provide reimbursement for the provision of health care.

Personal Representative. A person entitled under applicable law to decide and act on behalf of an Individual with respect to the Individual's health care. For example, parents of minor children and court-appointed guardians generally are Personal Representatives. The executor, administrator, or other person with authority to act on behalf of a deceased Individual's estate will be treated as the

deceased Individual's Personal Representative. A Personal Representative is entitled to act on behalf of the Individual under this Policy.

Protected Health Information (PHI). Individually identifiable health information that (i) relates to the past, present, or future physical or mental condition of an Individual, provision of health care to an Individual, or payment for such health care; (ii) can either identify the Individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the Individual; and (iii) is received or created by or on behalf of a Covered Entity. Genetic Information shall be treated as health information.

Qualified Protective Order. An order of a court or an administrative tribunal or a stipulation by two or more parties that prohibits the parties from using or disclosing PHI for purposes other than the underlying litigation or proceeding for which the records are requested and requires the return of the PHI to a Covered Entity or the destruction of the PHI at the end of the litigation or proceeding.

Responsible Person. A Company partner or employee to whom the HIPAA Privacy Officer has delegated duties assigned to the HIPAA Privacy Officer.

Transaction. Access to, request for, receipt, transmittal, examination, and application of PHI, and other uses and disclosures of PHI as "use" and "disclosure" are defined under the Privacy Rule.

Treatment. The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Unsecured PHI. PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of the technology or methodology specified in regulations or other guidance issued by HHS. Two methods for rendering PHI unusable, unreadable, or indecipherable include encryption and destruction consistent with the National Institute of Standards Technology (NIST) Guidelines such that the PHI cannot be retrieved.

3. HIPAA Privacy Officer

3.1. Duties of HIPAA Privacy Officer

LifeWorks appointee for the role of HIPAA Privacy Officer has the following responsibilities which may be delegated where appropriate:

- Amending, implementing, updating, and interpreting this Policy;
- Providing and documenting appropriate privacy training for Workforce;
- Receiving, investigating, and responding to Individuals' complaints regarding possible impermissible uses or disclosures of PHI and related Policy violations, as described herein;
- Receiving, investigating, and responding to reports by Workforce and other employees/partners regarding possible impermissible uses or disclosures of PHI and related Policy violations or improvements;
- Providing notification of a Breach;
- Receiving and responding to requests to amend PHI maintained in a Designated Record Set, as described herein;
- Receiving and responding to requests for an accounting of disclosures of PHI, as described herein;
- Receiving and responding to requests for information by HHS for purposes of determining compliance with the Privacy Rule, as described herein;
- Approving disclosures to law enforcement or to the military for government purposes, as described herein;
- Maintaining documentation pursuant to the record-keeping requirements;
- Ensuring that Business Associate Agreements are entered into with appropriate parties; and
- Investigating and responding to any other compliance concerns under this Policy.

The HIPAA Privacy Officer may delegate any of their responsibilities under this Policy to one or more other Responsible Persons.

3.2. Responsible Persons

The HIPAA Privacy Officer and any other Company partner or employee to whom the HIPAA Privacy Officer has delegated any of their responsibilities are Responsible Persons.

4. Minimum Necessary Rule

The Company is permitted to request, use, or disclose PHI without the Individual's Authorization for the purposes set forth in Article 5. Unless otherwise provided in HHS guidance, when using and disclosing PHI, the Company must limit such PHI to a Limited Data Set or, if necessary, to the Minimum Necessary amount of PHI to achieve the particular purpose.

In addition to limiting the PHI used or disclosed, the Company must take steps to ensure that only the person needing the PHI for the intended purpose receives it. Prior to any disclosure of PHI in response to a request, the Company must take reasonable steps to verify the identity and authority of the person requesting such information. Workforce will access and use only that PHI necessary to accomplish their legitimate job duties pursuant to the Minimum Necessary standard.

5. Permitted Uses and Disclosures of Protected Health Information

The Company is permitted to use and disclose PHI (*i.e.*, engage in a Transaction) without an Authorization as set forth herein.

5.1. Uses and Disclosures for Treatment, Payment or Health Care Operations

The Company may use and disclose PHI for Treatment, Payment or Health Care Operations activities. Questions regarding whether disclosure is appropriate should be directed to the HIPAA Privacy Officer.

5.2. Disclosures to a Plan Sponsor

The Company may disclose PHI to a Health Plan sponsor without the Individual's Authorization provided the disclosure is:

- Summary health information (as defined under HIPAA) for the purpose of obtaining health insurance coverage or premium bids for the Health Plan, or for making decisions to modify, amend, or terminate the Health Plan; and
- Information regarding whether an Individual is participating in the Health Plan, or enrollment and disenrollment information.

Other than as may be permitted or required by law, LifeWorks will not use or disclose PHI to a Plan Sponsor for employment-related decisions or in connection with any other benefit program (other than workers' compensation coverage) without the Individual's Authorization. Disclosures to the Plan Sponsor must be documented for purposes of providing an Individual with an accounting.

5.3. Disclosures to Individuals, Friends or Family

The Company may disclose PHI to a family member, close personal friend, or other person identified by an Individual without an Authorization, provided that (a) such disclosure is limited to the Minimum Necessary PHI that is directly relevant to that person's involvement with the Individual's care or payment for health care, and (b) at least one of the following conditions also is met:

- The Individual agrees to the disclosure;
- The Individual is present or otherwise available and has an opportunity to agree or object to the disclosure and does not object;
- Based on professional judgment and the circumstances, it can reasonably be inferred that the Individual does not object to the disclosure; or
- The Individual is not available to agree or object, or cannot agree or object due to the Individual's incapacity (e.g., due to an emergency situation verified by a hospital), but the disclosure is in the Individual's best interest.

Uses and disclosures under these circumstances do not need to be documented for purposes of providing the Individual with an accounting.

5.4. Uses and Disclosures for Workers Compensation Purposes

The Company may disclose PHI as necessary to comply with workers' compensation and similar laws that provide benefits for work-related injuries or illnesses without regard to fault. Such disclosure must be within the Workforce member's assigned job functions of the Workforce member who makes the disclosure, and the Privacy Officer should be consulted if necessary. Uses and disclosures to comply with workers' compensation laws must be documented for purposes of providing the Individual with an accounting.

5.5. Uses and Disclosures Pursuant to Legal Proceedings and for Certain Law Enforcement Purposes

The uses and disclosures for legal and law enforcement purposes listed below are permitted under this Policy. The HIPAA Privacy Officer must be consulted prior to making any disclosures for law enforcement purposes.

5.5.1. Legal Proceedings with Court Order

The Company may, to the extent ordered, disclose PHI in the course of a judicial or administrative proceeding in response to an order from a court or an administrative tribunal. To the extent that the court order applies to PHI of an Individual, and the Individual does not otherwise have notice of the order, the Company shall first notify the Individual if permitted by law.

5.5.2. Legal Proceedings without Court Order

The Company may disclose PHI in the course of a judicial or administrative proceeding in response to a subpoena, discovery request, or other legal process not accompanied by a court order, provided one or more of the following conditions are met:

- The Company receives documentary evidence from counsel that (i) the requesting party provided or made a reasonable attempt to provide written notice to the Individual (including sufficient information to enable the Individual to raise an objection to the court or administrative tribunal), (ii) the time for raising an objection has elapsed, and (iii) either no objection was raised or all objections have been resolved in a way that permits the disclosure; or
- The Company receives documentary evidence from counsel that the requesting party obtained or made a reasonable attempt to obtain a Qualified Protective Order (i.e., an agreed

Qualified Protective Order has been presented to the court or the requesting party has sought such an order from the court or tribunal).

5.5.3. Law Enforcement

The Company may disclose PHI to a law enforcement officer for law enforcement purposes, provided the following conditions are met, as applicable:

- **Court Orders.** The disclosure is required by law or is in compliance with (i) a court order or court-ordered warrant, subpoena, or summons issued by a judicial officer; (ii) a grand jury subpoena, or (iii) an administrative request (including an administrative subpoena or summons), or a civil or authorized investigative demand or similar process authorized under law. However, information requested must be relevant and material to a legitimate law enforcement inquiry and must be limited to the extent reasonably practicable in light of the purpose of that inquiry and de-identified information could not reasonably be used.
- **Suspects, Missing Persons, etc**. The disclosure is in response to a law enforcement officer's request for the purpose of locating a suspect, fugitive, material witness, or missing person, provided that the disclosure is limited to following information:
    - name and address;
    - date and place of birth;
    - Social Security number;
    - ABO blood type and RH factor;
    - type of injury;
    - date and time of treatment;
    - date and time of death; and/or
    - distinguishing physical characteristics.
- **Victims of a Crime**. The disclosure is in response to a law enforcement officer's request for information about an Individual who is a suspected crime victim, and the Individual/victim agrees to the disclosure. If the Individual/victim is unable to agree to the disclosure because of incapacity or emergency circumstances, the Company may make the disclosure only if the law enforcement official represents in writing that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others and (i) the disclosure is necessary to determine if someone other than the Individual/victim committed a crime, (ii) it is necessary for immediate enforcement activity, (iii) it will not be used against the Individual/victim, and (iv) the disclosure is in the Individual's/victim's best interests. Non-emergency requests should be referred to the Privacy Office for evaluation and approval.
- **Crime Related to Individual's Death.** The disclosure is made to a law enforcement officer and is about a deceased Individual whose death may have resulted from a crime.
- **Crime on Company Premises.** The disclosure is made to a law enforcement officer and is evidence of a crime that occurred on the Company's premises.

5.6. Disclosures to Secretary of Health and Human Services

The Company may, with the approval of the HIPAA Privacy Officer, disclose PHI to the Secretary of HHS when requested by the Secretary of HHS for purposes of determining the Company's or a

Covered Entity client's compliance with HIPAA and the Privacy Rule. The HIPAA Privacy Officer must be consulted prior to making any such disclosures.

5.7. Uses and Disclosures for Other Government Purposes

The uses and disclosures for governmental purposes listed below are permitted under HIPAA. The HIPAA Privacy Officer must approve each such use or disclosure.

5.7.1. Armed Forces

The Company may use or disclose PHI about Individuals who are members of the Armed Forces for activities necessary to assure proper execution of a military mission, provided the appropriate military authority has published a notice in the Federal Register that includes appropriate military command authorities and permitted purposes for the use or disclosure, or to a foreign military authority regarding Individuals who are foreign military personnel for the same purpose.

5.7.2. National Security

The Company may use or disclose PHI to an authorized federal officer for intelligence, counterintelligence, or other national security activities authorized by the National Security Act, as amended.

5.7.3. Federal Protective Services

The Company may use or disclose PHI to an authorized federal officer for the provision of protective services to the President, foreign heads of state, or other designated persons, or for the conduct of investigations authorized by law.

5.7.4. Correctional Institution or Lawful Custody

The Company may use or disclose PHI to a correctional institution or law enforcement officer who has lawful custody of the Individual if the information is necessary for provision of health care to the Individual or for ensuring the health and safety of the Individual, other inmates, or correctional institution employees.

5.8. Uses and Disclosures for Health and Safety Purposes

The uses and disclosures for health and safety purposes listed below are permitted under HIPAA. The HIPAA Privacy Officer must be consulted prior to making any such disclosures.

5.8.1. Threat to Public Health or Safety

The Company may use or disclose PHI as believed necessary to prevent or lessen a serious and imminent threat to public health or safety if made to someone reasonably able to prevent or lessen the threat.

5.8.2. Abuse, Neglect, or Domestic Violence

The Company may disclose PHI of an Individual who is a suspected victim of abuse, neglect, or domestic violence to a government authority authorized by law to receive such reports. Such disclosure must meet at least *one* of the following conditions:

- Disclosure is made only to the extent required by a law;
- The Individual agrees to the disclosure; or
- The disclosure is authorized by a law or regulation, and either (i) the disclosure is necessary to prevent serious harm to the Individual or others, or (ii) the Individual is unable to agree to the disclosure because he or she is incapacitated, but, according to an official authorized to receive the disclosure, it is necessary for an immediate enforcement activity and it will not be used against the Individual.

The Company must promptly notify the Individual about the disclosure unless it believes such notification would place the Individual at risk of serious harm, or the disclosure would be made to the Individual's Personal Representative and the Company believes the Personal Representative is responsible for the injury and that informing such person would not be in the Individual's best interest.

If the abuse, neglect, or domestic violence *involves a child*, the Company may use or disclose PHI to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

5.8.3. Public Health Activities

The Company may use or disclose PHI (i) to a public health authority authorized by law to collect or receive such information for prevention purposes (*e.g.*, disease, injury, or disability), (ii) to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect, or (iii) to a person subject to jurisdiction of the Food and Drug Administration under limited circumstances (*e.g.*, to track product defects or improper labeling).

5.8.4. Health Oversight Activities

The Company may use or disclose PHI to a health oversight agency for activities authorized by law, including audits, investigations, inspections, and licensure or disciplinary actions. Health oversight activities do not include investigations or other activities in which the Individual is the subject of that investigation or activity unless it arises out of and is related to the receipt of health care, a claim for public health benefits, or eligibility for or receipt of public benefits or services when the Individual's health is integral to the claim for public benefits or services.

5.9. Uses and Disclosures Concerning Decedents

The uses and disclosures concerning decedents listed below are permitted under HIPAA. The HIPAA Privacy Officer must be consulted prior to making any such disclosures.

5.9.1. Post-mortem Identification, etc.

The Company may disclose Minimum Necessary PHI to (i) a coroner or medical examiner for purposes of identifying the decedent, determining cause of death, or other lawful purpose, or (ii) a funeral director as necessary for purposes of carrying out their duties.

5.9.2. Tissue Donation

The Company may use or disclose Minimum Necessary PHI for purposes of cadaveric organ, eye, or tissue donation to organizations engaged in procuring, banking, or transplanting such cadaveric organs, eyes, or tissues.

5.10. De-identification

To the extent permitted by any applicable contractual arrangements, the Company may use PHI to create de-identified PHI if authorized by the Privacy Officer or their designee. The Company may also disclose PHI to a business associate that will de-identify PHI on behalf of the Company. PHI may only be de-identified in accordance with the methods specified under HIPAA in Section 45 CFR 164.514 of the Privacy Rule, which include either (a) removing the 18 patient identifiers specified in HIPAA; or (b) engaging a biostatistician or other person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information as de-identified. Prior to de-identifying any PHI, the HIPAA Privacy Officer or their designee must approve of both the method used for de-identification and any uses or disclosures of the de-identified information in accordance with HIPAA.

5.11. Other Laws

In addition to the reasons listed in this Article 5, the Company may use or disclose PHI to the extent required by applicable federal, state, or local law. The HIPAA Privacy Officer must be consulted prior to making any such disclosures.

6. Individuals' Rights Regarding Protected Health Information

An Individual has a number of rights under the Privacy Rule, as described below, which may be modified and/or delegated to LifeWorks under a Business Associate Agreement, if applicable. As a result, references to the Covered Entity may also apply to LifeWorks, and all references to Individual shall include the Individual's Personal Representative. All documents relating to this Section must be retained for six (6) years from the date of creation or receipt by the Company, or longer as may be required by the Company's Records Management Policy and Schedule.

6.1. Individual Access to Protected Health Information

An Individual may request to inspect and obtain a copy of their PHI maintained by the Company within the Designated Record Set, except for information in Psychotherapy notes or compiled in preparation for legal proceedings.

6.1.1. Requirements for Requests.

- **Request for Access by Individual**. If the Individual requests a copy of their own record, the Individual must complete the appropriate form or provide a written request for their record that includes the Individual's name, date of birth and signature.
- **Request for Access to Third Party**. If the Individual (or their Personal Representative) requests that their records be sent to any third party, the request must be signed by the Individual and clearly identify (i) the third party; (ii) the format in which the records are to be sent; (iii) the method/manner of delivery; and (iv) where the records should be sent. Any third-party requests for records must include an Authorization form that is completed, signed and dated by the Individual (whose identity should be verified prior to releasing the record).

6.1.2. Responding to Requests.

Requests shall be directed to the Company Line of Business responsible for the records requested:

- **Format/Delivery**. Whenever possible, copies of records should be provided in the format and delivered in the method requested by the Individual. If the Individual requests that copies of records are to be provided in an unsecure format or form of transmission (e.g. via email), the foreseeable risk of the method of delivery requested by the Individual should be noted to the Individual in the request form.
- **Timing**. Record requests must be responded to within thirty (30) days. If an extension is necessary, the Individual must be notified in writing and provided with the reason for the delay and the anticipated date of response.
- **Fees**. The Individual may be charged a reasonable, cost-based fee associated with obtaining access to their records. Such fees shall be calculated using one of the methods permitted by HHS. The Company may impose fees for third party requests for records in accordance with applicable state law.

6.1.3. Denials

The Company shall evaluate whether to grant or deny the access request. The Company may deny a requesting Individual access in the following circumstances, so long as the Individual is given the right to have such denial reviewed in the following circumstances:

- A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the Individual or another person;
- The record requested makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
- The request for access is made by the Individual's Personal Representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such Personal Representative is reasonably likely to cause substantial harm to the Individual or to another person.

In the event the Line of Business evaluating the request chooses to deny an Individual access to their record, it must review that determination with the HIPAA Privacy Officer and/or legal counsel to ensure that such action is merited. If it is determined that a denial is merited, written notice of the denial must be provided to the Individual, in plain language, of this decision and informing the Individual of their right to have the decision reviewed and how to request such a review. The Individual must also be informed about their right to complain to the Company or HHS. All requests for such a review should be referred to the Privacy Office for evaluation.

6.2. Request for Restriction on Uses and Disclosures

An Individual has the right to request restrictions on the Company's use and disclosure of their PHI by the Company. Any request for a restriction must be made in writing on the form prescribed by the HIPAA Privacy Officer. Once completed, this form should be submitted to the Privacy Officer or their designee for a decision regarding whether the Individual's request can be honored, who will review and respond to the request within a reasonable time, but not later than forty-five (45) days after receipt.

6.2.1. Health Plan Requests for which Payment Made Out-of-Pocket.

The Company must agree to restrict disclosures of PHI to health plans when the Individual requests such a restriction and when the PHI pertains to items or services for which the Individual has paid "out of pocket in full."

6.2.2. All Other Requests.

For all other requests, if the Company agrees to a restriction, the Individual will be notified in writing, the restriction will be documented in the Individual's record, and the appropriate staff and Business Associates will be notified of the restriction as needed. The Individual will also be notified that such restriction may not be honored when the restricted PHI is: (i) needed to provide emergency treatment to the Individual; or (ii) required for uses and disclosures where an Individual's Authorization is not required (Article V of this Policy). If the request for a restriction is denied, the Individual will be notified in writing of this decision including the reasons for the denial.

6.3. Confidential Communication

An Individual has the right to request that all communications regarding their receipt of sensitive services be sent directly to them (either to the individual's contact information on file or to a designated alternative address, email, or phone number).

An Individual may make a request using the contact information below. LifeWorks will respond to requests received by email or phone within seven (7) calendar days, and requests received by first-class mail within fourteen (14) calendar days.

An Individual does not need to obtain the permission of the primary subscriber or other enrollee in order to receive sensitive services or submit a claim for sensitive services. LifeWorks will not disclose information related to sensitive health care services Individuals receive to the primary subscriber or any plan enrollees without the Individual's express authorization. An Individual's enrollment or coverage will not be affected by exercising this right.

Requests will be valid until the Individual revokes the request or submits a new one. Requests for confidential communications will apply to all communications that disclose medical information or provider name and address related to an Individual's receipt of medical services.

Requests for confidential communications can be submitted to:

By regular mail:	Privacy Office LifeWorks (US) Ltd. 115 Perimeter Center Place NE Suite 1050 Atlanta, GA 30346 United States
By electronic mail:	privacy-vieprivee@lifeworks.com
By phone:	1-800-234-5154

6.4. Amendment of Protected Health Information

An Individual may request that the Company amend their PHI to the extent that it is maintained in a Designated Record Set. The request should be submitted to the Privacy Officer or their designee.

Upon receipt of a request for amendment, the Privacy Officer or their designee will review the request and respond within sixty (60) days. A one-time extension of thirty (30) days is allowed, if necessary, provided that the Individual requesting the amendment is informed in writing of the reason for the delay and the date by which they can expect action to be taken on their request. Any amendments to the record must be made by the appropriate personnel as a separate, corrected entry, dated and timed at the time of the correction. The original entry will be retained. A patient's request for amendment may also be denied if (i) the information was not created by the Company; (ii) the information would not be available for access; or (iii) the information is accurate and complete.

6.5. Accounting for Disclosures

All disclosures of PHI made by Company or any of its Business Associates must be documented for accounting purposes, except those made: (i) pursuant to the Individual's specific written authorization; (ii) to entities external to the Company (including Business Associates) for treatment, payment or healthcare operations purposes; (iii) to friends and family, made in accordance with this Policy; (iv) to the Individual; or (v) for governmental purposes in accordance with this Policy (collectively, "Covered Disclosures").

6.5.1. Documentation

The following information must be documented for each Covered Disclosure:

- The date of disclosure;
- The name of the recipient (and address, if known);
- A description of the PHI disclosed; and
- The purpose for the disclosure (or a copy of the request for disclosure).

6.5.2. Individual Requests for Accounting.

An Individual may request an accounting of Covered Disclosures of their PHI made by the Company during any period of time falling within the six-year period before the date of the request. All requests from Individuals for an accounting of disclosures should be referred to the appropriate line of business at LifeWorks. The line of business will be responsible for performing the requested accounting and responding to the Individual.

The accounting provided to the Individual must include the information outlined above for each Covered Disclosure within the period requested.

6.5.3. Timing of Response

Within 30 days of receiving the request with appropriate identifying information, the HIPAA Privacy Officer or their designee must either provide the Individual with an accounting or provide written notice that an extension of time is needed to respond to the request. If an extension of time is needed, LifeWorks will have up to 30 additional days to provide the accounting, as long as LifeWorks notifies

the Individual in writing, before the expiration of the initial 30-day period, of the reason for the delay and the amount of additional time needed to comply.

6.5.4. Record Retention

LifeWorks must retain a record of each request for an accounting, including the request, responses to the request, the information subject to the accounting, and the written accounting provided to the Individual. Such documentation must be maintained for at least six years from the date created or last in effect, and be handled in accordance with the Company's Records Management Policy and the associated Record Retention Schedule.

6.6. Complaints

An Individual has the right to complain to the HIPAA Privacy Officer and to HHS about this Policy and/or the Company's compliance with HIPAA and the Privacy Rule. LifeWorks and its employees/partners must refrain from retaliating against or intimidating the complainant in any way for filing a complaint. The complainant and any involved employees/partners must cooperate with any investigation and other action taken in response to the complaint. No person may be intimidated, threatened, or discriminated against in any way for participating in an investigation of a complaint.

The HIPAA Privacy Officer or their designee must address each complaint promptly and confidentially. The HIPAA Privacy Officer or their designee first will investigate the complaint and document their investigation efforts and findings. To the extent that the HIPAA Privacy Officer finds that PHI has been used or disclosed in violation of this Policy or the Privacy Rule, they must take immediate steps to mitigate any harm caused by the violation. The HIPAA Privacy Officer or their designee also must take steps to minimize the possibility that such a violation will recur. Employees and workforce members found to have violated this Policy are subject to disciplinary action in accordance with the Company's policies.

The HIPAA Privacy Officer or their designee will provide a written response to the complainant if they submitted the complaint in writing (other than anonymously). The response will include a description of the investigation, the findings, and, to the extent appropriate, a description of the actions taken to mitigate harm and prevent recurrence.

The HIPAA Privacy Officer must retain documentation describing the complaint (or, if submitted in writing, a copy of the complaint), its investigation, its findings, mitigation and prevention steps, and its response (or a copy of the response). Such documentation must be maintained for a period of at least six years from the date created or last in effect and be handled in accordance with the Company's Records Management Policy and the associated Record Retention Schedule.

7. Notice of Privacy Practices

The Company will provide a Notice of Privacy Practices to Individuals, if appropriate, upon their first visit to the Provider, post it in the lobby of those locations where required, and will include a copy of such Notice on its website.

To the extent required by HIPAA, the Notice shall be provided to the Individual no later than the first date of service. The Individual or their Personal Representatives will be requested to sign a written Acknowledgment of Receipt of the Notice.

The Notice shall be updated whenever there is a material change to the uses or disclosures, Individuals' rights, legal duties or other privacy practices stated in the Notice. If the Notice is updated, the revised version will be made available to Individuals and be posted in a clear and prominent location.

8. Training Requirements

Comprehensive HIPAA training shall be included in the orientation process for all new Workforce. In addition, all Workforce shall be required to complete HIPAA training. Failure to complete the requisite HIPAA training within a timely manner may result in disciplinary action. Workforce will receive retraining regularly and more frequently if privacy or security policies and procedures change. Periodic security reminders will be provided to all Workforce to ensure awareness of security issues and concerns related to PHI.

9. Contracts Involving PHI

9.1. Business Associates

Where Company is acting as a Covered Entity, each third party, vendor or service provider that may receive, view, access, use, disclose or create PHI from the Company to perform a function on behalf of the Company (such as billing or consulting services, claims processing, data analysis, case management, utilization review, quality assurance) or provide certain specified services on behalf of the Company (such as data storage, legal, actuarial, accounting, consulting, accreditation, or financial services) is a Business Associate of Company and must enter into a Business Associate Agreement ("BAA") with the Company. Questions regarding whether a BAA is needed should be submitted to Legal or the HIPAA Privacy Officer.

9.1.1. Business Associate Agreement.

If Company is acting as a Covered Entity, all new contracts and renewal of service contracts with Business Associates will incorporate the "Company BAA" template as an exhibit to and as a part of such contract. Any requests for material deviations from or amendments to the "Company BAA" template must be submitted to Legal or the Privacy Office for approval. A Business Associate may not commence services until a BAA has been signed.

If Company is acting as a Business Associate, the Company will request that the Covered Entity in question allow Company's form of "Contractor BAA" template to be utilized. If the Contractor BAA template is used, any requests for material deviations from or amendments to the "Contractor BAA" template must be submitted to Legal or the HIPAA Privacy Officer for approval.

Upon receipt of a signed BAA from the third party/vendor, copies of the executed BAA should be forwarded promptly to the line of business vendor manager for filing. A copy of the BAA must be retained in the Company's records for a period of at least six years from the date on which the relationship is terminated and be handled in accordance with the Company's Records Management Policy and the associated Record Retention Schedule.

9.2. Subcontractors

Where Company is acting as a Business Associate, each third party, vendor or service provider that may create, receive, maintain, or transmit PHI on behalf of the Company should be evaluated to determine if they are a "Downstream Business Associate" of the Company. All Downstream Business Associates must enter into a Downstream Business Associate Agreement ("Downstream BAA") with the Company. Questions regarding whether a Downstream BAA is needed should be submitted to Legal or the Privacy Office.

9.2.1. Downstream Business Associate Agreement.

All new contracts and renewal of contracts with Downstream Business Associates will incorporate a "Company Downstream BAA" template as an exhibit to and as a part of such contract. Any requests for material deviations from or amendments to the "Company Downstream BAA" template must be submitted to Legal or the Privacy Office for approval. A Subcontractor may not commence services until a Downstream BAA has been signed.

Upon receipt of a signed Downstream BAA from the Subcontractor, copies of the executed Downstream BAA should be promptly forwarded to the line of business vendor manager or other appropriate team for filing. A copy of the Downstream BAA must be maintained for a period of at least six years from the date on which the relationship is terminated and be handled in accordance with the Company's Records Management Policy and the associated Record Retention Schedule.

9.3. Contracts between Covered Entities.

Where both the Company and the other party are Covered Entities, contracts for services that may involve the sharing of PHI shall be referred to the Privacy Office or LifeWorks Legal to determine if a BAA is necessary. Contracts with Counselors or affiliates deemed not part of the Company's Workforce may, depending on the nature of the arrangement, need to enter into the Company's Counselor BAA provision as a part of such contract.

10. Privacy Breaches and Notification

10.1. Identifying and investigating Breaches

When a Breach is suspected, Workforce members will report the details of the event to their manager, who will notify the LifeWorks Breach response team consisting of line of business leadership, the Legal department and Responsible Persons. Actual or suspected Breaches should be documented in an Incident Report. Using the information in the Incident Report, the Breach response team will determine what, if any, Breach may have occurred and what steps have been or need to be taken to contain the Breach.

Any impermissible acquisition, access, use, or disclosure of an Individual's unsecured PHI is presumed to be a Breach, unless either (i) the Breach falls within one of the recognized exceptions; or (ii) a risk assessment conducted by the Company has determined there is a low probability that the PHI involved has been compromised.

10.1.1. Exceptions

LifeWorks Breach response team will review each Incident Report to determine whether the suspected Breach falls within one the following recognized impermissible uses or disclosures:

1. An unintentional acquisition, access, or use of PHI by a Workforce member or other person acting under the authority of the Company, if such acquisition, access, or use was in good faith and within the scope of authority and did not result in a further impermissible use or disclosure;
2. An inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI within the Company, and the information received was not further used or disclosed in a manner not permitted under the Privacy Rule; or
3. A disclosure of PHI where LifeWorks had a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

If the incident does not fit within one of these exceptions, a breach risk assessment will be conducted as set forth below.

10.1.2. Breach Risk Assessment

LifeWorks Breach response team will conduct a breach risk assessment to determine the probability that the PHI involved has been compromised. This risk assessment will consider, at a minimum, the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made (e.g. is the recipient obligated to protect the privacy and security of the information?);

- Whether the PHI was actually acquired or viewed (or only the opportunity existed to acquire or view the information); and
- The extent to which the risk to the PHI has been mitigated. For example, were satisfactory assurances obtained from the recipient that the information would not be further used or disclosed (e.g. confidentiality agreement) or will be destroyed (e.g. with a destruction certificate)?

If the risk assessment establishes that there is a low probability that the PHI has been compromised (i.e. the potential is low for the recipient's unauthorized use or misuse of the PHI), then the Company may determine that a Breach did not occur under HIPAA.

10.2. Procedure Following Determination that Breach Occurred

If, following an investigation, LifeWorks determines that a potential Breach (i) is an impermissible use or disclosure of PHI under HIPAA; (ii) "compromises" the security or privacy of the PHI pursuant to a risk assessment; and (iii) does not satisfy one the exceptions listed under above, LifeWorks will follow the notification procedure outlined below.

10.2.1. Notice to the Covered Entity

If LifeWorks is acting as a Business Associate, it will report to the Covered Entity the results of its investigation. Notification to the Covered Entity must be made as soon as possible, but in no case later than 60 days after Discovery of the Breach. Upon request by the Covered Entity and/or as set forth in a BAA, LifeWorks may provide the notices to Individuals and the media where applicable in accordance with the notification requirements under HIPAA.

10.2.2. Notice to the Media

When a Breach affects more than 500 Individuals, LifeWorks and/or the Covered Entity will provide notice to prominent media outlet(s) serving the relevant state or jurisdiction, in addition to the notice it provides to affected Individuals. The notice will be in the form of a press release and will be provided without unreasonable delay, and in no case later than 60 days after Discovery of the Breach. The notice will include the same information required for notice to Individuals. If the Breach occurs while the Company is acting as a Business Associate, the Company will cooperate with the Covered Entity and provide whatever information it can to assist.

10.2.3. Notice to HHS

LifeWorks and/or the Covered Entity will provide notice to HHS of a Breach of Unsecured PHI as follows, and LifeWorks will cooperate fully with the Covered Entity, if applicable, and provide whatever information it can to assist:

- **500 or More Individuals**. If a Breach involves 500 or more Individuals, LifeWorks and/or the Covered Entity will notify HHS at the same time notice is made to the Individuals, but in no

case later than 60 days after Discovery of the Breach. The notice will be provided in the manner specified on the HHS website.

- **Less Than 500 Individuals.** For Breaches involving fewer than 500 Individuals, LifeWorks will maintain a log of all such Breaches and will, not later than 60 days after the end of each calendar year, provide the notification required for Breaches discovered during the preceding calendar year in the manner specified on the HHS web site. Where LifeWorks is a Business Associate, it will submit the log to each Covered Entity responsible for those Individuals.

10.2.4. Notice to Individuals

Notice must be provided to any Individual affected by the Breach without unreasonable delay, but in no case later than 60 days after Discovery of the Breach.

10.3. Content and Method of Notice to Individuals.

10.3.1. Content of Notice.

The notice provided to Individuals will be written in plain language and contain the following information:

- A brief description of what happened to cause the Breach;
- A description of the types of Unsecured PHI involved in the Breach (e.g., whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;
- A brief description of what has been done to mitigate the harm to Individuals and protect against further Breaches; and
- Contact information and procedures for Individuals to ask questions or learn additional information, including a toll-free telephone number, an e-mail address, website or postal address.

As appropriate for the Individuals to whom notice is given, and on an as needed basis, reasonable steps shall be taken to have the notification translated into languages that are frequently encountered by LifeWorks and/or the Covered Entity, and to ensure effective communication with Individuals with disabilities.

10.3.2. Methods of Notice to Individuals

- **Written Notice**. The notification to affected Individuals will be by mail to the Individual at the last known address of the Individual or, if the Individual has agreed to electronic notice, by electronic mail. The notification may be provided in one or more mailings as information is available. If LifeWorks and/or the Covered Entity know the Individual is deceased and has the address of the next of kin or Personal Representative of the Individual, LifeWorks and/or the

Covered Entity will deliver written notification to either the next of kin or the Personal Representative.

- **Substitute Notice**. If there is insufficient or out-of-date contact information for some or all of the affected individuals that precludes written notification to the Individual, a substitute form of notice will be used depending upon the number of unreachable Individuals.
- **If Fewer Than 10 Individuals**: If there are fewer than ten (10) Individuals to receive substitute notice, the substitute notice may be provided by an alternate form of notification such as telephone, or other means.
- **If 10 or More Individuals**: If there are ten (10) or more Individuals to receive substitute notice, then the substitute notice will be in the form of either: (a) a posting for ninety (90) days on the home page of the website of LifeWorks and/or the Covered Entity; or, (b) a notice in prominent media outlet(s) serving the relevant state or jurisdiction; and include a toll-free telephone number that remains active for at least ninety (90) days where an Individual can receive more information.

10.4. Law Enforcement Delay

Notwithstanding anything in this Section to the contrary, if a law enforcement official states to LifeWorks that a notification, notice, or posting required by this Section would impede a criminal investigation or cause damage to national security, the Privacy Officer will document the statement if it has not already been provided in writing. The Privacy Officer will then delay the notification, notice, or posting for a period of 30 days or for the time period otherwise specified by the law enforcement official in writing.

LifeWorks personnel who are contacted by a law enforcement official in this regard will be advised to refer the official to the Privacy Officer or their designate.

11. Disposal of PHI

11.1. Disposal of Paper Media

All PHI must be disposed of so that unauthorized individuals are unable to access it. Permissible means of disposal include use of shredders or disposal in specified locked receptacles that are intended for confidential or sensitive documents (shred bins). These shred bins must remain locked and in a secured area that are generally inaccessible to the public that are picked up by a trusted and compliant shredding company. Recycle bins are not to be used to dispose of documents containing PHI.

11.2. Disposal of Electronic Media

Disposal of electronic media containing electronic PHI shall be done in accordance with HIPAA, and industry standard methods must be used to wipe and dispose of electronic media devices. If uncertain of industry-standard methods for disposal, the Security Officer should be contacted.

12. Change/Review Tracking

Policy Details	
HIPAA Policies and Procedure Manual - US Policy title	October 13,2022 Effective date
Privacy Officer Policy owner (VP/SVP/EVP/Department)	VP Legal; Legal, Risk & Privacy Required approvals
Annual Review frequency/cycle	October 13, 2022 Effective date of last review/revisions
January 18, 2011 First release date	October 13, 2023 Next review