Janus Youth Programs

HIPAA Privacy Policy and Procedures Manual

June 30, 2016

Table of Contents

Additional Items:

- **HIPAA Manual Forms**
  - Authorization To Use and/or Disclose PHI
  - Privacy Complaint Form
  - Request For Amendment of PHI
  - Request For Access To Designated Record Set (DRS)
  - Request For Accounting of Disclosures of PHI
  - Revocation of Authorization To Use and/or Disclose PHI
  - Request For Restriction of PHI
  - PHI Disclosure Log
  - PHI Fax
  - Letter of Misdirected Fax
- **HIPAA Sample Letters**
  - Response To Request To Amend PHI
  - Letter of Extension To Amend PHI
- **Breach Notification**
  - Breach Notification Summary
  - Breach Notification Policy [sample]
  - Breach Notification Log
  - HHS of a HIPAA Breach [sample]
  - HIPAA Breach Notice To Individual [sample]
- **HIPAA Business Associate**
  - Business Associate Agreement Contract [sample]
  - Business Associate Agreement Log
- **Patients Rights and Responsibilities**
  - PHI Notice: Your Information. Your Rights. Our Responsibilities.
- **HIPAA Training**
  - Acknowledgement of HIPAA Security Awareness Training
  - Employee Confidentiality Statement PHI

Introduction

This publication provides authoritative information regarding requirements of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as amended, and its implementation regulations.

In order to protect the privacy and the confidentiality of individual Protected Health Information (PHI) in compliance with federal privacy and security rules mandated under HIPAA, HITECH and state laws, all employees of the Janus Youth Program, a highway, street, and bridge construction contractor, who have access to PHI must comply with the policies and procedures explained in this manual. The privacy and security rules consider a "workforce member" to include employees, volunteers, interns, and other individuals whose work performance is under the direct control of Janus Youth Program, whether or not they are paid directly or indirectly by Janus Youth Program.

The purpose of these policies and procedures is to establish Janus Youth Program's good faith interpretation as to how the HIPAA privacy and security rules should be implemented and enforced. No third-party rights (including, but not limited to rights of health plan individuals, beneficiaries, patients or Business Associates) are intended to be created by these policies and procedures. Janus Youth Program reserves the right to amend or change these policies and procedures at any time (and even retroactively) without notice to comply and as amended in accordance with medical privacy rules and regulations.

This guide is broken down into several different components to include: HIPAA's Privacy, Security and other Administrative simplification provisions. The first, a general overview of the rules, is not meant to be all-inclusive. Employers, "Entities," are strongly encouraged to research the privacy and security rules and to seek legal advice regarding their compliance efforts.

Many defined terms are employed in this manual. The definitions of these terms are set forth in the Key Definitions Addendum of this manual.

HIPAA General Overview

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996. It includes administrative simplification regulations or mandates that are applicable to various health plans. These regulations were designed to ensure the privacy and confidentiality of individual health information, otherwise known as Protected Health Information (PHI).

As part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Department of Human Health Services (HHS) issued regulations entitled "Standards for Privacy of Individual Health Information." Within HHS, the Office of Civil Rights ("OCR") has the responsibility for implementation and enforcement of the Privacy Rule with regards to compliance and penalties.

On September 23, 2013, HHS increased protection and control of protected health information (PHI) requiring all Entities and Business Associates to comply. The recent changes expanded penalties for noncompliance based on the level of negligence. The changes also strengthen the Health Information Technology for Economic and Clinical Health ***(HITECH)*** Breach Notification requirements by clarifying when breaches of unsecured health information must be reported to HHS.

The ***final omnibus rule*** is based on statutory changes under the HITECH Act, enacted as part of the American Recovery and Reinvestment Act of 2009 and the Genetic Information Nondiscrimination Act of 2008 (GINA). The rule clarifies that genetic information is protected under the HIPAA Privacy Rule and prohibits the use of genetic information from discrimination based on genetic purposes.

HITECH
The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law in February 2009.

The security rules (45 CFR Parts 160, 164) specify a series of administrative, technical, and physical security procedures for providers and Entities to use to ensure the confidentiality of electronic health information. Title 45 CFR 164.103 also defines what stipulates a "breach", except as otherwise provided under the definition.

HIPAA's administrative simplification requirements were designed in part to reduce healthcare costs by standardizing the electronic processing of healthcare claims. The three primary components are:

- ***Privacy standards*** - addressing who is authorized to access information and the right of individuals to determine how their information is to be used or disclosed.
- ***Security standards*** - addressing the ability to control access and to protect information from accidental or intentional disclosure to unauthorized persons and from unauthorized alteration, destruction, or loss.
- ***Transaction standards*** - promoting the standardization of certain payment-related electronic transactions (also referred to as the electronic data interchange or "EDI" standards).

HIPAA defines persons who may be authorized for access to protected health information created or maintained by certain covered Entities (and Business Associates). It focuses on the rights of individuals to determine how their information is to be used or disclosed to others and promotes the protection of privacy and security of certain healthcare information.

What Information is covered?

The privacy requirements generally cover “individually identifiable protected health information” transmitted or maintained in any form or medium (electronic or otherwise), while the security requirements apply to “electronic PHI”. When such information is created or received by a covered Entity (or by a Plan sponsor or Business Associate acting on behalf of the covered Entity), it becomes “Protected Health Information” (PHI) subject to the medical privacy security rules.

Section 1- Permitted Use and Disclosure of Protected Health Information

- General Rule - Non-Disclosure of PHI
- Permitted Disclosures - For Payment Purposes and Health Care Operations
- Required Disclosures - To Individuals who are the subject of PHI and to HHS
- Required Disclosures - Disclosures Required by Law
- The Minimum Necessary Disclosure Rule

General Rule - Non-Disclosure of PHI

Purpose

To protect the privacy and security of Individual's Protected Health Information.

Policy

Protected Health Information ("PHI") should not be disclosed to any party or any individual unless the disclosure is made pursuant to one of the permitted disclosures or required disclosures described in this manual (or otherwise required by law).

The individual with the privacy right to be protected is the recipient of the services.

To protect against unnecessary disclosures of PHI, and to comply with the requirements of HIPAA, only those workforce individuals, beneficiaries and those Business Associates needed to administer Janus Youth Program health plans and health care services may have access to PHI; and only then for permitted purposes and to fulfill job responsibilities.

Procedures

Every workforce member of Janus Youth Program and Business Associates authorized to receive, distribute or disseminate protected health information of a Janus Youth Program workforce individual (or covered beneficiaries) or patients should become acquainted with the definition of PHI. See the Key Definitions - Glossary section of this manual to find the definition.

If a workforce member has any question(s) about whether health information constitutes PHI, or whether a disclosure of PHI is permitted, the workforce member should review the matter with the Janus Youth Program HIPAA Privacy Officer.

Please refer to the Classes of Workforce Members "Employees" and Approved Uses in the Appendix for a list of those Classes of Workforce Members "Employees" who have approved access to PHI and a brief detailed description of approved uses and disclosures of PHI. However this is subject to change depending on an organization's business structure of providing health care services. Generally, except for certain permitted disclosures to workforce individuals (or covered beneficiaries) or patient's of their own PHI, no other unauthorized individual may have access to PHI unless an "Authorization To Use and/or Disclosure of Protected Health Information (PHI)" form has been provided and only disclosure that which is authorized.

Even if a Disclosure of PHI is a permitted disclosure, the disclosure should be made only to the individual properly entitled to receive the disclosure. Generally, except in the case of processing claims for payments of benefits and health care operations, health plan individuals and beneficiaries (family individual, beneficiaries) are not entitled to disclosures of the PHI of their spouses and adult child(ren), unless authorized.

The following disclosures of PHI may be made by Operations & Administration of a workforce member without the review or approval of the HIPAA Privacy Officer:

- Disclosure of health information (other than psychotherapy notes) to a health plan individual, beneficiary or patient in connection with performing the administrative functions of benefits, services or payment of

claims under a Janus Youth Program Group Health Plan and Business Associate health care service agreement;
- Disclosure of PHI required by a Business Associate who is providing services to Janus Youth Program under a Business Associate Agreement.

All other disclosures of PHI must be reviewed and approved by the HIPAA Privacy Officer. Without limiting the forgoing, such disclosures include:

- Disclosures to any third-party pursuant to an authorization from the health plan individual, beneficiary or patient;
- Disclosures of PHI that are required by law, including mandatory disclosures of abuse to social service agencies;
- Disclosures of Psychotherapy Notes;
- Disclosures of PHI for Public Safety and Health Activities.

Permitted Disclosure of PHI - For Payment Purposes and Health Care Operations

Purpose

Janus Youth Program may use or disclose PHI only as permitted or required in accordance with HIPAA privacy and security rules, regulations and state law. The HIPAA privacy and security rules permit Janus Youth Program to use or disclose a health plan individual, beneficiary or patient's PHI without the authorization of the health plan individual or beneficiary to the extent necessary for claim payment purposes and Janus Youth Program business health care operations and administration.

Policy

PHI may be accessed and disclosed by an approved benefit plan administration designated workforce individual, beneficiary "employees" (see Classes of Workforce Individual, beneficiary "Employee" and Approved Uses in the Appendix) for purposes of processing benefit claims and payments under Janus Youth Program health plans, and administration of these plans and organization business structure of providing health care services.

Except in the case of psychotherapy notes (limited), access and use of PHI does NOT require the authorization of the health plan individual, beneficiary or patient.

Our ability to use or disclose a health plan individual, beneficiary or patient's PHI is limited to those uses and disclosures that relates to our status as a Health Plan or health care services. As a result, should the health plan not receive an authorization from the health plan individual, beneficiary (as discussed in "Participant Authorization") workforce individual, beneficiary may not use health plan individual, beneficiary, or patient's protected health information for the payment or operations of "non-health" benefits (e.g., disability, worker's compensation, life insurance, etc.).

Procedures

1. If engaged in a task related to the payment or health care operations and administration of an individual's health plan information, beneficiary or health care services, a workforce individual and/or a beneficiary may use and/or disclose of a health plan individual, beneficiary or patient's protected health information to perform these functions only if it is a necessary element to the performance of the job duties. See Classes of Workforce Individual, beneficiary "Employee" and Approved Uses in the Appendix for those approved uses and disclosures of PHI associated with the job responsibilities.

2. If a workforce individual/beneficiary routinely engage in tasks that relate to either the Health Plans, non-health benefits and health care services, workforce individual, beneficiary must ensure not to use protected health information to perform payment or health care operations activities for the non-health benefits (unless the individual has provided an authorization, as discussed in "Individual Authorization Disclosure").

3. If a workforce individual/beneficiary requires a health plan individual, beneficiary's or patient's PHI for the payment or health care operations and administration of non-health benefits, the workforce individual/beneficiary must first communicate with the HIPAA Privacy Officer to verify that Janus Youth Program obtained a signed authorization from the health plan individual, beneficiary or patient permitting Janus Youth Program to use their PHI in connection with the payment or operations and administration of non-covered lines of services. Do not attempt to draft/create an authorization form that has not been

approved by the HIPAA Privacy Officer. Janus Youth Program has drafted specific authorization forms that comply with the detailed requirements concerning the information that must be contained in an authorization.

4. If a workforce individual/beneficiary is unsure as to whether a task being performed qualifies as a payment activity or a business health care operation, communicate with the Janus Youth Program HIPAA Privacy Officer.

5. An approved workforce individual/beneficiary may disclose PHI to affiliated business associates who are assisting Janus Youth Program in payment functions, its health care operations and administration or business health care service functions, provided that the approved workforce individual/beneficiary verify with the Janus Youth Program HIPAA Privacy Officer that Janus Youth Program has a signed Business Associate Agreement on record with that particular business associate (See “Communications with Business Associates").

6. Psychotherapy notes may NOT be disclosed to any third-party without the consent of the health plan individual, beneficiary or patient receiving treatment, even if the notes are to be used to process a benefit claim. The only times psychotherapy notes may be disclosed without the authorization of the individual, beneficiary or patient are:

    i. Notes may be provided without the consent of the patient to the therapist who made such notes, if the notes are being provided for treatment purposes;
    ii. Notes may be provided without the consent of the patient, if required by law.

7. PHI of the spouse or child of a health plan individual, beneficiary (including any adult child who is a beneficiary of the health plan) and patient may be disclosed (without the authorization of the spouse or child) to the extent that the disclosure is made for the purpose of processing benefit claims or business health care service operations and administration as designated or as authorized.

Required Disclosure of PHI - To Individuals Who Are The Subject of PHI & To The Department of Health and Human Services (HHS)

Purpose
Janus Youth Program may use or disclose PHI only as permitted or required by federal and state HIPAA privacy and security rules and regulations.

Policy
Janus Youth Program is required to disclose a health plan individual, beneficiary or patient's PHI in two situations:

1. Janus Youth Program must disclose PHI to the individual who is the subject of the PHI when the individual exercises their rights under the privacy and security rules to access their PHI (See "Processing Requests for Access to Protected Health Information"); and

2. Janus Youth Program must disclose PHI to HHS in connection with its enforcement and compliance review actions.

Procedure
Any health plan individual, beneficiary or patient may request disclosure of PHI for the processing of benefits administration functions or benefit payments for the health plan individual, beneficiary and patient (including the minor AND adult children) of the health plan individual, beneficiary or patient as authorized.

Any health plan individual, beneficiary or patient may request disclosure of PHI for other purposes for the health plan individual, beneficiary or patient, and the individual for whom the health plan individual, beneficiary or patient is a personal authorized representative (generally, the individual's minor children, and other individuals who are legally entitled to represent such persons).

A health plan individual, beneficiary or patient may request PHI in writing. If the, request is ambiguous, or if the health plan individual, beneficiary or patient request their PHI verbally, the workforce individual/beneficiary are to request that the individual complete a "Request for Access to PHI Form" (see Forms Addendum – request for Access To Designed Record Set PHI).

If a health plan individual, beneficiary, patient or HHS makes a disclosure request, the disclosure is not required to be limited to the minimum amount necessary to comply with the request.

If a request is received from a health plan individual, beneficiary, patient or an authorized representative from HHS for disclosure of a health plan individual, beneficiary or patient's PHI, the workforce individual/beneficiary must follow the procedures explained in the "Verification of Identity of Individuals Requesting PHI" procedures.

Related Procedures
Verification of Identity of Individual Requesting PHI

Required Disclosure of PHI – Disclosures Required by Law

Purpose
Janus Youth Program may use or disclose PHI as required by federal and security HIPAA rules and regulations.

Policy
Janus Youth Program must disclose a health plan individual, beneficiary or patient's PHI, without the health plan individual, beneficiary or patient's authorization in situations of which the disclosure is required by law, provided that Janus Youth Program complies with any applicable requirements of the other laws and disclosure of PHI is made consistent with HIPAA rules and regulations.

Procedure
If the use or disclosure is required by law, Janus Youth Program may disclose a health plan individual, beneficiary or patient's PHI. Janus Youth Program must determine that the disclosure is permissible limited to the amount required by both federal and state law. The Privacy Rule provides an extensive list of permitted disclosures. However, where state laws provide greater privacy protections or privacy rights with respects to individuals' PHI, state laws will override HIPPA rules and regulations.

The following exceptions include, but are not limited to:

1. Court issued subpoenas (Minimum Necessary Rule does NOT apply);
2. Grand jury issued summons or subpoenas (Minimum Necessary Rule does NOT apply);
3. Administrative requests for records by government Entities in the exercise of their health oversight responsibilities (Minimum Necessary Rule does NOT apply);
4. Mandatory disclosure of acts of abuse or neglect to government agencies (Minimum Necessary Rule does NOT apply);
5. Disclosures for law enforcement purposes (HIPAA restricts type of information that may be provided);
6. Disclosures to Public Health Agencies (Minimum Necessary Rule Applies);
7. Disclosures to HHS (Minimum Necessary Rule does NOT apply).

Even if the Minimum Necessary Rule does not apply to a disclosure required by law, reasonable effort and good judgment should be made to assure that the disclosure complies with the terms of the order or the request for PHI.

If it is believed that a disclosure is required by law, the information should be forwarded to the HIPAA Privacy Officer, who is responsible for the determination of the final decision concerning the necessity to disclose PHI and the amount of PHI to disclose.

Certain disclosures that are required by law and are subject to additional requirements before any PHI can be disclosed are listed below:

- Disclosures about victims of abuse, neglect or domestic violence - if a workforce individual/ beneficiary becomes aware of a case involving abuse, neglect or domestic violence, State and local agencies may require that the information concerning such matters be disclosed even in the absence of a governmental investigation. In such events, workforce individual/beneficiary should immediately contact the HIPAA

Privacy Officer to determine Janus Youth Program's duty to disclose the information, agency to provide the disclosure to and the extent of the disclosure necessary.

- Disclosures for law enforcement purposes. Federal, State and local enforcement agencies may request disclosure of PHI in connection with criminal investigations. In the event a workforce individual/beneficiary receives a request for PHI with respect to a law enforcement investigation, the workforce individual/beneficiary should immediately communicate with the HIPAA Privacy Officer to determine Janus Youth Program's duty to disclose the information, the recipient to provide the disclosure to, and the extent of the disclosure necessary.
- Disclosure to health enforcement authorities of public health. In the event that a workforce individual/beneficiary receives a request for PHI with respect to a public health agency, the workforce individual/beneficiary should immediately communicate with the HIPAA Privacy Officer to determine Janus Youth Program's duty to disclose the information, the recipient to provide the disclosure to, and the extent of the disclosure necessary. These disclosures should be limited to the minimum required amount of disclosure rules applicable to other disclosures. For example, if a workforce individual/beneficiary receives a request for protected health information from the State Department of Health and Human Services, the request should be forwarded to the HIPAA Privacy Officer.
- General Public Health Activities. The Privacy Rule permits disclosure of PHI, without authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability. A "public health authority" is an:

    a. Agency or authority of the United States government;
    b. A State, a territory, a political sub of a State or territory;
    c. Indian Tribe that is responsible for public health matters as part of its official mandate;
    d. A person or entity acting under a grant of authority from, or under a contract with a public health agency such as a state sanctioned health department, the Food and Drug Administration (FDA), the Center of Disease Control and Prevention, and the Occupational Safety and Health Administration (OSHA).

- Certain disclosure is about decedent. Disclosure of PHI concerning decedents to parties other than the personal authorized representatives of their estates are required by law, including:

    a. To alert law enforcement in the suspension of death resulting from criminal conduct;
    b. Disclosures to coroners or medical examiners and funeral directors in the performance of their duties;
    c. To organ procurement organizations or other agencies involved in the procurement.

Disclosure of PHI is Generally Limited to the Minimum Necessary Disclosure

Purpose
HIPAA regulation 164.502 requires that reasonable effort is made not to disclose more than the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure, or request within the constraints of practical and technical limitations.

Appropriate steps should be taken to disclose only the minimum amount of PHI necessary to accomplish the particular use or disclosure, as required by HIPAA regulation and other applicable federal, state, and/or local laws and regulations.

Policy

1. Janus Youth Program workforce individual/beneficiary will follow proper procedures to ensure that only the minimum amount of the health plan individual, beneficiary or patient's PHI necessary to accomplish the specific purpose of a use or a disclosure is actually used or disclosed (the "Minimum Necessary Information").

2. Unless an exception to the Minimum Necessary Information rule applies, a Janus Youth Program workforce member will request only the minimum amount of a health plan individual, beneficiary or patient's PHI necessary to accomplish the specific purpose of the request.

3. This policy does not apply to the following uses or disclosures:

    a. Disclosure to or request by a provider for purposes of treatment;
    b. Uses or disclosure made to the health plan individual, beneficiary or patient who is the subject of the information or in request to a response from HHS;
    c. Uses or disclosure pursuant to an authorization from a health plan individual, beneficiary or patient to provide information;
    d. To a third-party;
    e. Uses or disclosures required by law;
    f. Uses or disclosure required for compliance with applicable local or state laws and regulations.

4. Examples of where the disclosure should be limited to the Minimum Necessary Information include:

    a. Processing claims for benefits;
    b. SOME disclosures for local and state law enforcement purposes;
    c. Disclosures about decedents, unless the disclosure is Required by Law;
    d. Disclosures for public health activities;
    e. Disclosing psychotherapy notes in processing claims for payment.

Procedures
Refer to Classes of Workforce Individual, beneficiary "Employee" and Approved Uses in the Appendix for a list of individual's allowed to access PHI.

1. When the Minimum Necessary rule applies, the use, disclosure, or request of PHI will only occur when specifically justified and only to the extent reasonably necessary to accomplish the purpose of the use, disclosure, or request.

2. Respond to workforce individual/beneficiary inquiries and assist workforce in resolving problems relating to their personal health insurance coverage(s):

   - If a workforce individual/beneficiary respond to a workforce individual, beneficiary or patient's inquiries or assist in resolving problems relating to their personal health insurance coverage, the workforce individual/beneficiary may obtain as much information as the workforce individual, beneficiary or patient is willing to provide the workforce regarding their issue or problem;
   - However, if workforce individual/beneficiary requires access to information maintained by health plans, the workforce individual/beneficiary must limit the information requested from the health plan to the amount of information necessary to assist the workforce individual, beneficiary or patient in resolving their problem. Workforce individual/ beneficiary may not request access to the health plan individual, beneficiary or patient's entire medical record. Furthermore, in the case of an insured health plan, that plan may require that the workforce individual/beneficiary obtain consent to access the workforce individual, beneficiary or patient's PHI in its possession.

3. Disclosures to Business Associates who respond to a workforce individual/beneficiary inquiries and assist in resolving problems relating to their health care benefits:

   - If a workforce individual /beneficiary are disclosing information to Business Associates so they may respond to a workforce individual, beneficiary or patient's inquiries and assist with problems relating to their health care coverage, the workforce individual/beneficiary may provide Business Associates with any of the information the workforce or patient has provided regarding their issue or problem.

4. Internal Analysis and Reconciliation:

   - If a workforce individual/beneficiary is engaged in internal analysis and reconciliation activities for Janus Youth Program health plans, the workforce individual/beneficiary may receive only the information required to perform the reconciliation activities in which they are engaged and authorized as part of their job responsibilities.

5. Enrolling workforce into Janus Youth Program health plans:

   - If a workforce individual/beneficiary is engaged in activities relating to enrolling workforce into Janus Youth Program sponsored health plans, the workforce individual/beneficiary may obtain information required on the plan enrollment form(s) provided by current carrier(s); and other valid information, if required.

Related Procedures

Classes of Workforce Individual, beneficiary "Employee" and Approved Uses

Section 2 - Individual Rights

- Right to Amend PHI
- Access to Inspect and Copy PHI Accounting for Disclosures Individual Authorization Disclosure

Right to Amend PHI

Purpose
Under HIPAA, individuals have the right to request an amendment or correction to their PHI.

Policy
HIPAA Privacy Laws allow health plan individuals, beneficiaries and patients the right to request amendments to PHI that Janus Youth Program (or its Business Associates) maintains about them in Designated Record Sets (DRS). In order to protect the privacy and confidentiality of the health plan individual, beneficiary and patient's PHI and to comply with the Privacy Laws, the Operations and Administration must comply with the following procedures in processing a health plan individual, beneficiary or patient's request to amend information and records.

Procedures

1. The Operations and Administration will be responsible for receiving, processing and responding to requests for amendments to PHI;

2. All individual requests for amendments to PHI or other health information will be in writing and directed to the Operations and Administration;

3. The health plan individual, beneficiary or patient must complete the Janus Youth Program Request to Amend PHI form and either fax, email (45 C.F.R. § 164.514(h) and 45 C.F.R. § 164.530(c)) or mail the completed, signed form to the attention of the HIPAA Privacy Officer.

Denials

- An individual's request for amendment may be denied if the form is not signed and/or does not state a reason for the amendment request;
- If the Janus Youth Program Request to Amend PHI Form is signed by a health plan individual, beneficiary or patient's personal representative, the representative must include documentation or information to support their authority to act on behalf of the health plan individual, beneficiary or patient. If such information, in accordance with the Verification Policy, is not included, the request does not need to be further processed and the defect should be noted on the Janus Youth Program Request to Amend PHI Form. A denial notice must be sent to the requestor (if proper Name and address has been provided) within 60 days of the receipt of the amendment request;
- Request to Amend PHI relates to a record that was not created by one of Janus Youth Program's self-funded plans. For example, in the case of a fully-insured health plan sponsored by Janus Youth Program, the request to amend PHI should be provided to the insurance company rather than to Janus Youth Program. The Response to Request to Amend PHI Form must be sent to the requestor within 60 days of the receipt of the amendment request;
- Request to amend PHI relates to information or a record that is not part of the Designated Record Set, the Response to Request to Amend PHI Form must be sent to the requestor within 60 days of the receipt of the amendment request;
- Request to amend PHI relates to information the health plan individual, beneficiary or patient is not authorized to inspect by law (psychotherapy notes) and information compiled in reasonable anticipation of, or for use in a civil, criminal, or administrative action or proceeding. The Response to Request to Amend PHI Form must be sent to the requestor within 60 days of the receipt of the amendment request;

- If the request to amend PHI has been forwarded to the author of the record or information in question and the author has determined the record is complete or accurate and does not require amendment, the Response to Request to Amend PHI form must be sent to the requestor within 60 days of the receipt of the amendment request;
- When an amendment request is denied, the notice must set forth the basis for the denial. The health plan individual, beneficiary or patient has the right to submit a statement of disagreement and the Operations and Administration or the author of the record or information in question has the right to prepare a rebuttal. If a rebuttal statement is prepared, a copy must be promptly sent to the health plan individual, beneficiary or patient and a copy placed in the health plan individual, beneficiary or patient's confidential file.

Amending the Record (Approvals)

- When an amendment or correction is approved by Janus Youth Program Operations and Administration workforce individual/ beneficiary, the Response to Request to Amend Protected Health information will be marked as "Amendment Granted" and placed in the health plan individual, beneficiary or patient's confidential file. Prior PHI, which has been amended, shall be identified as having been amended;
- When an amendment is accepted, the Operations and Administration will provide appropriate notice to the health plan individual, beneficiary or patient and all persons or Entities listed on the health plan individual, beneficiary or patient's amendment request form, if any, and also provide notice of the amendment to any persons/Entities who have the particular record and who may rely on the uncorrected information to the detriment of the health plan individual, beneficiary or patient. The Operations and Administration will document the Request to Amend PHI with the names of the person(s)/Entities receiving the amendment notice;
- If the health plan for example is informed by another Entity of an amendment to a health plan individual, beneficiary or patient's PHI, Janus Youth Program must notify the Operations and Administration to amend the PHI in the designated record sets in accordance with the procedures explained above.

Extensions

- If the Operations and Administration is unable to process a request for amendment within the required 60 days, one 30-day extension may be taken. The health plan individual, beneficiary or patient must be notified of the extension in writing and the notice must be sent before the original 60 days have lapsed. Only one extension may be taken and the notice must inform the health plan individual, beneficiary or patient of the reasons for the extension and the date by which a response is intended.

Related Documents
Request to Amend PHI
Letter of Extension to Amend PHI
Response to Request to Amend PHI

Access to Inspect and Copy PHI

Purpose
Health plan individual, beneficiary, patient and their representatives have the right to access, inspect and obtain a copy of their PHI.

Policy
The HIPAA Privacy Laws allows health plan individuals, beneficiaries, patients and their representatives the right to access and obtain copies of their PHI that Janus Youth Program Business Associates maintains in Designated Record Sets. Only requests for information after HIPAA's effective date (April 14, 2004) need be filled. The Operations and Administration is responsible for administering requests by a health plan individual, beneficiary and patient for access to their PHI.

Procedure

1. The Operations and Administration will be responsible for receiving, processing and responding to requests for access to inspect and copy PHI.

2. All health plan individual, beneficiary and patient's requests for access to inspect and copy PHI or other health information will be in writing, and directed to the Operations and Administration, attention HIPAA Privacy Officer.

3. The health plan individual, beneficiary, patient or the representative must complete the Request to Access DRS form and either fax or mail the completed, signed form to the Operations and Administration, attention HIPAA Privacy Officer.

4. Notice of approval/denial must be sent to the health plan individual, beneficiary, patient or the representative no later than 30 days from receipt of the request if the information is accessible on-site.

5. If the request is for DRS that is not maintained or accessible on-site, the notice of approval/denial must be sent no later than 60 days after the request.

6. The access requested must be provided in the form or format requested by the health plan individual, beneficiary, patient or the representative, if readily producible in such a manner. Otherwise, the information must be provided in a readable hard copy or such other form as agreed to by the health plan individual, beneficiary, patient or authorized representative.

7. The health plan individual, beneficiary, patient or the representative has the right to receive a copy by mail to the address provided, by email in accordance with electronic transactions privacy rule, or pick up a copy provided authorization forms have been completed, signed and proper identification has been obtained.

8. If the health plan individual, beneficiary, patient or the representative has requested a statement or summary and explanation of the requested information in lieu of, or in addition to, the full information, the statement or summary and explanation of the information requested must be prepared and made available to the health plan individual, beneficiary, patient or representative in the form or format requested.

9. Copies of all requests for access and all communications between the health plan individual, beneficiary, patient or representative and the Operations and Administration should be obtained and kept in the health plan individual, beneficiary or patient's confidential file.

10. Steps should be taken to confirm that a representative in fact has the authority to act on behalf of a health plan individual, beneficiary or patient. See "Verification of Identity of Persons Requesting PHI".

    NOTE - In accordance with "Verification of Identity of Persons Requesting PHI" the document establishing a person's relationship as a representative should be submitted to and reviewed by the HIPAA Privacy Officer prior to providing the PHI to the representative.

11. A representative of a health plan individual, beneficiary or patient may be provided PHI of a health plan individual, beneficiary or patient only to the extent that the PHI is relevant to the matter for which the representative seeks to act.

Denials

Denials of a health plan individual, beneficiary or patient's request for PHI may be based on the following grounds.

- The access request form is not signed by the health plan individual, beneficiary, patient or the authorized representative.
- The health plan individual, beneficiary or patient's representative signs the access request form and the representative has not provided information on the source of his/her authority to act on behalf of the health plan individual, beneficiary or patient consistent with Janus Youth Program Verification Policy.
- Part or the entire access request relates to a record that is not maintained by Janus Youth Program (or one of Janus Youth Program Business Associates), in which event the denial shall be limited to the information, which is not part of a Designated Record Set.
- Part or the entire access request relates to information or a record that is not part of the health plan individual, beneficiary or patient's designated record set.
- Part or the entire access request relates to information that has been compiled in anticipation of or for use in a civil, criminal, or administrative proceeding. This would include any documents marked "Attorney-Client Privileged" or similar.
- Part or all of the access request relates to information that makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined the access requested is reasonably likely to cause substantial harm to such other person.
- The request for access is made by the health plan individual, beneficiary or patient's personal representative and a licensed health care professional has determined that access by such personal representative is reasonably likely to cause substantial harm to the health plan individual, beneficiary, patient or another person.
- The request is made by an inmate of a correctional institutional to receive a copy of the information (an inmate may not receive a copy but does retain the right to inspect the information).
- Part or the entire access request relates to information obtained by Janus Youth Program from a non-health care provider under a promise of confidentiality and access would likely reveal the source of the information.
- Federal and state law forbids making the requested information available for inspection.

Extensions

- If the Operations and Administration is unable to process a request for access within the required 60 days, one 30-day extension may be taken. The health plan individual, beneficiary, patient or authorized personal representative must be notified of the extension in writing and the notice must be sent before the original 60 days have lapsed. Only one extension may be taken and the notice must inform the health plan individual, beneficiary, patient or personal representative of the reasons for the extension and the date by which a response is intended.

Related Documents
Request to Access PHI / Request For Amendment DRS
Letter of Extension to Access DRS
Review of Request for Access to DRS

Accounting for Disclosures

Purpose
The purpose of this policy is to explain the procedures involved in accounting for disclosures of health plan individual, beneficiary or patient's PHI.

Policy
Health plan individual, beneficiary, patients or authorized personal representative shall have the right to receive an accounting of PHI disclosures made by Janus Youth Program in the six years prior to the request. Janus Youth Program is not required to account for any disclosures that occurred prior to the compliance date of April 14, 2004.

Janus Youth Program must account for disclosures of PHI for occurrences other than Treatment, Payment or Health care Operations (TPO). These types of disclosures require an authorization from either the health plan individual, beneficiary, patient or personal representative.

Disclosures for law enforcement purposes or required by law do not need an authorization.

Procedure

Requests for an Accounting
All requests for an accounting must be submitted in writing and signed by the health plan individual, beneficiary, patient or their personal representative.

- Do not process any request that is not in writing and appropriately signed;
- Do not process any requests if signed by the health plan individual, beneficiary or patient's personal representative and the personal representative has not provided information to support his/her authority to act on behalf of the health plan individual, beneficiary or patient; (see "Verification of Identity of Persons Requesting PHI")
- If the request form does not specify a period of time for the accounting, prepare the accounting to include all applicable disclosures between the date of receipt and April 14, 2004.

Response Time

- When a written request for an accounting is received, the accounting must be provided within 60 days after receipt of the accounting request;
- If the accounting request cannot be processed within the required 60 days, one 30-day extension may be taken.

The health plan individual, beneficiary, patient or personal representative must be notified of the extension in writing and the notice must be sent before the original 60 days have lapsed. Only one extension may be taken and the notice must inform the health plan individual, beneficiary, patient or personal representative of the reasons for the extension and the date by which a response is intended.

Business Associates

- The accounting must include all applicable disclosures made by our Business Associates, as well as those made by one of our Plans;
- When an accounting request is received, each Business Associate with access to the health plan individual, beneficiary or patient's records will be sent a copy of the Request for Accounting of Disclosures of PHI Form within five days of the receipt of the accounting request.

Content of the Accounting

- The accounting must include disclosures (but not uses) of the requesting health plan individual, beneficiary or patient's PHI made by a Health Plan and Business Associate during the period requested by the health plan individual, beneficiary or patient up to six years prior to the request. Note, however, that there is no requirement to account for any disclosures made prior to April 14, 2004.
- The accounting must include the following information for each reportable disclosure of the individual's protected health information:

    - The date of disclosure;
    - The description of PHI disclosed;
    - The Name of the Plan for which PHI was collected or held;
    - The Name of the Entity or person to whom the information was disclosed;
    - The reason for the disclosure; and
    - The Name of the person making the disclosure.

- Approval/denial for a Request for Accounting of Disclosures of PHI should be made by the HIPAA Privacy Officer and a copy of the approval/denial should be included in the health plan individual, beneficiary or patient's confidential file.

Disclosures Janus Youth Program is not required to track:

For example, the Privacy Rule does not require Janus Youth Program to account for disclosures that a person has authorized. Disclosures that need not be tracked include:

- Disclosures covered by a HIPAA authorization form that the person or his or her personal representative has signed;
- Disclosure of PHI in the form of a limited data set;
- Disclosures made to the subject of the PHI; and
- Disclosures that Janus Youth Program makes for treatment, payment, or internal audit or investigation purposes, or for very specific national security, intelligence or law enforcement purposes.

Disclosures Janus Youth Program must track:

- Disclosures of PHI to health oversight agencies;
- Disclosures of PHI to law enforcement agencies;
- Disclosures of PHI to government agencies;
- Disclosures of PHI for research purposes under an Institutional Review Board (IRB) waiver (when a Limited Data Set (LDS) is NOT used);
- Disclosures Required by Law; and
- Any unintentional and intentional breaches.

In the event of a disclosure of PHI, which Janus Youth Program is required to track, the disclosure should be recorded in a PHI disclosure log and maintained with the health plan individual, beneficiary or patient's confidential file. See Forms Addendum - Form of PHI Disclosure Log.

Related Documents
Request for Accounting of Disclosures of PHI
Approval/Denial Letter
PHI Disclosure Log
Authorization To Use and/or Disclose PHI

Individual's Authorization

Purpose
Janus Youth Program may use or disclose PHI only as permitted or required by state law and HIPAA regulations. HIPAA regulations require a health plan individual, beneficiary or patient's signed authorization to use or disclose PHI for all purposes not explicitly permitted under the regulations.

Policy
A health plan individual, beneficiary or patient in a Health Plan may request that Janus Youth Program disclose PHI Janus Youth Program retains about them to a third party. For example, a health plan individual, beneficiary or patient request assistance in helping them resolve claims issues with their health plans. As this type of disclosure is not for our "payment or health care operations", to the person who is the subject of the information, to the Department of HHS or "required by law".

Janus Youth Program may not make these types of disclosures unless it receives an authorization from the health plan individual, beneficiary, patient or personal representative.

Procedure

1. If an authorization is required, no use or disclosure of PHI shall be made until the health plan individual, beneficiary, patient or the personal representative has signed an authorization permitting the use or disclosure.

2. Before making any uses or disclosures as permitted by a signed authorization form, determine if the authorization form is valid. Valid authorization forms are those that:

    - Are properly signed and dated by the health plan individual, beneficiary, patient or the personal representative;
    - Are not expired or revoked (The expiration date of the authorization form must be a specific date (such as July 1, 2003) or a specific time period (e.g., one year from the date of signature), or an event directly relevant to the health plan individual, beneficiary or patient for the purpose of the use or disclosure (e.g., for the duration of the health plan individual, beneficiary or patient's coverage);
    - Contain a statement regarding the health plan individual, beneficiary or patient's right to revoke the authorization and the procedures for revoking authorizations; and
    - Contain a statement regarding the possibility for a subsequent re-disclosure of the information.

All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

If an authorization form is signed by the health plan individual, beneficiary or patient's personal representative, a Janus Youth Program workforce member must verify the authority of the personal representative to act on behalf of the health plan individual, beneficiary or patient in accordance with our Verification Policy (see "Verification of Identity of those Requesting Protected Health Information").

Related Documents
Authorization To Use and/or Disclose PHI

Section 3 - Safeguarding PHI

- Communications with Business Associates
- Verification of Identity of Persons Requesting PHI
- Copying and Printing PHI
- Disposal of PHI
- Storage of PHI Faxing PHI Privacy Complaint
- Sanctions for Violations of Privacy Procedures
- Workforce Training

Communications with Business Associates

Purpose
The purpose of this policy is to identify Janus Youth Program Business Associates and define a Business Associate.

Policy
Janus Youth Program may disclose PHI to the Business Associates and Janus Youth Program may allow its Business Associates to create or receive PHI on its behalf. However, prior to doing so, Janus Youth Program must first obtain assurances; through Business Associate Agreements, from the Business Associate that it will appropriately safeguard the information.

Janus Youth Program Business Associates (see list of current Business Associates)

- Benefits Broker
- Service Consultants
- Account Administrator
- Other External IT Providers
- Other Health Care Service Providers

Procedures
Disclosures of PHI may NOT be made to external consultants, firms or administrators in the absence of a written Business Associate Agreement.

If you regularly interact with external consultants or contractors who meet the definition of a "Business Associate", a Janus Youth Program workforce member must contact the HIPAA Privacy Officer and verify that a "Business Associate" contract is obtained and valid. The Business Associate contract will contain provisions to ensure that the Business Associate complies with the privacy laws in its use and disclosure of PHI.

For example, the Business Associate contract must:

- Establish the permitted and required uses and disclosures by the Business Associate, which may not exceed that which is allowed for in the underlying service agreement such as, “as necessary to perform the services set forth in service agreement.”
- Be prohibited from using or disclosing the PHI other than as permitted by law; including implementing requirements of HIPAA security Rules with regards to Electronic Protection Health Information (EPHI);
- Implement safeguards to prevent the improper use and disclosure of PHI; including incidents that constitute breaches of unsecured Protected Health Information (PHI);
- Inform Janus Youth Program HIPAA Privacy Officer when it becomes aware of any use or disclosure of PHI that is not provided for in the Business Associate contract;
- Impose the same requirements on all subcontractors of the Business Associate;
- Make PHI available in compliance with the individual's right to access, amend and receive an accounting related to such information; as well as to make available Protected Health Information for amendments (and incorporate any amendment, if required);

- Carry out a covered Entity's obligation under the Privacy Rule, require the Business Associate to comply with the requirements applicable to the obligation;
- Make its internal books and records available to the HHS for purposes of determining Janus Youth Program compliance with the federal and state privacy laws;
- Return or destroy all PHI received from, or created or received by or on behalf of Janus Youth Program, if feasible, upon termination of the relationship;
- Ensure that any subcontractors it may engage on its behalf that will have access to PHI agree to the same restrictions and conditions that apply to the Business Associate with respect to such information; and
- Authorize Janus Youth Program to terminate the contract if the Business Associate has violated a material term of the contract; contracts between Business Associates and Business Associates that are subcontractors are subject to these same requirements.

Verification of Identity of Persons Requesting PHI

Purpose
The purpose of this policy is to verify the identity and the authority of those health plan individuals, beneficiaries and patients requesting PHI.

Policy
Janus Youth Program must take steps to verify the identity of a health plan individual, beneficiary or patient who request access to PHI and the authority of any such person to have access to PHI, if the identity or authority of such person is not known to us.

Procedure

When a health plan individual, beneficiary or patient requests access to their PHI:

Janus Youth Program is required to give its health plan individuals, beneficiaries or patients access to PHI about them, under most circumstances. If the health plan individual, beneficiary or patient requests access in person, follow these procedures:

- Request a form of identification from the health plan individual, beneficiary or patient. A Janus Youth Program workforce member may rely on a valid driver's license, passport or other photo identification issued by a government agency;
- Make a copy of the identification provided by the health plan individual, beneficiary or patient and file it with the health plan individual, beneficiary or patient's designated record set;
- Verify that the identification matches the identity of the health plan individual, beneficiary or patient requesting access to the PHI. If the workforce member has any doubts as to the validity or authenticity of the identification provided or the identity of the health plan individual, beneficiary or patient requesting access to the PHI, communicate with the Janus Youth Program HIPAA Privacy Officer.

1. If the health plan individual, beneficiary or patient requests PHI over the telephone, verify their identity by requesting their Social Security number, date of birth and other verifiable information (consider having the health plan individual, beneficiary or patient sign a release form prior to releasing PHI).

2. Verification of a Personal Representative:

   If a personal representative of a health plan individual, beneficiary or patient requests access to PHI about the health plan individual, beneficiary or patient, a workforce member must either:

   - Ask relevant questions to assess whether an adult acting for a young child has the requisite relationship to the child; or
   - Be provided a copy of a valid power of attorney or other document or order appointing the person as a personal representative. Other documents may include a court order appointing a guardian or personal representative, or in the case of a deceased health plan individual, beneficiary or patient, letters testamentary. The document, and the personal representative's

request for PHI, should be reviewed and approved by the HIPAA Privacy Officer prior to providing the PHI to the personal representative, and should be maintained in the health plan individual, beneficiary or patient's confidential file.

3. Verification of a Public Official:

   If a public official requests access to PHI follow these procedures to verify their Identity:
   - If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status. Make a copy of the identification provided and file it with the health plan individual, beneficiary or patients designated record set.
   - If the request is in writing, verify that the request is on the appropriate government letterhead;
   - If the request is by a person purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

4. When a public official or person acting on behalf of a public official requests access to PHI, follow these procedures to verify their authority:

   - Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority, together with evidence of their capacity, such as an identification card; or
   - If the individual's request is made pursuant to a legal process, warrant, subpoena, order, or other legal processes issued by a grand jury, a judicial or administrative tribunal, communicate with the HIPAA Privacy Officer.

5. Prior to disclosing information to a public official (or person acting on behalf of a public official), communicate with Janus Youth Program HIPAA Privacy Officer so that it may conduct a second level verification of the identity and authority of the public official (or person acting on his behalf).

Related Documents
Authorization To Use and/or Disclose PHI

Copying and Printing PHI

Purpose

The purpose of this policy is to minimize inadvertent disclosures of PHI by providing procedures for management and workforce members regarding copying and printing PHI.

Policy

All Janus Youth Program workforce members must strictly observe the following procedures relating to the printing and copying of PHI.

Procedures

- Printed versions of PHI should not be copied indiscriminately or left unattended and open to compromise;
- Printers and copiers used for printing of PHI should be in a secure, non-public location. If the equipment is in a public location, the information being printed or copied must be strictly monitored;
- PHI printed to a shared printer should be promptly removed.

Disposal of PHI

Purpose

The purpose of this policy is to minimize inadvertent disclosures of PHI by providing management and workforce members with the procedures for the proper disposal of PHI.

Policy

It is the duty of Janus Youth Program to protect the confidentiality and integrity of its health plan individual, beneficiary or patient's PHI. PHI may only be disposed of by means that are reasonably intended to prevent its accidental release to an external party.

Procedures

1. All workforce members must strictly observe the following standards relating to disposal of hardcopy and electronic copies of PHI.

2. PHI must not be discarded in trash bins or other public accessible locations. This information must be personally shredded or placed into secure recycling containers for proper disposal of confidential documents.

3. Printed material and electronic data containing PHI shall be disposed of in a manner that ensures confidentiality.

4. It is the workforce member's responsibility to ensure the document has been secured or destroyed. And it is the HIPAA Privacy Officer's responsibility to ensure that all workforce members are adhering to the policy.

Electronic Copies

Secure methods will be used to dispose of electronic data and output. Any questions of appropriateness of action or carrying out of this procedure should be brought to the attention of the Janus Youth Program HIPAA Privacy Officer. Disposal of electronic data may consist of the following methods:

a. Deleting online data using the appropriate utilities;
b. Removing PHI from mainframe disk drives being sold or replaced, using the appropriate initialization utilities;
c. Erasing flash drives or disk drivers to be re-used using a special utility to prevent recovery of data;
d. Destroying discarded flash drives, CDs, or other removable data forms.

Storage of PHI

Purpose
The purpose of this policy is to provide information for management and workforce members regarding the storage of PHI. This policy also conforms to Administrative Safeguards under Section 164.308.

Policy
Janus Youth Program has a duty to maintain and protect the confidentiality and integrity of health plan individual, beneficiary and patient's PHI. This policy defines the guidelines and procedures that must be followed for the storage of PHI. All workforce members must strictly observe the following standards relating to the storage of PHI:

Procedure

1. Outside of regular working hours, all desks and working areas that contain PHI are properly secured or the entire area can be secured from unauthorized access.

2. When not in use, PHI must always be protected from unauthorized access. When left in an unattended room, such information must be appropriately secured.

3. Workstation's handling of EPHI are equipped with electronic devices to ensure the security of PHI in accordance with HIPAA Security Rule §164.308(a)(4) and the HIPAA Privacy Rule at §164.508.

4. If PHI is to be stored on the hard disk drive or other internal components of a personal computer, laptops, PDA (Personal Digital Assistant) or any other form of electronic devices, they are to be appropriately protected by password, encryption, software and other necessary means of access control. When not in use, unless device is encrypted, this media must be secured from unauthorized access.

5. If PHI is stored on flash drive, CD-ROM or other removable data storage media, it cannot be co-mingled with other electronic information or devices.

6. Each health plan individual, beneficiary or patient's PHI must be maintained in accessible form for a period of six years, or as designated by federal or state Law. Thereafter, the PHI may be disposed of as provided in these policies and procedures.

Faxing Protected Health Information

Purpose
The purpose of this policy is to minimize inadvertent disclosures of PHI by defining appropriate standards for transmitting PHI via fax.

Policy
It is the policy of Janus Youth Program to protect the fax transmission of PHI and hold workforce members responsible for following the proper procedure when PHI is sent via fax. This policy defines the minimum guidelines and procedures that must be followed when transmitting a health plan individual, beneficiary or patient's PHI via fax.

Procedures

1. Information transmitted must be limited to the minimum necessary to meet the requestor's needs.

2. Except as authorized by the health plan individual, beneficiary or patient's consent for Treatment, Payment, or Health Care Operations (TPO) or federal or state law, a properly completed and signed authorization must be obtained before releasing PHI. (See Individual's Authorization)

3. A "Fax Cover Letter" must be used to send faxes containing PHI:

    a. Confidential documents must be marked "Confidential" before they are transmitted. Workforce members must make reasonable efforts to ensure that the fax is being transmitted to the correct destination;
    b. The Fax Cover Letter MUST contain an appropriate confidentiality notice - see Forms Addendum - Form of Fax Containing PHI.

4. Misdirected Faxes:

    a. If a fax transmission containing PHI is not received by the intended recipient because of a mis-dial, check the fax machine to obtain the misdialed number.
    b. If possible, a phone call, supplemented by a note referencing the conversation, should be made to the recipient of the misdirected fax requesting that the entire content of the misdirected fax be destroyed.
    c. If the recipient cannot be reached by phone, a fax using the "Notice of Misdirected Fax" should be sent to the recipient requesting that the entire content of the misdirected fax be destroyed. See Forms Addendum - Notice of Misdirected Fax.
    d. A Log of Misdirected Faxes must be maintained for Accounting of Disclosures of PHI.

5. Fax PHI to the HIPAA Privacy Officer using the fax number listed on the form.

6. When expecting the arrival of a fax containing PHI, schedule with the sender whenever possible so the faxed document can be promptly retrieved.

7. Make sure faxes containing PHI are placed in a secure and confidential place when they are delivered.

8. Confirm the accuracy of fax numbers (and security of recipient machines) by calling the intended recipients to double-check the numbers, verify the security of their machines, notify them that your fax is on the way, and request verification of its receipt. Do not rely on fax numbers listed in directories or provided by persons other than the recipient.

9. Make sure fax machine prints a confirmation of each outgoing transmission and require machine operators to (a) make sure the intended destination matches the number on the confirmation, and (b) staple the confirmation to the document that was faxed.

Related Documents/Procedures
Fax Cover Letter
Notice of Misdirected Fax
Authorization To Use and/or Disclosure PHI

Privacy Complaint

Purpose
The purpose of this policy is to provide information for management and workforce members for handling privacy complaints.

Policy
Any individual who believes his or her rights granted by the HIPAA Privacy regulations or any other state or federal laws dealing with privacy and confidentiality of health information have been violated may file a complaint regarding the alleged privacy violation.

Procedure

1. Janus Youth Program has established three ways to receive health plan individual, beneficiary or patient complaints regarding privacy issues on a confidential and/or anonymous basis, including:

    - By calling and speaking with or leaving a message at the designated number listed on the form.
    - By sending an email to the email address listed on form. (NOTE: To ensure confidentiality, this e-mail account automatically removes the sender's contact information from the message header. A health plan individual, beneficiary or patient who wishes to disclose his or her identity will need to include contact information in the body of the e-mail.)
    - By sending a letter via U.S. Mail or overnight delivery to:

        Dennis Morrow
        HIPAA Privacy Officer
        Janus Youth Programs
        707 NE Couch Street
        Portland, OR 97232
        (503) 542-4607

2. Investigation of Complaints:

    - Janus Youth Program will investigate alleged privacy violations and complaints made by health plan individuals, beneficiaries or patients regarding alleged breaches of their privacy. Workforce members and management may be requested to assist in investigations regarding complaints made by health plan individuals, beneficiaries or patients who believe fellow workforce members have violated individual privacy standards.
    - Janus Youth Program will begin an investigation to determine if a breach of privacy has occurred. All complaints will be reviewed and researched promptly, although no response can be made directly to any individuals who provide anonymous and/or confidential tips.
    - Janus Youth Program will not discharge, demote, suspend, threaten, harass, or in any manner illegally discriminate against a workforce member who uses the complaint process. Any workforce member found to be in violation of this policy or breaches the confidentiality of an individual's protected health information will be subject to disciplinary action, termination of employment and civil or criminal penalties as defined by law.

Sanctions for Violations of Privacy Procedures

Purpose
Employment related sanctions and civil and criminal penalties support the enforcement of privacy laws in the workplace.

Policy
It is a workforce member's responsibility to report any suspected or actual privacy violations to the Janus Youth Program HIPAA Privacy Officer.

Sanction Exemptions

Sanctions will not apply to disclosures by workforce members who are ***whistleblowers*** or ***crime victims***. Janus Youth Program is not considered to have violated PHI disclosure requirements if the disclosure is by a workforce member or Business Associate as follows:

***Disclosure by Whistleblowers*:**

- The workforce member is acting in good faith on the belief that Janus Youth Program has engaged in conduct that is unlawful or otherwise violates professional standards;
- The disclosure is made to a federal or state health oversight agency or public health authority authorized by law to oversee the relevant conduct or conditions of the covered Entity; or
- The disclosure is made to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by Janus Youth Program; or
- The disclosure is made to an attorney retained by or on behalf of the health plan individual, beneficiary, patient, personal representative or Business Associate for the purpose of determining legal options regarding disclosure conduct.

Disclosure by Crime Victims:

- A covered Entity is not considered to have violated the use and disclosure requirements if a member of its workforce who is the victim of a criminal act discloses PHI to a Law Enforcement Official about the suspected perpetrator of the criminal act and the disclosed PHI is limited to identification and location purposes.

Mitigation

- Janus Youth Program will take all practical steps to reduce the harmful effects caused by uses or disclosures of PHI in violation of its policies or procedures and the HIPAA Privacy Rule;
- As soon as it learns about such a violation by the health care provider or its Business Associates, Janus Youth Program's HIPAA Privacy Officer will halt the use or disclosure and seek the return or destruction of any documents or other information that was disclosed.

Retaliation

Janus Youth Program will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an individual who:

- Exercises his or her rights or participates in the complaint process; or,
- Files a complaint with the Secretary of Health and Human Services; or,
- Testifies, assists or participates in an investigation, compliance review, proceeding or hearing; or,
- Opposes any act or practice unlawful under HIPAA, provided the individual acted in good faith, believing that the practice was unlawful, the manner of opposition is reasonable, and does not involve disclosure of PHI in violation of HIPAA regulations.

Employment Related Sanctions - Categories of Breaches

The following is a general guideline to managers to serve as an aid in the reporting, investigatory and/or disciplinary processes.

1. Failing to demonstrate appropriate care in handling confidential information that results in accidental access, incidental access or inappropriate access due to lack of awareness and/or education. Examples include but are not limited to:

    - Failing to sign off a computer terminal when leaving the work area;
    - Leaving confidential information unattended in a non-secure area or disclosing a health plan individual, beneficiary or patient's identifiable information by careless telephone use, or discussions in hallways, elevators or other work areas;
    - Leaving confidential information displayed on computer screens, desks, or work stations where others can view it;
    - Accessing personal demographic information, such as dates of birth, addresses or telephone numbers when these are not required to do job responsibilities.

2. Purposeful disregard of organization policy related to the appropriate use and disclosure of confidential information, or continued demonstration of behaviors listed above. Examples include but are not limited to:

    - Sharing ID/passwords with co-workers or encouraging them to share;
    - Failure to follow appropriate guidelines for the use of fax, email, or computer transmission of health plan individual, beneficiary or patient's information.

3. Unauthorized access to health plan individual, beneficiary or patient's information or repeated violations of previous breaches. Examples include but are not limited to:

    - Accessing confidential medical information on a health plan individual, beneficiary or patient for whom you have no job-related responsibility, including friends and family individual, beneficiary, patient's;
    - Providing ID or password to unauthorized workforce members or persons.

4. Major disregard of organization policies or repeated demonstrations of behaviors listed above. Examples include but are not limited to:

    - Using another workforce member's password without their knowledge;
    - Releasing data for personal gain;
    - Use or disclosure of PHI requiring health plan individual, beneficiary or patient's authorization without it;
    - Destroying or altering data intentionally;
    - Releasing data with intent to harm the reputation of an individual or the organization;
    - Accessing sensitive records when the information is not needed to perform Janus Youth Program workforce member job responsibilities.

Retention and Accounting for Disclosures

Specific records related to disciplinary action as a result of breach of confidentiality policies or procedures will be maintained in the workforce member file. All confirmed violations will be reported in any accounting for disclosures of the respective health plan individual, beneficiary or patient.

Procedure and Employment Related Sanctions

1. Janus Youth Program workforce member will be required to attend a refresher HIPAA training session, if workforce member inadvertently discloses PHI;

2. If repeated inadvertent disclosures of PHI occur, Janus Youth Program workforce member is subject to disciplinary action up to and including termination;

3. If a Janus Youth Program workforce member intentionally discloses a health plan individual, beneficiary or patient's PHI, and such disclosure is neither a permitted nor required disclosure, the Janus Youth Program workforce member will be subject to termination.

Civil and Criminal Penalties

In addition to the employment related sanctions described above, HIPAA imposes civil and criminal penalties for unauthorized disclosure of PHI. The penalties that may be imposed for Privacy Rule Violations are as follows:

- ***Civil Penalties**:* $100 per violation up to $25,000 per category of violation per year. One act or failure to comply could amount to more than one standard, so potential penalties are more than $25,000 per year.
- ***Criminal Penalties**:* Fines up to $250,000 and up to 10 years imprisonment, for impermissible use of PHI or for disclosure made under false pretenses, or for personal gain, commercial advantage, or to cause malicious harm.

  Example – an employee "workforce member" with access to PHI obtains the PHI of a health plan member or patient and, without consent, provides the PHI to a third party to use as evidence in a child custody matter against the health plan member or patient. Such disclosure could subject the employee "workforce member" to significant civil and criminal penalties.

Workforce Training

Purpose
To comply with the HIPAA Privacy Laws, Janus Youth Program must provide privacy training to those members of our workforce who will be impacted by the HIPAA Privacy Laws.

Policy
It is Janus Youth Program policy to train those members of our workforce (see Classes of Workforce "Employee" and Approved Uses), who will be impacted by the HIPAA Privacy Laws, on our privacy policies and procedures. The Operations and Administration shall develop training schedules and programs so that our workforce members receive the training necessary and appropriate to permit them to carry out their functions.

All workforce members handling and administering PHI are required to complete PHI Confidentially Agreement as part of the employment process.

Procedure

1. **Training Announcement.** Janus Youth Program HIPAA Privacy Officer and/or the Operations and Administration will determine the appropriate means by which to announce to the workforce the HIPAA training sessions. Such means may include intranet announcements, postings on the Janus Youth Program Event Calendar, email or etc.

2. **General Training and Education.** Designated members of the workforce are required to complete a general training and education session as defined under section §164.308, §164.503, §164.501, §164.508 and §164.530. Completion is mandatory and will be documented to ensure full compliance. Topics to be covered at the general session will include:

    - The responsibilities of workforce members with respect to handling a health plan individual, beneficiary and patient's confidential information;
    - Janus Youth Program HIPAA Privacy Policies and Procedures applicable to the workforce;
    - The personal and ethical obligations of each workforce individual, beneficiary with respect to health plan individual, beneficiary or patient's PHI; and
    - The disciplinary actions and legal sanctions applicable to workforce members who violate the privacy policies and procedures.

3. **Timing.** The members of the workforce must receive the appropriate privacy training within a reasonable period of time after joining Janus Youth Program.

4. **Subsequent Training.** Subsequent training will be provided for workers whose job functions are affected by a material change in the policies and procedures within a reasonable period of time after the change becomes effective, but no more than once every two years or as required by federal or state law.

5. **Records and Documentation.** The Operations and Administration shall assure that records of training and education sessions are being kept and maintained. Such records and documentation should at least include the following information:

    - The date, time and approximate duration of the training sessions;
    - List of attendees;
    - The general subject matter and method of presentation;
    - Any feedback;
    - A certificate of completion.

HIPAA Security Rules & Policies

Purpose
Janus Youth Program is committed to ensuring the privacy and security of PHI. In order to manage the facilitation and implementation of activities related to the privacy and security of PHI, Janus Youth Program will appoint and maintain an internal HIPAA Security Officer position.

As required in 45 C.F.R. § 164.308(a)(2), Assigned Security Responsibility, the purpose of this policy is to establish how the HIPAA Security Officer will serve as the focal point for security compliance-related activities and responsibilities, as listed below. The final responsibility for the implementation and maintenance of the security program must rest with one individual. In general, the HIPAA Security Officer is charged with developing, maintaining, implementing organizational policies and procedures, conducting educational programs, reviewing conduct of those assigned security responsibilities and administering reviews relating to the Janus Youth Program HIPAA security program.

Applicability
A covered Entity or Business Associate must comply with the applicable standards, implementation specifications and requirements of this subpart with respect to electronic PHI of a covered Entity as in section §164.302.

Definitions

Reference Janus Youth Programs “HIPAA-HITECH Privacy and Security Glossary”

Access. The ability or the means necessary to read, write, modify, communicate data/information or otherwise use any system resource. (This definition applies to “access” as used in section 164.304 subpart, not as used in subparts D or E of this part.)

Administrative Safeguards. Administrative actions, policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered Entity's or Business Associate's workforce in relation to the protection of that information.

Authentication. The corroboration that a person is the one claimed.

***Availability*.** The property that data or information is accessible and useable upon demand by an authorized person.

Confidentiality. The property that data or information is not made available or disclosed to unauthorized persons or processes.

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

Facility. The physical premises and the interior and exterior of a building(s).

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

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

***Malicious Software*.** Software, for example, a virus, designed to damage or disrupt a system.
Password means confidential authentication information composed of a string of characters.

Physical Safeguards. The physical measures, policies, and procedures to protect a covered Entity's or Business Associate's electronic information systems and related buildings and equipment from natural hazards, environmental hazards, and unauthorized intrusion.

Security or Security Measures. Encompass all of the administrative, physical, and technical safeguards in an information system.

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

Technical Safeguards. The technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

Policy
HIPAA Security Rule Policies

Janus Youth Programs will identify the security official who is responsible for the development and implementation of the policies and procedures required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and, specifically, Subpart C Security Standards for the protection of electronic protected health information (EPHI) of PART 164 - Security and Privacy.

Procedures:

Qualifications

1. The HIPAA Security Officer must demonstrate familiarity with the legal requirements relating to privacy and health care operations, as well as the ability to communicate effectively with and coordinate the efforts of technology and non-technology. Information security will cover legal issues, hardware and software security, as well as physical security.

2. It is desirable that the HIPAA Security Officer has a background that includes the following:

    a. Bachelor's degree or higher from an accredited institution in Management Information Systems, Computer Science, Business Administration or similar discipline;
    b. Security certification (e.g., Certified Information Systems Security Professional (CISSP));
    c. Minimum of three years of information security experience.

Identification and Replacement

1. The current HIPAA Security Officer is:

   Tanika Barsegian
   (503) 341-1557

2. The backup HIPAA Security Officer is:

   TBD

3. In the event that the HIPAA Security Officer needs to be replaced, the backup HIPAA Security Officer will be the interim HIPAA Security Officer. A search for a replacement HIPAA Security Officer will be conducted and the position filled as soon as possible. Final determination of a newly designated HIPAA Security Officer will be appointed by Janus Youth Programs Executive Director.

4. All workforce members will be made aware of the HIPAA Security Officer's identity, as well as the HIPAA Security Officer's role and responsibilities. Any HIPAA Security Officer changes will be promptly communicated.

Responsibilities

1. The HIPAA Security Officer leads in the development, awareness and enforcement of information security policies and procedures, measures and mechanisms to ensure prevention, detection, containment and correction of security incidents. The HIPAA Security Officer will also ensure that the policy/procedure requirements comply with statutory and regulatory requirements regarding security of EPHI.

2. The HIPAA Security Officer maintains security policies that include:

   - Administrative Safeguards: Formal mechanisms for risk analysis and management, information access controls and appropriate sanctions for failure to comply;
   - Physical Safeguards: Ensure assigned security responsibilities, control access to media (e.g., flash drives, tapes, backups, disposal of data), protect against hazards and unauthorized access to computer systems and secure workstation locations and use. The HIPAA Security Officer may co-ordinate with the building security or facilities management for this purpose;
   - Technical Safeguards: Establish access controls, emergency procedures, authorization controls and data/Entity access and authentication.

3. The HIPAA Security Officer maintains security procedures that include:

   - Evaluation of compliance with security measures;
   - Contingency plans for emergencies and disaster recovery;
   - Security incident response process and protocols;
   - Testing of security procedures, measures and mechanisms and continuous improvement;
   - Security incident reporting mechanisms and sanction policy;

- Proper documentation of security incidents and the responses to them.

4. The HIPAA Security Officer maintains appropriate security measures and mechanisms to safeguard against unauthorized access to electronically stored and/or transmitted patient data and protect against reasonably anticipated threats and hazards, for example:

   - Integrity controls
   - Authentication controls
   - Access controls
   - Encryption
   - Abnormal condition alarms, audit trails, Entity authentication and event reporting.

HIPAA Security Rule Policies

1. The HIPAA Security Officer oversees and/or performs on-going security monitoring of organization information systems

2. The HIPAA Security Officer is responsible for directing or conducting periodic risk assessments as systems or processes change or new ones are added. The HIPAA Security Officer will also be responsible for obtaining sign-off from appropriate management for acceptance of residual risks.

3. The HIPAA Security Officer will conduct functionality and gap analyses to determine the extent to which key business areas and infrastructure comply with statutory and regulatory requirements.

4. The HIPAA Security Officer will evaluate and recommend new information security technologies and counter-measures against threats to information or privacy.

5. The HIPAA Security Officer ensures ongoing compliance through suitable training/awareness programs and periodic security audits.

6. The HIPAA Security Officer serves as a resource regarding matters of informational security, and on a periodic basis, reports the status of information security activities to the Executive Director of the organization. Who is responsible for over all forms of electronic transmission of data such as Executive Compliance Committee.

7. The HIPAA Security Officer will ensure that security concerns have been addressed in system implementations including EHRs and any exchange of health information with health plan individuals, beneficiaries, patients or external Entities.

Regulatory Authority

45 C.F.R. §164.308(a) (2) Administrative Safeguards
(a) A covered Entity* must, in accordance with § 164.306:2. Standard: Assigned security responsibility. Identify the HIPAA Security Officer who is responsible for the development and implementation of the policies and procedures required by this subpart for the Entity.

Notification in Case of Breach

1. **In General**. A covered Entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered Entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered Entity to have been, accessed, acquired, or disclosed as a result of such breach.

2. **Notification of Covered Entity by Business Associate**. A Business Associate of a covered Entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered Entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during such breach.

3. **Breaches Treated as Discovered**. For purposes of this section, a breach shall be treated as discovered by a covered Entity or by a Business Associate as of the first day on which such breach is known to such Entity or associate, respectively, (including any person, other than the individual committing the breach, that is a workforce member, officer, or other agent of such Entity or associate, respectively) or should reasonably have been known to such Entity or associate (or person) to have occurred (determined in accordance with the Federal common law of agency).

4. **Timeliness of Notification**:

    a. **In General**. Subject to subsection (g), all notifications required under this section shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by the covered Entity involved (or Business Associate involved in the case of a notification required under subsection (b));
    b. **Burden of Proof**. The covered Entity involved (or Business Associate involved in the case of a notification required under subsection (b)), shall have the burden of demonstrating that all notifications were made as required under this part, including evidence demonstrating the necessity of any delay.

5. **Methods of Notice**:

    a. **Individual Notice**. Notice required under this section to be provided to an individual, with respect to a breach, shall be provided promptly and in the following form:
        i. Written notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if specified as a preference by the individual, by electronic mail. The notification may be provided in one or more mailings, as information is available;
        ii. In the case in which there is insufficient, or out-of-date contact information (including a phone number, email address or any other form of appropriate communication) that precludes direct written (or, if specified by the individual under subparagraph (A), electronic) notification to the individual, a substitute form of notice shall be provided, including, in the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a period of 90 days

determined by the Secretary on the home page of the website of the covered Entity involved or notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting will include a toll-free phone number where an individual can learn whether or not the individual's unsecured protected health information is possibly included in the breach;

iii. In any case deemed by the covered Entity involved to require urgency because of possible imminent misuse of unsecured protected health information, the covered Entity, in addition to notice provided under subparagraph (A), may provide information to individuals by telephone or other means, as appropriate.

b. **Media Notice**. Notice shall be provided to prominent media outlets serving a State or jurisdiction, following the discovery of a breach described in subsection (a), if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

c. **Notice to Secretary**. Notice shall be provided to the Secretary by covered Entities of unsecured protected health information that has been acquired or disclosed in a breach. If the breach was with respect to 500 or more individuals, then such notice must be provided immediately. If the breach was with respect to less than 500 individuals, the covered Entity shall maintain a log of any such breach occurring and other documents. Additionally, no later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS website.

d. **Posting on HHS Public Website**. The Secretary shall make available to the public on the Internet website of the Department of Health and Human Services a list that identifies each covered Entity involved in a breach described in subsection (a) in which the unsecured protected health information of more than 500 individuals is acquired or disclosed.

6. **Content of Notification**. Regardless of the method by which notice is provided to individuals under this section, notice of a breach shall include, to the extent possible, the following:

   a. A brief description of what happened, including the date of the breach and if known, the date of the discovery of the breach;
   b. A description of the types of unsecured protected health information that was involved in the breach (such as full Name, Social Security number, date of birth, home address, account number, or disability code);
   c. The steps individuals should take to protect themselves from potential harm resulting from the breach;
   d. A brief description of what the covered Entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches;
   e. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll free telephone number, an e-mail address, website, or postal address.

7. **Delay of Notification Authorized for Law Enforcement Purposes**. If a law enforcement official determines that a notification, notice, or posting required under this section would impede a criminal investigation or cause damage to national security, such notification, notice or posting shall be delayed in the same manner as provided under section 164.528(a)(2) of title 45, Code of Federal Regulations, in the case of a disclosure covered under such section.

8. **Unsecured Protected Health Information**:

    a. **Definition** -
        i. **In General**. Subject to subparagraph (B), for purposes of this section, the term ''unsecured protected health information'' means protected health information that is not secured through the use of a technology or methodology specified by the Secretary in the guidance issued under paragraph (2).
        ii. **Exception in Case Timely Guidance Not Issued**. In the case that the Secretary does not issue guidance under paragraph (2) by the date specified in such paragraph, for purposes of this section, the term ''unsecured protected health information'' shall mean protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.
    b. **Guidance**. For purposes of paragraph (1) and section 13407(f)(3), no later than the date that is 60 days after the date of the enactment of this Act, the Secretary shall, after consultation with stakeholders, issue (and annually update) guidance specifying the technologies and methodologies that render protected health information unusable, unreadable or indecipherable to unauthorized individuals, including the use of standards developed under section 3002(b)(2)(B)(vi) of the Public Health Service Act, as added by section 13101 of this Act.

9. **Report to Congress on Breaches**:

    a. **In General**. Not later than 12 months after the date of the enactment of this Act and annually thereafter, the Secretary shall prepare and submit to the Committee on Finance, the Committee on Health, Education, Labor, and Pensions of the Senate, as well as the Committee on Ways and Means, the Committee on Energy and Commerce of the House of Representatives a report containing the information described in paragraph (2) regarding breaches for which notice was provided to the; Secretary under subsection (e)(3).
    b. **Information.** The information described in this paragraph regarding breaches specified in paragraph (1) shall include:
        i. The number and nature of such breaches; and
        ii. Actions taken in response to such breaches.

10. **Regulations; Effective Date**. To carry out this section, the Secretary of Health and Human Services shall promulgate interim final regulations by no later than the date that is 180 days after the date of the enactment of this title. The provisions of this section shall apply to breaches that are discovered on or after the date that is 30 days after the date of publication of such interim final regulation.

11. **Effect On State Law**. Sec. 1178. **[**42 U.S.C. 1320d–7**]** (a) General Effect. —

    (1) General rule. Except as provided in paragraph (2), a provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1172 through 1174, shall supersede any contrary provision of state law, including a provision of state law that requires medical or

health plan records (including billing information) to be maintained or transmitted in written rather than electronic form.

(2) Exceptions. A provision or requirement under this part, or a standard or implementation specification adopted or established under sections 1172 through 1174 shall not supersede a contrary provision of state law, if the provision of state law;

(A) Is a provision the Secretary determines,
(i) is necessary -
(I) to prevent fraud and abuse
(II) to ensure appropriate state regulation of insurance and health plans;
(III) for state reporting on health care delivery or costs; or
(IV) for other purposes; or
(ii) addresses controlled substances; or
(B) Subject to section 264(c)(2) of the Health Insurance Portability and Accountability Act of 1996, relates to the privacy of individually identifiable health information.

(b) Public Health. Nothing in this part shall be construed to invalidate or limit the authority, power, or procedures established under any law providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention.
(c) State Regulatory Reporting. Nothing in this part shall limit the ability of a state to require a health plan to report, or to provide access to, information for management audits, financial audits, program monitoring and evaluation, facility licensure or certification, or individual licensure or certification.

Risk Assessment

The purpose of a risk assessment is to identify conditions where EPHI could be disclosed without proper authorization, improperly modified or made unavailable when needed. This information is then used to make risk management decisions on whether the HIPAA-required implementation specifications are sufficient or what additional addressable implementation specifications are needed to reduce risk to an acceptable level.

Key Terms Defined
When talking about risk, it is important that terminology be defined and clearly understood. This section defines important terms associated with risk assessment and management.

- ***Risk*** is the potential impact that a threat can have on the confidentiality, integrity, and availability on EPHI by exploiting vulnerability.
- ***Threats*** are anything that can have a negative impact on EPHI. Threats are:
    a. Intentional (e.g., malicious intent); or
    b. Unintentional (e.g., mis-configured server, data entry error).

    ***Threat sources are*:**
    a. Natural (e.g., floods, earthquakes, storms, tornados);
    b. Human (e.g., intentional such as identity thieves, hackers, spyware authors; unintentional such as data entry error, accidental deletions); or
    c. Environmental (e.g., power surges and spikes, hazmat contamination, environmental pollution).

- ***Vulnerabilities*** are a flaw or weakness in a system security procedure, design, implementation or control that could be intentionally or unintentionally exercised by a threat.
- ***Impact*** is a negative quantitative and/or qualitative assessment of a vulnerability being exercised on the confidentiality, integrity and availability of EPHI. It can be easy to confuse vulnerabilities and threats. An organization may be vulnerable to damage from power spikes. The threats that could exploit this vulnerability may be overloaded circuits, faulty building wiring, dirty street power, or too much load on the local grid. It is important to separate these two terms in order to assist in proper security control selection. In this example, security controls could range from installing UPS systems, additional fuse boxes, or standby generators or rewiring the office. These additional security controls may help to mitigate the vulnerability but not necessarily for each threat.

HIPAA Risk Assessment Requirements
Standard 164.308(a)(1)(i), *Security Management Process,* requires covered Entities to: *Implement policies and procedures to prevent, detect, contain, and correct security violations.*

The Security Management Process standard includes four required implementation specifications. Two of these specifications deal directly with risk analysis and risk management.

- **Risk Analysis (R123)** - 164.308(a)(1)(ii)(A): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by the covered Entity.

- **Risk Management (R)** - 163.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).

How to Conduct the Risk Assessment: Risk assessments can be conducted using many different methodologies. There is no single methodology that will work for all organizations and all situations. The following steps represent key elements in a comprehensive risk assessment program and provide an example of the risk assessment methodology described in NIST SP 800-30. It is expected that these steps will be customized to most effectively identify risk for an organization based on its own uniqueness. Even though these items are listed as steps, they are not prescriptive in the order that they should be conducted. Some steps can be conducted simultaneously rather than sequentially.

1. **Scope the Assessment.** The first step in assessing risk is to define the scope of the effort, resulting in a general characterization of the information system, its operating environment and its boundary. To do this, it is necessary to identify where EPHI is created, received, maintained, processed or transmitted.

   The scope of a risk assessment should include both the physical boundaries of a covered Entity's location as well as a logical boundary covering the media containing EPHI, regardless of its location. Ensure that the risk assessment scope takes into consideration the remote work force and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and backup media).

2. **Gather Information.** During this step, the covered Entity should identify: The conditions under which EPHI is created, received, maintained, processed or transmitted by the covered Entity; and "R" indicates a required implementation specification.

   This step is essential to ensure that vulnerabilities and threats are correctly identified. For example, an invalidated belief that a policy is being followed can miss a potential vulnerability, and not knowing about portable media containing EPHI can miss a threat to that environment. The level of effort needed to gather the necessary information depends heavily on the scope of the assessment and the size of the covered Entity.

3. **Identify Realistic Threats.** Often performed simultaneously with step 4 (*Identify Potential Vulnerabilities)* the goal of this step is to identify the potential threat sources and compile a threat statement listing potential threat-sources that are applicable to the covered Entity and its operating environment. The listing of threat sources should include realistic and probable human and natural incidents that can have a negative impact on an organizations ability to protect EPHI. Threats can be easily identified by examining the environments where EPHI is being used.

   Many external sources can be used for threat identification. Internet searches, vendor information, insurance data and crime statistics are all viable sources of threat data. Examples of some common threat sources are listed in **Table 5** on the following page.

Table 5. Common Threat Sources

Type	***Examples***
Natural	Floods, earthquakes, tornados, landslides, avalanches, electrical storms, and other such events.
Human	Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network-based attacks, malicious software upload, and unauthorized access to confidential information).
Environment	Long-term power failure, pollution, chemicals, liquid lead, etc.

4. **Identify Potential Vulnerabilities.** Often performed simultaneously with step 3 (*Identify Realistic Threats)* the goal of this step is to develop a list of vulnerabilities (flaws or weaknesses) that could be exploited by potential threat sources. This list should focus on realistic technical and nontechnical areas where EPHI can be disclosed without proper authorization, improperly modified or made unavailable when needed.

   Covered Entities should use internal and external sources to identify potential vulnerabilities. Internal sources may include previous risk assessments, vulnerability scan and system security test results, and audit reports. External sources may include Internet searches, vendor information, insurance data and vulnerability databases such as the National Vulnerability Database (http://nvd.nist.gov). At the end of this appendix, a suggested (but not all-inclusive) source list is provided that organizations may wish to use to help in vulnerability identification.

5. **Assess Current Security Controls.** Often performed simultaneously with step 2 (*Gather Information)* the purpose of this step is to determine if the implemented or planned security controls will minimize or eliminate risks to EPHI. A thorough understanding of the actual security controls in place for a covered Entity will reduce the list of vulnerabilities, as well as the realistic probability of a threat attacking (intentionally or unintentionally) EPHI. Covered Entities should evaluate technical and nontechnical security controls at all places where EPHI is created, received, maintained, processed or transmitted. This evaluation should determine whether the security measures implemented or planned are adequate to protect EPHI, and whether those measures required by the Security Rule are in place, configured and used properly. The appropriateness and adequacy of security measures may vary depending on the structure, size and geographical dispersion of the covered Entity.

6. **Determine the Likelihood and the Impact of Threat Exercising Vulnerability.** The next major step in measuring the level of risk is to determine the likelihood and the adverse impact resulting from a threat successfully exploiting vulnerability. This information can be obtained from existing organizational documentation, such as business impact and asset criticality assessments. A business impact assessment prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions. If these organizational documents do not exist, the system and data sensitivity can be determined based on the level of protection required to maintain the EPHI's confidentiality, integrity, and availability. The adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security objectives: integrity, availability, and confidentiality. **Table 6** provides a brief description of each security objective and the consequence (or impact) of it not being met. See **Table 6** on the following page.

Table 6. Security Objectives and Impacts.

Security Objective	Impacts
Loss of Confidentiality	System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment or legal action against the organization.
Loss of Integrity	System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.
Loss of Availability	If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

Some tangible impacts can be measured quantitatively in terms of lost revenue, the cost of repairing the system or the level of effort required to correct problems caused by a successful threat action. Other impacts, such as the loss of public confidence, the loss of credibility or damage to an organization's interest cannot be measured in specific units but can be qualified or described in terms of high, medium and low impacts. Qualitative and quantitative methods can be used to measure the impact of a threat occurring.

7. **Determine the Level of Risk.** The purpose of this step is to assess the level of risk to the IT system. The determination of risk takes into account the information gathered and determinations made during the previous steps. The level of risk is determined by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk-level determination may be performed by assigning a risk level based on the average of the assigned likelihood and impact levels. A risk-level matrix, such as the sample depicted in **Table 7**, can be used to assist in determining risk levels.

Table 7. Sample Risk-Level Matrix

Threat Likelihood	Impact		
	Low	**Moderate**	**High**
High – a high probability exists that a threat will trigger or exploit one or more vulnerabilities that may be caused by organizations deficiencies, such as absence, inadequacy or improper configuration of security controls, or due to geographic location (such as, within flood zone).	**Low**	**Moderate**	**High**
Moderate – probability exists that a threat will trigger or exploit one or more vulnerabilities due to the existence of a single organizational deficiency, such as lack of security measures.	**Low**	**Moderate**	**Moderate**
Low – a low probability exists that a threat will trigger or exploit a single vulnerability due to the existence of a single organization deficiency, such as improper configuration of security controls.	**Low**	**Low**	**Low**

8. **Recommend Security Controls.** During this step, security controls that could mitigate the identified risks, as appropriate to the organization's operations, are recommended. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. Security control recommendations provide input to the risk mitigation process during which the recommended security controls are evaluated, prioritized and implemented. It should be noted that not all possible

recommended security controls can be implemented to reduce loss. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis should be conducted for the proposed recommended controls to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition to cost, organizations should consider the operational impact and feasibility of introducing the recommended security controls into the operating environment.

9. **Document the Risk Assessment Results.** Once the risk assessment has been completed (threat sources and vulnerabilities identified, risks assessed and security controls recommended); the results of each step in the risk assessment should be documented. NIST SP 800-30 provides a sample risk assessment report outline that may prove useful to covered Entities.

Risk Assessment Results Affect Risk Management

The results of a risk assessment play a significant role in executing an organization's risk management strategy. In the context of the HIPAA Security Rule, the security control baseline, which consists of the standards and required implementation specifications, should be viewed as the foundation or starting point in the selection of adequate security controls necessary to protect EPHI. In many cases, additional security controls or control enhancements will be needed to protect EPHI or to satisfy the requirements of applicable laws, policies, standards or regulations.

The risk assessment provides important inputs to determine the sufficiency of the security control baseline. The risk assessment results, coupled with the security control baseline, should be used to identify which addressable implementation specifications should be implemented to adequately mitigate identified risks (see Health Care Providers for available tools provided through HHS).

Civil and Criminal Penalties (Security HITECH)

CATEGORIES OF VIOLATIONS AND
RESPECTIVE PENALTY AMOUNTS AVAILABLE (as of 2013)

Violation Category—Section 1176(a)(1) Each Violation

All such violations of an identical provision in a calendar year.

- **Tier A** is for violations in which the offender didn't realize he or she violated the Act and would have handled the matter differently if he or she had. This results in a $100 fine for each violation, and the total imposed for such violations cannot exceed $25,000 for the calendar year.
- **Tier B** is for violations due to reasonable cause, but not "willful neglect". The result is a $1,000 fine for each violation, and the fines cannot exceed $100,000 for the calendar year.
- **Tier C** is for violations due to willful neglect that the organization ultimately corrected. The result is a $10,000 fine for each violation, and the fines cannot exceed $250,000 for the calendar year.
- **Tier D** is for violations of willful neglect that the organization did not correct. The result is a $50,000 fine for each violation, and the fines cannot exceed $1,500,000 for the calendar year.

Definitions as used in subpart §160.401

***Reasonable Cause*.** An act or omission in which a covered Entity or Business Associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered Entity or Business Associate did not act with willful neglect.

Reasonable Diligence. The business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

***Willful Neglect*.** Conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

Section 4 – Health Care Providers

The healthcare industry has experienced many changes over the last several years that dramatically increased security requirements as new technology has been adopted. With new technology come additional administrative responsibilities for Health Care Providers.

HIPAA covers a number of important health care industries' administrative requirements with Electronic Transactions and other related areas that may be referred in other sections of this manual including definitions.

There are four parts of HIPAA's Administrative Simplifications:

- Electronic transactions and code sets standards requirements
- Privacy requirements
- Security requirements
- National identifier requirements

HIPAA Administration in healthcare is designed to promote uniformity by adopting transaction standards for a specific purpose for several types of electronic health information transactions, processing of claims and payments and other related functions.

Electronic Transactions and Code Set Requirements
Transactions are activities involving the transfer of health care information for a specific purpose. Healthcare providers engaging in one of the identifiable transaction must comply with the standards of that transaction.

Privacy Requirements
The privacy requirements govern disclosure of patient protected health information (PHI), while protecting patient's rights.

Security Requirements
The security regulation adopting administrative, technical and physical safeguards required to prevent unauthorized access to protected health care information.

National Identifier Requirements
HIPAA requires health care providers, health care plans and employers have standard national numbers that identifies them on standard transactions.

Transactions include the following types of information transmissions:

- Health care claims or equivalent encounter information.
- Health care payments and remittance advice.
- Coordination of benefits.
- Health care claims status.
- Enrollment and disenrollment in a health care plan.
- Eligibility for a health care plan.
- Health plan premium payments.
- Referral certification and authorization.

- First report of injury.
- Health claims attachments.
- Health care electronic funds transfers (EFT) and remittance advice.
- Other transactions that the Secretary may prescribe by regulations.

Preemption of State Law § 160.201 Statutory Basis
The provisions of this subpart implement section 1178 of the Act, section 262 of Public Law 104-191, section 264(c) of Public Law 104-191, and section 13421(a) of Public Law 111-5.
[78 FR 5689, Jan. 25, 2013]

§160.202 Definitions.
For purposes of this subpart, the following terms have the following meanings:

Contrary, when used to compare a provision of state law to a standard, requirement, or implementation specification adopted under this subchapter, means: (1) A covered Entity or Business Associate would find it impossible to comply with both the state and federal requirements; or (2) The provision of state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104-191, or sections 13400-13424 of Public Law 111-5, as applicable.

More Stringent means, in the context of a comparison of a provision of state law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a state law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:

(i) Required by the Secretary in connection with determining whether a covered Entity or Business Associate is in compliance with this subchapter; or (ii) To the individual who is the subject of the individually identifiable health information.

(2) With respect to the rights of an individual, who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable.

(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

Relates to the privacy of individually identifiable health information means, with respect to a state law, that the state law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

State Law means a constitution, statute, regulation, rule, common law, or other state action having the force and effect of law.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 74 FR 42767, Aug. 24, 2009; 78 FR 5689, Jan. 25, 2013]

Duration of Effectiveness of Exceptions Determinations § 160.205

An exception granted under will remain in effect until:

a. Either the state law or the federal standards, requirement or implementation specification that provide the basis for the exceptions is materially changed such that the ground for the exceptions no longer exists; or
b. The Secretary revokes the exception based on a determination that the ground supporting the need for the exception no longer exists.

Principles for Achieving Compliance §160.304

a. *Cooperation.* The Secretary will, to the extent practicable and consistent with the provisions of this subpart, seek the cooperation of covered Entities and Business Associates in obtaining compliance with the applicable administrative simplification provisions.
b. *Assistance.* The Secretary may provide technical assistance to covered Entities and Business Associates to help them comply voluntarily with the applicable administrative simplification provisions. [78 FR 5690, Jan. 25, 2013]

Security Standard
Covered Entities need to identify someone as a privacy officer. This person is responsible to make sure that the organization complies with HIPAA standards. The privacy officer may ask healthcare workforce to:

- **Take an inventory of medical information.** Organizations need to identify all ways they communicate patient information, including faxes, medical records and lab slips. Healthcare workers should know where information is kept and where it is going, making sure that all these transmissions are secure.
- **Respect the privacy reminders posted in public areas.** Many healthcare facilities post signs in corridors and elevators, reminding workforce to maintain patient confidentiality.
- **Participate in HIPAA training.** All healthcare workforce members are to attend HIPAA training sessions.

Risk Assessment

HIPAA requires organizations that handle PHI to regularly review the administrative, physical and technical safeguards they have in place to protect the security of the information. By conducting these risk assessments,

health care providers can uncover potential weaknesses in their security policies, processes and systems. Risk assessments also help providers address vulnerabilities, potentially preventing health data breaches or other adverse security events. A vigorous risk assessment process supports improved security of patient health data.

Conducting a security risk assessment is a key requirement of the HIPAA Security Rule and a core requirement for providers seeking payment through the Medicare and Medicaid EHR Incentive Program, commonly known as the Meaningful Use Program.

The national coordinator for health information technology provides health care providers access to security assessment tools. "The SRA tool and its additional resources have been designed to help health care providers conduct a risk assessment to support better security for patient health data."

The SRA tool's website is found on **www.healthit.gov/providers-professionals/security-risk-assessment.**

Section 5 - Key Definitions - Glossary

Key Definitions – Glossary

Catch-All Definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

***Amendment*.** The parties agree to take such action as is necessary to amend the Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

Authorization. A detailed written form signed by the individual to whom PHI pertains, specifying what PHI may be used or disclosed, by whom and to whom, for what purpose(s) and for what time period.

Breach. The acquisition, access, use or disclosure of PHI in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

Business Associate (BA). Entities that perform functions or activities on behalf of Covered Entities (CEs) provide services to CEs that involve the creation, use or disclosure of PHI, or receive PHI from a CE. BAs do not include members of a CE's workforce who provide services involving PHI. Examples of Business Associates include third-party administrators (TPAs), brokers, consultants, utilization review Entities, attorneys, auditors, pharmacy, benefit managers (PBMs) COBRA administrators or Health FSA administrators.

A Business (i) On behalf of such covered Entity or of an organized health care arrangement (as defined in section 160.103) in which the covered Entity participates, but other than in the capacity of a member of the workforce of such covered Entity or arrangement, creates, receives, maintains, or transmits PHI for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or (ii) Provides, other than in the capacity of a member of the workforce of such covered Entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered Entity, or to or for an organized health care arrangement in which the covered Entity participates, where the provision of the service involves the disclosure of protected health information from such covered Entity or arrangement, or from another Business Associate of such covered Entity or arrangement, to the person, except as provided under 45 CFR 160.103 (4).

***Business Associate Agreement (BAA).*"**Business Associate" shall generally have the same meaning as the term "Business Associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean the contract between a Covered Entities and Business Associate (including sub-contractors).

Covered Entities (CEs). "Covered Entity" shall generally have the same meaning as the term "Covered Entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean covered Entity.
There are three categories of covered Entities: health plans (fully insured and self-insured plans); health care providers who transmit specified health information ("standard transactions") in electronic form, and health care clearinghouses.

Designated Record Set (DRS). A group of records maintained by or for Janus Youth Program or its Business Associates. For a health plan sponsored and funded by Janus Youth Program, the DRS includes enrollment, payment, claims adjudications and case or medical management record systems.

Disclosure. The release, transfer, provision of access to or divulging in any manner of information outside the Entity holding the information.

Electronic Media. (1) Electronic storage material on which data is or may be recorded electronically. Including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; (2) Transmission media used to exchange information already in electronic storage media. Transmission media includes, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via fax, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Employment Records. Not specifically defined in the regulations. Medical information needed for an employer to carry out its obligations under FMLA, ADA and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance and fitness-for-duty test of workforce.

Group Health Plan (also see definition of *health plan* in this section) means a workforce welfare benefit plan (as defined in section 3(1) of the Workforce Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to workforce or their dependents directly or through health plan, reimbursement or otherwise.

Health Care Provider. Any person or Entity that furnishes bills or is paid for health care in the normal course of business.

Health Information. Any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university or health care clearinghouse; and (2) Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual.

Health Plan. An individual plan or group health plan that provides, or pays the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)). The HIPAA regulations specifically include group health plans under ERISA (but not those that have fewer than 50 Health plan members and are self-administered), health insurance issuers, health maintenance organizations (HMOs), Medicare Parts A or B, Medicaid, Medicare supplement policies, long-term care policies, multiple employer welfare arrangements (MEWAs), health care programs for active military persons or for veterans, CHAMPUS, the Indian Health Service program, the Federal Workforce Health Plan Program, approved state child health care plans (SCHIP), Medicare Plus Choice plans. The term “health plan” does not include life insurance, disability plans, workers’ compensation plans, automobile insurance, property and casualty insurers and certain forms of limited benefits coverage (even if such arrangements do actually provide for health care services).

***Health Care Clearinghouse*.** A public or private Entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions: (1) 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. (2) 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.

HIPAA Rules. HIPAA Rules shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Individually Identifiable Health Information*.* Information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Interpretation. Any ambiguity in the Agreement shall be interpreted to permit compliance with the HIPAA Rules.

Limited Data Set (LDS). Health information from which specified direct identifiers have been removed. LDS is between PHI and de-identified information. LDS may be used or disclosed for research, public health or health care operations purposes, but only if a data use agreement has been signed between the CE and the recipient of the LDS.

***Minimum Necessary*.** The minimum necessary PHI required to accomplish the intended purpose.

Modifications. **Compliance dates for implementation of new or modified standards and implementation specifications.** Except as otherwise provided, with respect to rules that adopt new standards and implementation specifications or modifications to standards and implementation specifications in this subchapter in accordance with §160.104 that become effective after January 25, 2013, covered Entities and Business Associates must comply with the applicable new standards and implementation specifications, or modifications to standards and implementation specifications, no later than 180 days from the effective date of any such standards or implementation specifications as required under Section §160.105.

Health Plan Member. The person with respect to whom PHI is maintained. If the family members of a Janus Youth Program workforce member benefit under a Janus Youth Program health plan, each family member is a separate Health plan member under the Health Plan.

Personal Representative. Any person authorized under applicable law to act on behalf of the Individual patient with respect to the individual patient's health care. For example, a Personal Representative may include the parent or guardian of a minor patient (unless the minor has the authority under state law to act on his or her own behalf), the guardian or conservator of an adult patient or the personal representative of a deceased patient.

Protected Health Information (PHI). Any individually identifiable health information that is communicated, stored or transmitted in any form (i.e., electronically, printed, or orally) by a CE. Health information relates to past, present or future physical or mental health condition, or provision of or payment for health care. It is

"individually identifiable" if it identifies the individual or if it is reasonable to believe that the individual could be identified based on the information provided.

Regulatory References. A reference in the Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

Standard. A rule, condition or requirement: (1) Describing the following information for products, systems, services or practices: (i) Classification of components; (ii) Specification of materials, performance or operations; or (iii) Delineation of procedures; or (2) With respect to the privacy of protected health information.

Standard Setting Organization **(SSO).** An organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

Subcontractor. A person to whom a Business Associate delegates a function, activity or service other than in the capacity of a member of the workforce of such Business Associate.

Trading Partner Agreement. An agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement.

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

Treatment, Payment or Health Care Operations (TPO). Treatment is the provision, coordination or management of health care by one or more providers of care to a patient. Payment is activities to obtain payment for health care services or activities to determine or fulfill responsibility to pay for health care services or for premiums for coverage. Payment includes subrogation, billing, claims management, collection and collecting payment from stop-loss carriers. Health care operations are services and activities necessary to the CE's performance of its activities with respect to treatment or payment. Insurance-related activities that are included as "health care operations" include "underwriting, premium rating and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of section 164.514(g) are met, if applicable".

Use. 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.

Workforce. 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 covered Entity or Business Associate, whether or not they are paid by the covered Entity or Business Associate.

SOME HIPAA ACRONYMS:

BA - Business Associate
BAA - Business Associate Agreement
CE - Covered Entity
DRS - Designated Record Set
GHP - Group Health Plan
HCO - Health Care Operations
HIPAA - Health Insurance Portability and Accountability Act
LDS - Limited Date Set
PHI - Protected Health Information
TPO - Treatment, Payment, or Health Care Operations

Section 6 - Appendix

Classes of Workforce "Employee" and Approved Uses

Forms Addendum

- Request for Access to DRS
- Letter of Extension for Request to Access DRS
- Response to Request to Access DRS
- Review of Request to Access DRS
- Request to Amend PHI
- Letter of Extension for Amendment to PHI
- Response to Request to Amend PHI
- Request for Accounting of Disclosures of PHI
- PHI Disclosure Log

Classes of Workforce Member "Employee" and Approved Uses

Classes of Workforce "Employee"	*Type of Protected Health Information*	*Conditions for Access to Information*
Financial Workforce	Limited Record, where necessary, to complete assignment.	For oversight of reimbursement, payment and financial services.
Operations and Administration Workforce (Assistant Financial Manager, Financial Manager, Executive Director)	Entire file, where necessary, to complete assignment.	▪ For enrollment, eligibility, income and insurance verification. ▪ For oversight of reimbursement, payment and financial services. ▪ Decisions for plan design/renewal.
Leadership & Management	Limited record, where necessary, to complete assignment.	Operation and management, executive decisions for health care operations.
Administrative Support (administrative assistants)	Limited record, where necessary, to complete assignment.	Administrative Support
IT (those responsible for system backup, software or hardware upgrades)	Entire electronic record, where necessary, to complete assignment.	Computer Systems Maintenance and Support

Note: Protected Health Information (PHI) access will be limited based on workforce member's job responsibilities and subject to change as business needs dictate.

Forms Addendum