VONTIER EMPLOYMENT SERVICES, LLC
HIPAA PRIVACY POLICY AND PROCEDURE MANUAL

Vontier Employment Services, LLC
HIPAA Privacy Policy and Procedures Manual (2/2024)

Company Name:	**Vontier Employment Services, LLC, its Parent Companies, Subsidiaries, Affiliates and OpCos as listed in Appendix 1 and only governed by HIPAA per the Vontier Sponsored Health Plan, hereinafter collectively "Covered Hybrid Organization" or "Hybrid Org"**
Policy Name:	HIPAA Privacy Policy
Policy Version:	Version 1.2
Effective Date:	2/12/2024
Privacy Official:	**Srikant Mikkilineni**
Security Official:	**Pablo DeLaRosa**
Responsible for Review:	**Srikant Mikkilineni, Privacy Official** **Pablo DeLaRosa, Security Official**

Table of Contents

Introduction to the HIPAA Privacy Policy and Procedures Manual

This HIPAA Privacy Policy and Procedure Manual sets forth the privacy policies and procedures applicable to the employee benefit programs sponsored by Vontier Employment Services, LLC and available to eligible employees and dependents of Vontier, its parent companies, subsidiaries, affiliates, and OpCos ("Covered Hybrid Organization", hereinafter "Hybrid Org") through the Vontier Health and Welfare Benefits Plan dated October 9, 2020 (the "Plan"). The Plan contains health care components, as described in **Appendix 2**, and non-health care components. Reference to the Plan in these Policies and Procedures shall mean only the health care components of the Plan. As the sponsor of the Plan, Vontier maintains its commitment to safeguard and keep confidential the Protected Health Information ("PHI") and Electronic Protected Information ("ePHI") of its employees and their families.

The purpose of this Policy Manual is to comply with the regulations issued by the Department of Health and Human Services ("HHS") under HIPAA, subsequent federal laws such as HITECH, and clarifying regulations. If any provision of this Policy is inconsistent with HIPAA or a more restrictive applicable state privacy law (to the extent not preempted), this Policy will be interpreted to comply with such law. This policy may be amended from time to time, and you can find the most recent version on the Vontier Benefits SharePoint page or by contacting your local People and Culture Benefits contact.

Vontier is considered a "hybrid entity", as it has health care components through its benefits program, but it is not in the healthcare business. As such, Vontier has designated only the health care components of the Plan as a "covered entity" subject to HIPAA. HIPAA requirements generally cover the protection of and access to an individual's health information and the personal information (e.g., name, date of birth, address, email) used to identify them.

This Policy does not apply to health insurance issuers or health maintenance organizations that provide benefits under the Health Plan because, as Covered Entities, such health insurance issuers and health maintenance organizations must have their own privacy policies and procedures. To learn more about each entities' Privacy Policy, please reference Appendix 2 for contact information on each provider. Health information provided to a Vontier employee by or on behalf of another employee in connection with verifying the latter's absence from employment, request for reasonable accommodation of a disability, or other employment-related purpose, is not subject to this Policy.

It is the intent of this Policy Manual, along with our other Policy manuals and stand-alone policies, to reflect the Hybrid Org's responsibilities in ensuring the privacy, integrity, and security of the personal health information ("PHI") and electronic personal health information ("ePHI") we use, transmit, create, and maintain. This Policy also covers individuals' rights to access, share, and amend their PHI and to be notified if their PHI is shared or accessed when it should not have been.

This Policy should be read in conjunction with the Vontier Employee Handbook for US Employees, the Vontier Code of Conduct, and the Vontier Information Security Policies and Guidelines. In instances of conflict between this Policy and the aforementioned policies, this Policy will take precedence regarding compliance with HIPAA privacy requirements. If you would like to review these documents, please visit the Vontier SharePoint site or contact your supervisor.

Consistent with the requirements of the Privacy Rule of HIPAA, any PHI received or created by or on behalf of the Plan may be used or disclosed solely in accordance with this Policy. Each Vontier employee who performs or may perform activities involving PHI or ePHI, hereinafter referred to as

a Responsible Employee, is bound by this Policy. See **Appendix 3** for the List of Responsible Employees. As a Responsible Employee, you agree to only use or share PHI when required to perform your job duties. You agree to read and understand the Synopsis of all the Policies, as well as the full content of any that apply directly to your role. You agree to read, understand, and abide by these policies and execute an attestation.

This Manual also covers the requirements for identifying and reporting incidences of potential improper use or disclosure of PHI. It discusses Hybrid Org's responsibilities for assessing incidents and giving appropriate notice if an incident is determined to be a breach of the Privacy Rule. The table of contents, synopses, or any search feature on your browser should help you find information to address most situations regarding the privacy of PHI. Always contact the Privacy Official or your supervisor for assistance if you are unsure how to proceed. Hybrid Org appreciates your efforts and contributions in meeting the requirements that apply to protected health information that has been entrusted to us.

HIPAA Confidentiality Agreement

As a Responsible Employee or contractor of Hybrid Org, I understand that Hybrid Org is subject to HIPAA regulations as described in this Manual. As such, Hybrid Org has a legal responsibility to protect the privacy and security of individual Protected Health Information ("PHI") and Electronic Protected Health Information ("ePHI").

During my employment with the Hybrid Org, I may create, see, hear, or touch PHI, ePHI, and other information that the Hybrid Org must maintain as confidential. By reading and understanding this Confidentiality Agreement, I acknowledge and understand that:

- I will not use or disclose PHI or ePHI, except when necessary to perform my job.
- With respect to other types of confidential information, I will only access, use, or disclose such information if it is required for the performance of my job.
- I will keep all security codes and passwords used to access any Hybrid Org facilities, equipment, or computer systems confidential at all times.
- When my employment with the Hybrid Org is terminated or completed, I will immediately return all property (physical, electronic, or other) to the Hybrid Org and shall not make any attempts to access Hybrid Org files which may contain PHI or ePHI.
- Even after my employment is concluded, I agree to meet the use, disclosure, and confidentiality obligations under this Confidentiality Agreement.

By reading and understanding this Confidentiality Agreement, I am confirming that I am bound by its terms, and that I will perform my duties in accordance with those terms. I understand that if I violate or fail to follow the terms of this Confidentiality Agreement, I am subject to disciplinary action, including but not limited to termination of my employment and may be subject to civil or criminal penalties.

Privacy Manual Synopsis

This section is for all Responsible Employees to review and attest. A Responsible Employee is an employee or contractor of **HYBRID ORG** who may access PHI/ePHI, or who supports others who access PHI/ePHI as part of his/her job responsibilities (see Glossary for more details). Below is a summary of each policy, including the relevant HIPAA regulations.

If a particular policy applies to your role or position, you must read the entire policy, not just the synopsis. To view the full policy, please click on the title of that section in the synopsis. Definitions for the terms used in this Manual are included in the Glossary at the end of the manual and defined terms are *italicized.*

Privacy Policy 1.0 HIPAA Privacy Program: General

HYBRID ORG centralizes its Plan operations internally within the Vontier Benefits Department. As a result, HYBRID ORG has limited the number of employees who have access to PHI or ePHI on a daily basis. Additionally, HYBRID ORG utilizes the services of **bswift** as the Plan Administrator and numerous healthcare vendors, as described in Appendix 2. The healthcare vendors provide HYBRID ORG with secure portals for communication regarding ePHI, and the vast majority of communications are through these portals. HYBRID ORG has also contracted with **Kiteworks** and the **Compliancy Group ("The Guard")** for software solutions. Kiteworks is a solution which provides end-to-end encryption for transmissions which may contain ePHI, such as emails. The Compliancy Group's product, "The Guard", is a HIPAA compliance management product which provides HYBRID ORG with tools to meets its regulatory obligations. As a Responsible Employee, you will be issued a Kiteworks license and an account with "The Guard." You will be trained on common forms of PHI, the use of Kiteworks and the Guard, and specific examples of how you may encounter and deal with PHI as part of your job.

Hybrid Org's Information Security measures are detailed in the Security Manual, which you will also review and sign.

Assigned Privacy Responsibility:
HYBRID ORG has appointed an official who has final responsibility for privacy governance. He is the HIPAA Privacy Official, and his name, title, and contact information are:

The Privacy Official's name is Srikant Mikkilineni.
The Privacy Official's title is Senior Counsel, Global Privacy and Data Protection.
The Privacy Official's contact information is HIPAAinquiry@vontier.com.

The *Privacy Official* (a) oversees **Hybrid Org's** efforts to secure and maintain the confidentiality and integrity of protected health information (*PHI*); (b) maintains sensitive Hybrid Org information; (c) prevents and detects inappropriate and illegal uses and disclosures of *PHI*; and (d) assures *individuals'* rights with regard to accessing, *amend*ing and accounting for use and disclosure of *PHI*.

Responsible Employees must be familiar with their responsibility to maintain the confidentiality and integrity of *PHI* and to disclose and use it only as allowed or required. *Responsible Employees* must contact the *Privacy Official* when this Policy requires that they do so.

45 CFR Part 164 Subpart E
45 CFR 164.530 HIPAA Privacy Program Administrative Requirements

Privacy Policy 2.0 Administrative, Technical and Physical Safeguards of PHI

Hybrid Org must safeguard and protect the privacy of *PHI* by instituting physical, administrative and technical safeguards. *Responsible Employees* must understand what safeguards are in place and abide by them to assure that *PHI* remains private and is only shared as is allowed under the Privacy Rule. Some examples of safeguards include locked doors to Hybrid Org facilities and home offices; policies and procedures; training; complaint resolution; incident reporting; and sanctions for violations of policies and procedures. *Responsible Employees* should refer to the Security Policy and Procedure Manual for specifics on Hybrid Org's safeguards for electronic *PHI* and equipment and the use of Kiteworks technology for transmitting ePHI.

45 CFR 164.528(c): *Accounting of Disclosures of Protected Health Information: Safeguards*

Privacy Policy 3.0 Minimum Necessary Standard

Under the *minimum necessary standard*, **Hybrid Org** may generally only use, request, or disclose *PHI* that is necessary to fulfill a request, or perform a job function. *Responsible Employees* are trained on this standard so that *PHI* is used, requested, or disclosed only to the extent that is legally required. Examples of the Minimum Necessary Standard are included in the Vontier HIPAA Training Guide, incorporated by reference. Visit the Vontier Benefits SharePoint site for the most recent version.

45 CFR 164.502(b)(1) *Minimum Necessary Standard*
45 CFR 164.514(d)(3) *Minimum Necessary Disclosures of Protected Health Information*
45 CFR 164.524(a) *Access to Protected Health Information*

Privacy Policy 4.0 Verification of Identity and Authority

Before Hybrid Org discloses *PHI* to an *individual* or another organization requesting it, Hybrid Org verifies the identity of the *individual* or other organization and their authority where required. The full policy outlines the requirements for identity and authority verification.

45 CFR 164.514(h)(1) *Standard Verification Requirements*

Privacy Policy 5.0 Complaints to the Hybrid Org

Hybrid Org has a complaint process, under which *individual*s may make complaints about Hybrid Org's compliance with the *HIPAA* Privacy Rule, the *HIPAA Breach* Notification Rule, and Hybrid Org's policies and procedures related to these rules. Hybrid Org has designated the *Privacy Official* as the person responsible for receiving these complaints. Any such complaints received by others, in whatever form, should be directed to the *Privacy Official*'s attention as soon as possible at HIPAAinquiry@vontier.com. The *Privacy Official*, or his/her designee, will review complaints, document them, and respond to them. Any complaint that is received that is also a Security Incident will be handled according to the process set forth in Privacy Policy 6: *HIPAA Incident Response and Reporting and Breach Determination*. Hybrid Org also acts to prevent anyone from intimidating, threatening, coercing, discriminating against, or retaliating against any *individual* who has exercised their right under *HIPAA* to file a complaint with the Hybrid Org concerning *HIPAA* compliance.

45 CFR 164.530(a)(d) and (g)*Administrative Requirements: Personnel Designations, Complaints and Refraining from Intimidating or Retaliatory Acts*
45 CFR 164.524(d) *Individual Right: Right to file Complaint Concerning Denial of Access*
45 CFR 164.520(b)(1)(vi) *Notice of Privacy Practice: Complaints*

Privacy Policy 6.0 HIPAA Incident Response and Reporting and Breach Determination

Hybrid Org has legal responsibilities to protect *PHI* under *HIPAA*, to identify and respond to suspected incidents, mitigate harm, require its *Responsible Employees* to report incidents, and to determine when there is a reportable *breach* of an *individual*'s *PHI*. Hybrid Org reviews all reported incidents and follows the InfoSec and IT internal procedures to determine if there has been a *Breach* (an acquisition, *access*, use, or disclosure of an Individuals *unsecured PHI* in a manner not permitted under *HIPAA*), as described in detail in the HIPAA Security Manual.

This policy establishes guidelines for Hybrid Org to:

- Require the reporting of suspected privacy and *security incident*s (any attempted or successful unpermitted or unauthorized *access*, use, disclosure, modification, interference or destruction of *unsecured PHI* in any form).

- Identify and respond to suspected or known incidents involving the security or privacy of protected health information, including mitigating any harmful effects. Any complaint that is filed with the Hybrid Org that is potentially a privacy or *security incident* will be handled under this Policy, which also appears in the Security manual, instead of Privacy Policy 5.0: *Complaints to the Hybrid Org*.

- Follow the *Breach* Notification Policy, Privacy Policy 7, whenever it determines that a *Breach* has occurred.

To report a security concern, you can report through the Guard by logging into your account and following the prompts or by submitting the "Reporting a Security Concern Form" available at Reporting a Security Concern (sharepoint.com). You can also reach out to Vontier Information Security at 1-800-999-4446 or contact the Security Official. DO NOT INCLUDE ANY MEDICAL OR MEDICAL RELATED INFORMATION. Once you have submitted your security concern, the Information Security team will be notified. The information provided will be assessed and a member of the team will contact you. If required, a call will be set up, inviting all relevant team members to discuss the situation and a decision will be made on how to proceed to appropriately manage the incident response.

45 CFR 164.308(a)(6)(i) *Security Incident Procedures*
45 CFR 164.308(a)(6)(ii) *Implementation Specification: Response and Reporting (Required)*
45 CFR 164.530(a)(c)(e)(f) *Administrative Requirements: Personnel Designations, Safeguards, Sanctions and Documentation, Mitigation*
45 CFR 402 *Definitions: Breach*

Privacy Policy 7.0 Breach Notification

Hybrid Org has legal responsibilities to protect *PHI* under *HIPAA*, to determine when there is a reportable *breach* of an *individual*'s *PHI*, and to make appropriate and timely notifications following a *breach*. This *Breach* Notification Policy establishes guidelines for Hybrid Org to:

- Make, or assure the appropriate *Covered Entity* or *Business Associate* makes, appropriate notifications to *individual*s impacted by a *Breach*;

- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to federal and state authorities if required by the details of the *Breach* determination;

- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to the media if the findings of the *Breach* determination require them;

- Determine when and if appropriate substitute notice is allowed and to use that substitute notice when appropriate; and

- Document compliance with the requirements of *Breach* notifications.

45 CFR 164.404 *Notification to Individuals*
45 CFR 164.406 *Notification to the Media*
45 CFR 164.408 *Notification to the Secretary*
45 CFR 164.410 *Notification by a Business Associate*
45 CFR 164.412 *Law Enforcement Delay*
45 CFR 164.414 *Administrative Requirements and Burden of Proof*
45 CFR 164.530 *Administrative Requirements*

Privacy Policy 8.0 Sanctions/Discipline

Responsible Employees who violate Hybrid Org's privacy policy and procedures may be subject to sanctions. Sanctions are disciplinary measures intended to address violations and to deter future violations. Hybrid Org, in deciding upon the appropriate sanction, reviews the severity of the violation, the impact of the violation, and the *Responsible Employee's* work history. Hybrid Org's policy for discipline is contained in the Vontier Employee Handbook for US Employees. If you need another copy, reach out to your supervisor.

45 CFR 164.530(e) *Sanctions*

Privacy Policy 9.0 Business Associates

Hybrid Org relies on *business associates*, which are vendors that handle *PHI* (create, receive, maintain, or transmit) on behalf of or for the benefit of Hybrid Org to carry out Hybrid Org's *HIPAA* functions. This policy covers how the Hybrid Org determines who is a *business associate*. The policy then covers the details and requirements of the *business associate* contract the Hybrid Org and a *business associate* must enter into to protect the privacy of health information, requirements for reporting incidents and *breach*es, what to do when those contracts end, as well as the Hybrid Org's due diligence to assure vendors properly handle *PHI* and train their *Responsible Employees*. Examples of Business Associates are bswift, United Healthcare and Cigna Dental.

45 CFR 160.103 *Business Associate Definition*
45 CFR 164.502(3)-(4) *Permitted and Required Uses and Disclosures; Business Associates*
45 CFR 164.504(e) *Standard Business Associate Contracts*

Privacy Policy 10.0 Notice of Privacy Practices

Hybrid Org provides individuals with its Notice of Privacy Practices. This Notice, which is incorporated herein by reference, describes how individual *PHI* is to be used and disclosed. The current version of the Notice is available on the Vontier Benefits SharePoint and the Vontier Privacy SharePoint. *Responsible Employees* should be familiar with the contents of this Notice.

45 CFR 164.520 *Notice of Privacy Practices for protected health information*

Privacy Policy 11.0 Use and Disclosure of PHI: General Rules

In general, *covered entities* and *business associates* may not use or disclose protected health information, except when the Privacy Rule specifically permits or requires such use or disclosure. This policy and the ones immediately following it describe when the Privacy Rule permits and requires use or disclosure of protected health information, documentation related to different required or permitted uses and disclosures, and other details related to each circumstance. If a *Responsible Employee* is unsure whether to allow or deny a use or disclosure that is related to their job responsibilities, they should contact the *Privacy Official* for clarification before acting.

45 CFR 164.502 *Uses and Disclosures of Protected Health Information: General Rules*
45 CFR 164.501 *Definitions*
45 CFR 160.203 *General Rule and exceptions*

Privacy Policy 12.0 Uses and Disclosures: *Individual* Opportunity to Agree or Object Required

Under some circumstances, Hybrid Org must provide an *individual* the opportunity to agree or object to disclosure of *PHI*. Hybrid Org affords *individuals* the opportunity to agree or object to a use or disclosure in the following circumstances:

1. disclosure of *PHI* to a person that is directly relevant to that person's involvement with an *individual*'s care including *payment* for that care,
2. limited disclosure for notification of an *individual*'s location, general condition, or death,
3. limited uses and disclosures for disaster relief purposes, and
4. uses and disclosures when an *individual* is deceased (prior prohibition on disclosures must be honored).

This policy covers how Hybrid Org provides such an opportunity and honors an *individual*'s choices. *Responsible Employees* only use or disclosure information in the above listed circumstances as described in this policy. *Responsible Employees* afford *individuals* an opportunity to agree or object to such uses and reflect any oral agreements or objections in the *individual*'s record. Other requirements may override an *individual*'s right, for example a response to a judicial or administrative order. If a *Responsible Employee* is not sure how to proceed, they should consult the *Privacy Official.*

45 CFR 164.510 *Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object*

Privacy Policy 13.0 Uses and Disclosures: Authorization Required and Requirements for a Valid Authorization

Hybrid Org obtains and requires valid written *individual* authorizations before it uses or discloses information in the circumstances described in this policy and as required under the Privacy Rule. Generally, Hybrid Org may not use or disclose *PHI* without a valid written authorization from the *individual* who is the subject of the information, unless otherwise allowed under the Privacy Rule. When the *individual* provides a valid authorization, Hybrid Org's use and disclosure of the information must be consistent with the authorization. *Responsible Employees* must be familiar with the requirements of a valid authorization and the situations which require that authorization be obtained prior to use or disclosure of information and must follow the terms of the authorizations

that are in place. See Privacy Policy 14: *Use and Disclosure: No Authorization or Right to Agree or Object* for more detail on situations in which an authorization is not required.

Hybrid Org allows revocation of authorizations in writing with some minor exceptions as further detailed below. Hybrid Org provides *individual*s with a copy of their authorizations. Hybrid Org uses and accepts only valid authorization forms written in plain language which contain all the core elements and required statements for an authorization and limits the use of compound authorizations to circumstances where they are allowed as detailed in the full policy. The Hybrid Org also documents and retains any signed authorizations.

Hybrid Org does not condition the provision of *treatment*, *payment*, enrollment in a health plan, or eligibility for benefits on the provision of an *individual*'s authorization except in limited circumstances as allowed under the Privacy Rule and further described in the policy. Hybrid Org meets the requirements for authorizations related to communications for marketing purposes.

45 CFR 164.508 *Uses and Disclosures for Which an Authorization is Required*
45 CFR 501 *Definitions*

Privacy Policy 14.0 Uses and Disclosures: No Authorization or Opportunity to Agree or Object Required

Under certain circumstances, Hybrid Org may use and disclose *PHI* when neither authorization nor an opportunity for an *individual* to agree or object is required. This policy informs *Responsible Employees* of what those circumstances are, and what steps *Responsible Employees* must take to fulfill requests for *PHI* when no authorization or opportunity for an *individual* to agree or object is required. Generally, written authorization or an opportunity to agree or object are not required when a use or disclosure is for *treatment*, *payment*, or healthcare operations purposes. In addition, written authorization or an opportunity to agree or object are generally not needed when a law *requires* that Hybrid Org use or disclose certain *PHI*. There are a few additional special circumstances that allow disclosure like for use by a *whistleblower*, the victim of a crime while at work at the Hybrid Org, and for Military and Veteran Activities.

Each *Responsible Employee* should be familiar with what activities are included in *treatment*, *payment* and *health care operations* under the Privacy Rule. Frequently referred to as TPO, it is very important to understand the scope of what is covered because it informs of the day-to-day privacy and information *access* decisions to be made concerning the use and disclosure of *PHI*. If a *Responsible Employee* is unsure of what is included, they should review this policy and seek assistance from the *Privacy Official*.

45 CFR 164.501 *Definitions: Healthcare Operations*
45 CFR 164.512 *Uses and Disclosures for which an Authorization or Opportunity to Agree or Object is Not Required*
45 CFR 164.506 *Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations*

Privacy Policy 15.0 Individual Right: Access to Protected Health Information

Hybrid Org must afford *individual*s the opportunity to *access* and inspect their protected health information maintained in a *designated record set*. This policy covers the requirements for responses to requests for *access*, inspection, and copies of *medical record*s by *individual*s and their *personal representative*s; when such requests can or must be denied; if and how an *individual* can appeal a

denial of *access*; in what format the *individual* may request and receive the records; and what fees may be charged for fulfilling the requests.

45 CFR 164.524 *Access of Individuals to Protected Health Information*

Privacy Policy 16.0 Individual Right: Request Restrictions and Alternate Confidential Communications

When feasible or required, Hybrid Org will honor *individuals'* requests to restrict uses and disclosures of *PHI* that are made to carry out *treatment*, *payment*, or *health care operations*, and that are made to family, friends, or others for involvement in care and notification purposes. Hybrid Org also honors requests made by *individual*s to receive communications of *PHI* by alternative means or at an alternate location when feasible or required. *Responsible Employees* are trained as to how to respond to all such requests. All such requests shall be required to be in writing or reflected in the record in writing at the time of the request. *Responsible Employees* need to be aware how to reflect and find these requests in the *individual*'s records.

45 CFR 164.502(c) *Uses and Disclosures of PHI Subject to an Agreed Upon Restriction*
45 CFR 164.502(h) *Confidential Communications*
45 CFR 164.522 *Rights to Request Privacy Protection for Protected Health Information*

Privacy Policy 17.0 Individual Right: Request Amendment of Designated Record Set

*Individual*s have the right to request *amendment* to certain protected health information in the *designated record set* of their *medical record*s. *Amendment* can consist of adding *PHI* to an existing record, or supplementing a record by, for example, submitting a second opinion. Hybrid Org promptly responds to requests to *amend PHI* and promptly informs *individual*s as to whether their request is granted or denied. Contact your *Privacy Official* if you receive a request for an *amendment* to *PHI* or notification from another *covered entity* of an *amendment* to *PHI* in Hybrid Org's records.

45 CFR 164.528 *Accounting of Disclosures of Protected Health Information*

Privacy Policy 18.0 Individual Right: Accounting of Disclosures

*Individual*s may have the right to receive an accounting of disclosures of their protected health information that have been made by Hybrid Org to another entity, including disclosures to or by *business associates*. Several categories of uses and disclosures are excluded from accountings such as those requested by the *individual* themselves or those made to other entities and persons for *treatment* purposes. *Individual*s can submit a request for an accounting to Hybrid Org at HIPAAinquiry@vontier.com or through US mail to the address indicated on the Notice of Privacy Practices. Hybrid Org will properly respond to the request and send the accounting when appropriate.

45 CFR 164.528 *Accounting of Disclosures of Protected Health Information*

Privacy Policy 19.0 Uses and Disclosures: Psychotherapy notes

Psychotherapy notes are treated differently from other mental health information both because they contain particularly sensitive information and because they are the personal notes of the therapist that typically are not required or useful for *payment* or *health care operations* purposes, other than by the mental health professional who created the notes. This policy describes how the Hybrid Org

is to respond to requests for *psychotherapy notes*; the distinction between *psychotherapy notes* and other mental health records; the mental health practitioner/individual privilege that applies to *psychotherapy notes*; and the requirement that these notes be separated from the *designated record set* to receive heightened protections. The Policy also describes the processes Hybrid Org follows to assure that it meets all requirements for use and disclosure of *psychotherapy notes* in the limited circumstances where it is allowed.

45 CFR 164.508(a)(2) *Uses and Disclosures for Which an Authorization is Required: Psychotherapy notes*

Privacy Policy: 20.0 Minors' Rights

This policy covers when minors must *access* their *PHI* through a *personal representative*, and when minors may *access* their *PHI* directly. Hybrid Org *Responsible Employees* must be familiar with the circumstances under which minors can *access* their *PHI* without parental, guardian or *personal representative* approval or knowledge. Hybrid Org *Responsible Employees* should also be familiar with the circumstances where parents, guardians and *personal representative*s of minors cannot *access* a minor's record without the minor's approval.

45 CFR 164.502(g) *Personal Representatives, Adults and Emancipated Minors*

Privacy Policy 21.0: Use of Social Media

This policy outlines the safeguards *Responsible Employees* must follow to ensure that their use of social media does not result in unauthorized disclosure of *PHI*. It applies to professional accounts, personal accounts, and all social media platforms (e.g., Facebook, Instagram, Tiktok). *Responsible Employees* using social media must take precautions to ensure *PHI* is not accidentally or intentionally disclosed during such use. This policy describes what precautions must be taken. This Policy should also be read and interpreted in conjunction with the Vontier Social Media Policy. Training on this Social Media Policy is also included in the Harassment Free Workplace video training.

45 CFR 164.530(c) *Privacy Safeguards*

Privacy Policy 22.0: Uses and Disclosures: Response to Judicial and Administrative Proceedings

Hybrid Org must disclose an individual's *PHI* when that *PHI* is properly sought in a judicial or administrative proceeding. Such proceedings include civil and criminal court proceedings, and proceedings before government agencies, such as Professional Licensing Boards, the Department of Health and Human Services ("*HHS*"), and the Centers for Medicare and Medicaid Services. Hybrid Org responds to judicial or administrative orders, as well as subpoenas, discovery requests, or other lawful process, that is not accompanied by an Order of a court or *administrative tribunal*, ONLY if certain criteria are met, including the provision of satisfactory assurances. *Responsible Employees* should always contact the *Privacy Official* if they receive such a request directly.

45 CFR164.512(e) *Use and Disclosure of Protected Health Information for Judicial and Administrative Proceedings*

Privacy Policy 23.0: Uses and Disclosures: Fundraising

Hybrid Org does not currently engage in fundraising for its own purposes. In the event Hybrid Org opts to engage or assist another entity in fundraising, the following Policy applies:

Hybrid Org must permit *individuals* the right to opt out of receiving *fundraising* communications, and to not receive the communications after opting out. Hybrid Org will not share an *individual*'s information for *fundraising* purposes unless its Notice of Privacy Practices contains provisions regarding the Hybrid Org's potential *fundraising* activity, the right to opt out, stop receiving fundraising communications, and to change their mind and ask to receive them again.

45 CFR 164.514(f)(2) *Uses and Disclosures for Fundraising & Implementation Specifications: Fundraising Requirements*
45 CFR 164.501 *Definitions*

Privacy Policy 24.0: Uses and Disclosures: Worker's Compensation

This policy provides rules for Hybrid Org's use or disclosure of *PHI* for worker's compensation, or other similar programs established by law, that provide benefits for work-related injuries or illness without regard to fault. Hybrid Org follows *HHS* guidance for complying with these varied laws in a number of ways including allowing disclosures without an *individual*'s authorization, allowing disclosures with an *individual*'s authorization, and requiring the application of the *minimum necessary standard* for worker's compensation disclosures. This policy describes the circumstances under which such disclosure is required, is allowed and how to make the disclosure.

45 CFR 164.512(l) *Uses and Disclosures for which an Authorization or Opportunity to Agree or Object is Not Required: Worker's Compensation*

Privacy Policy 25.0: Limited Data Set and Data Use Agreements

Hybrid Org may share a *Limited Data Set,* which is a set of *PHI* with certain identifiers removed, to a requesting party who seeks the *PHI* disclosure for purposes of *research*, public health, or healthcare operations. Such disclosure may only be made if the Hybrid Org obtains a signed, written Data Use Agreement (DUA) from the person or entity to whom the *Limited Data Set* is to be disclosed. This policy defines a *limited data set*; sets forth appropriate uses for *limited data sets*; requires that a data use agreement meeting the defined criteria be in place between the parties; requires that the Hybrid Org adhere to applicable data use agreements and monitor the recipient's use of the data set for patterns of activity or practices in violation of the data use agreement, and requires Hybrid Org to end sharing of the data set and report to *HHS* if any violations are not reasonably cured.

45 CFR 164.514(e) *Limited Data Set and Data Use Agreement*

Privacy Policy 26.0: Guidance on Minimum Necessary Standard for Routine Transactions

Hybrid Org provides guidance for Responsible Employees on the minimum necessary standard, that is, what limited PHI a Responsible Employee may share for a given transaction undertaken within the scope of the Responsible Employee's job duties. Examples of the Minimum Necessary Standard are included in the Vontier HIPAA Training Guide, incorporated herein.

Attestation

I hereby attest and acknowledge that I have read and understood the contents of this *HIPAA* Privacy Policy and Procedure Manual. Through my attestation, I hereby confirm that I am bound by Hybrid Org's privacy policies and procedures and will perform my job duties accordingly. I understand that if I violate any Hybrid Org privacy policy or procedure, I may be subject to disciplinary action, up to and including termination of my employment. I may also be subject to civil or criminal penalties. I hereby acknowledge and agree that this attestation is the equivalent of a physical or e-signature.

Privacy Policy 1.0 HIPAA Privacy Program: General

FULL POLICY LANGUAGE:

Policy Purpose:

Hybrid Org complies with its responsibilities to ensure the privacy, integrity, and security of the information we use, transmit, create and maintain as well as the *individual* 's rights for accessing, sharing, *amend*ing and accounting for the use and disclosure of their *PHI* and to be notified when *PHI* is shared or accessed when it should not have been.

Policy Description:

Hybrid Org has appointed a *Privacy Official* who implements and operationalizes policies and procedures, trains its *Responsible Employees*, safeguards protected health information, establishes procedures for the receipt and response to complaints regarding *HIPAA* compliance, establishes disciplinary processes for violations of *HIPAA* requirements, mitigates any harm from improper use or disclosure of protected health information, prohibits retaliation against anyone seeking in good faith to enforce *HIPAA* rights or responsibilities, and appropriately retains *HIPAA* documentation. **Hybrid Org** does not require *individual*s to waive their rights to file a complaint with *HHS* regarding *HIPAA* compliance as a condition of the provision of *treatment*, *payment*, enrollment in a health plan, or eligibility for benefits.

Hybrid Org's *Responsible Employees* must understand the protections to *PHI*'s security and integrity, when and how *individual*s and others can *access* this information, and what to do when they notice it may have been used improperly when working with this protected health information (*PHI*) on the **Hybrid Org's** behalf.

The **Hybrid Org** follows the below procedures.

Procedures:

Designation of Individuals:

1. Hybrid Org has Designated a *Privacy Official*, who is responsible for development and implementation of **Hybrid Org's** policies and procedures, as follows:
   - The Privacy Official's name is Srikant Mikkilineni.
   - The Privacy Official's title is Senior Counsel, Global Privacy and Data Protection.
   - The Privacy Official's contact information is HIPAAinquiry@vontier.com.

2. Hybrid Org has designated a mailing address, phone number, and email address for receiving privacy-related complaints and to provide further information about **Hybrid Org's** Notice of Privacy Practices as follows: Vontier Employment Services, LLC, 5438 Wade Park Blvd., Suite 600, Attn: HIPAA Inquiry/Benefits Department, Raleigh, NC 27607, Phone: (817) 323-1405, email: HIPAA@Vontier.com.

Training:

1. **Hybrid Org** trains all *Responsible Employees* on its Privacy Policies and Procedures, as necessary and appropriate for *Responsible Employees* to carry out their functions within the **Hybrid Org**. Training is provided as follows:
   a. To all Responsible Employees upon hire and annually.
   b. To any individuals who have been determined to be *responsible employee*s once said determination is complete (based on a change in the employees roles and responsibilities).

   c. To Responsible Employees whose functions are affected by a significant change in **Hybrid Org's** privacy policies and procedures or legal requirements, within a reasonable period of time after a change becomes effective.
2. Training is provided through the Compliancy Group's "The Guard", on the use of Kiteworks (for secure end to end encrypted messages), on Vontier specific procedures and Use cases. Additional written resources are also provided.
3. **Hybrid Org** documents when responsible employees complete trainings through the Guard, attend live trainings, and sign attestations.
4. Questions concerning training or any aspect of training may be directed to the *Privacy Official* or his designee.

Safeguards:
Hybrid Org reasonably safeguards protected health information (*PHI*) from any intentional or unintentional use or disclosure that violates the *HIPAA* Privacy Rule. **Hybrid Org** also reasonably safeguards protected health information to limit incidental *PHI* uses or disclosures that are made pursuant to an otherwise permitted or required use or disclosure. Following any risk assessment of the *PHI* held by **Hybrid Org**, Hybrid Ord implements or modifies Physical, Administrative and Technical safeguards to reasonably address the risk of improper *access*, use or disclosure of *PHI* in all forms including oral, visual, paper, electronic (addressed separately in the security policy), film, or any other format.

Examples of safeguards are:
- Administrative safeguards: Policies and Procedures including discipline, training, and guidance;
- Physical Safeguards: locks, segregation of *PHI* in secured areas, *access* restrictions, and sign-in sheets for vendors; and
- Technical Safeguards: encryption, key card *access*, firewalls, *access* reviews.

Hybrid Org conducts physical audits of its locations to identify and address risks which require reasonable safeguards. The results of these audits are logged in the Facility Directory in the Guard. **Hybrid Org** reviews privacy complaints and incidents to determine if additional safeguards are necessary for any recurring incident or complaint types.

Complaints:
Hybrid Org provides a process for *individual*s to make complaints concerning its compliance with the *HIPAA* Privacy Rule, the *HIPAA Breach* Notification Rule, and **Hybrid Org's** policies and procedures related to these rules. **Hybrid Org** addresses all complaints received and keep records of complaints and their resolution. Please refer to Privacy Policy 5.0: *Complaints to the Hybrid Org* for more details. **Hybrid Org** will handle any complaints that are also found to be Privacy incidents under Privacy Policy 6.0: *HIPAA Incident Response and Reporting and Breach Determination*.

Sanctions:
Hybrid Org has determined that the sanctions for failure to comply with privacy policies and procedures are adequately outlined in the Vontier Employee Manual for US personnel. **Hybrid Org** documents all sanctions and applies them in a consistent manner. The *Privacy Official* is responsible for the determination of appropriate sanctions and may involve human resources in any decision. In deciding upon the appropriate sanction, **Hybrid Org** may review the severity of the violation, the impact of the violation, and the *Responsible Employee's* work history. The *Privacy Official*, in his or her discretion, may review the sanction decision at the request of a *Responsible Employee*.

Mitigation:
Hybrid Org mitigates, to the extent practicable, any harmful effect that is known to it of a use or disclosure of *PHI* in violation of its policies and procedures or the *HIPAA* Privacy Rule by **Hybrid Org** or its *business associates*.

Hybrid Org ensures that mitigation plans are developed, implemented, modified and applied in accordance with these policies and procedures. In response to a report of or information about a *Responsible Employee's* or *business associate's* unauthorized use or disclosure of *PHI*, **Hybrid Org** acts promptly to reduce any known or reasonably anticipated harmful effects from the disclosure. **Hybrid Org** contacts the recipient of the information that was subject of the unauthorized disclosure and requests that such recipient either destroy or return the information. **Hybrid Org** takes other appropriate action to prevent further use or disclosure.

No Retaliation:
Hybrid Org will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against anyone who files a complaint either with the **Hybrid Org** or with *HHS*, who exercises a right to which they are entitled under the Privacy Rule, or the *Breach* Notification Rule, or who testifies, assists with or participates in an investigation, compliance review, or proceeding, or opposes any act or practice that he or she reasonably believes is unlawful under these regulations.

Waiver of Rights:
Hybrid Org does not require any *individual* to waive his or her right to file a complaint with **Hybrid Org** or *HHS*. Hybrid Org may not condition the provision of *treatment*, *payment*, enrollment in a health plan, or eligibility for benefits on an *individual*'s waiver of their right to file such a *HIPAA* compliance complaint.

Changes to Policies and Procedures:
Hybrid Org changes its policies and procedures as necessary and appropriate to comply with changes in the law, organizational changes, and/or regulatory changes. Whenever a change necessitates modification of **Hybrid Org's** policies or procedures, **Hybrid Org** promptly documents and implements the revised policy or procedure. If any change materially affects the content of the Notice of Privacy Practices, **Hybrid Org** changes the contents of the notice accordingly.

Documentation:
Hybrid Org maintains its policies and procedures in written or electronic form for six years.

RELEVANT HIPAA REGULATIONS:
45 CFR Part 164 Subpart E
45 CFR 164.530 HIPAA Privacy Program Administrative Requirements

Privacy Policy 2.0 Administrative, Technical and Physical Safeguards of PHI

FULL POLICY LANGUAGE:
Policy Purpose:
It is the policy of **Hybrid Org** to ensure that *PHI* is protected from misuse, loss, tampering, or use by unauthorized persons. This policy addresses the safeguarding of *PHI* received, created, used, maintained, and/or transmitted and reflects some of the safeguards implemented by **Hybrid Org** to protect the privacy of *PHI*.

Policy Description:

The *HIPAA* Privacy Rule, 45 CFR 164.530, requires **Hybrid Org** to develop and implement safeguards to protect the privacy of *PHI*. This policy reflects the development of safeguards appropriate to Hybrid Org's operations and some of the safeguards **Hybrid Org** has implemented to protect the privacy of *PHI* that is not in electronic form. **Hybrid Org** has also implemented safeguards for the protection of *ePHI* as required concurrently by the Privacy Rule and the Security Rule. (The *HIPAA* Security Rule section 164.306(a) requires the safeguarding of the confidentiality, integrity, and availability of *ePHI* that **Hybrid Org** creates, receives, maintains, or transmits). The *ePHI* safeguards are reflected in the Security Manual.

Procedures:

Hybrid Org protects the privacy of *PHI*. In order to do so, **Hybrid Org** implements safeguards for the protection of *PHI* and *Responsible Employees* are encouraged to make suggestions regarding additional safeguards that could aid them in protecting the privacy of *PHI.* Safeguards include, for example, putting away *PHI* when not in use, not keeping PHI where it is easily accessible to others, obscuring a computer screen from view by others, and locking cabinets containing *PHI*. Hybrid Org offers training through the Guard on these safeguards.

When operations, facilities or circumstances change, **Hybrid Org** promptly assesses the new situation and develops and adapts safeguards appropriate to the circumstances if current safeguards will not sufficiently address the privacy of *PHI*. Hybrid Org then updates the Facilities Directory in the Guard. The Privacy Official or their designee and others involved in the management of the operations or facility that are new or changing work together with the *workforce* to assure reasonable and appropriate safeguards are in place to protect the privacy and integrity of the *PHI*.

Responsible Employees are required to ensure that PHI is adequately safeguarded by:

- Complying with the Privacy and Security Manuals and other **Hybrid Org** Policies and Procedures, including the Vontier Code of Conduct;
- Following directions of your supervisor within the Hybrid Org related to the privacy of *PHI*;
- Taking trainings through the Guard, Kiteworks, and Vontier specific use training and following the guidance in the trainings;
- Use common sense strategies to protect *PHI* from public view, incidental disclosure and harm or theft appropriate to the situation;
- Securely storing all documents with *PHI* when they are not in use in locked cabinets or in sturdy boxes kept off the ground to avoid damage in a locked area or office;
- Shielding *PHI* from the view of others;
- Follow faxing instructions including: the use of the Hybrid Org's fax cover sheet (which includes a confidentiality notice), ensuring that the person is expecting the fax, confirming the fax number, and periodically updating any stored fax numbers;
- Utilizing first class mail for delivery services or other reliable delivery services such as UPS, FedEx, and DHL;
- Utilize services such as certifying and tracking deliveries when signatures or proof of delivery is desirable or required;
- Using packaging which protects the contents of a letter or package from view and using appropriately sized and quality packaging to protect *PHI* in transit;

- Following appropriate disposal methods, including shredding or other means of rendering PHI undecipherable;
- Locking doors and not sharing keys, *access* codes or badges and secure same when not in use;
- Assuring that the facility where *PHI* is present has smoke detectors and fire extinguishers on hand and operational. If sprinklers are present, assuring they are in working order;
- Performing necessary building maintenance and assuring the facility is properly ventilated and clean to avoid damage from temperature, humidity, dust and dirt;
- Obtaining consents or authorizations prior to sharing information when required;
- Utilizing an emergency power shutdown management system, when appropriate;
- Utilizing sign in and sign out sheets for all vendors entering the facility and assuring that vendors are accompanied in the facility;
- Using common sense tactics to avoid theft, inadvertent exposure, and damage to *PHI;*
- Making suggestions for changes or for more formal safeguards for recurring situations you may encounter; and
- Following the *minimum necessary standard* whenever it applies**.**

RELEVANT HIPAA REGULATIONS:

45 CFR 164.528(c): *Accounting of Disclosures of Protected Health Information: Safeguards*

Privacy Policy 3.0 Minimum Necessary Standard

FULL POLICY LANGUAGE:

Policy Purpose:

To establish rules for ensuring that Hybrid Org appropriately applies use of the *Minimum Necessary Standard* when requesting, using and disclosing protected health information.

Policy Description:

The *HIPAA* Privacy Rule generally requires *covered entities*, including **Hybrid Org**, to make reasonable efforts to adhere to a "minimum necessary" standard with respect to requests for the use and disclosure of *PHI*. When requesting, using or disclosing *PHI*, **Hybrid Org** makes reasonable efforts to limit *PHI* to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request under circumstances where the standard applies.

Procedures:

Applicability of Standard:

The *minimum necessary standard* applies in many situations so *Responsible Employees* must be aware of the situations in which it does not apply and act in accordance with the standard in all other circumstances. **Hybrid Org** and all *Responsible Employees* will apply the Minimum Necessary standard for requesting, using, and disclosing *PHI* except for requests, uses and disclosures made in the following circumstances:

1. Disclosures to or requests by a health care *provider* for *treatment* purposes;
2. Uses or disclosures made to the *individual* who is the subject of the information or their legal representative including those made pursuant to an *individual*'s request under the Privacy

Rule Right of *Access* Standard (164.524), or the Accounting of *PHI* Disclosures Standard (164.528).
3. Uses or disclosures made pursuant to a valid and *HIPAA* compliant authorization (information provided in these circumstances will be limited by the terms of the authorization itself);
4. Disclosures made to the U. S. Department of Health and Human Services (*HHS*) when disclosure of information is required for enforcement purposes (i.e., in response to a complaint filed with the Secretary of *HHS*); and
5. Uses and disclosures that are required by law to the extent that the use or disclosure complies with and is limited to the relevant requirements of such law (i.e., victims of abuse; neglect or domestic violence; judicial administrative proceeding; and law enforcement purposes).

Procedure for Limiting *Access* When Standard Must be Followed:

1. **Hybrid Org** has identified the classes of persons or job titles within **Hybrid Org's** *workforce* who need *access* to *PHI* to carry out their job duties and responsibilities. These individuals are Responsible Employees and are listed in **Appendix 1**, as amended from time to time.
2. **Hybrid Org** authorizes *access* to computerized health information. Use of this information is limited based on reasonable determination regarding an *individual*'s position and/or department. The majority of health information is held by the Vontier Benefits Department, so a small number of individuals regularly handle PHI and are trained on how to do so.
3. Hybrid Org controls an individual's *access* via user IDs and passwords. The sharing of login IDs and passwords is strictly prohibited.

Routine or Recurring Requests and Disclosures for *Individual*'s Information when the Standard Applies:

1. Requests for individual information made on a routine or recurring basis shall be limited to the minimum amount of the *individual*'s information necessary to meet the needs of the request/disclosure.
2. Hybrid Org has established minimum necessary definitions and standard protocols for routine and recurring requests/disclosures.
3. Hybrid Org is not required to individually review requests/disclosures made on a routine or recurring basis where standard protocols have been developed; however, Hybrid Org will periodically review routine or recurring requests to ensure they are still valid and necessary.

Non-Routine Requests for Disclosure of *Individual*'s Information when the Standard Applies:

1. Hybrid Org reviews non-routine requests for individual information on an individual basis to limit the individual information requested/disclosed to the minimum amount necessary to accomplish the purpose of the request/disclosure.
2. *Responsible Employees* perform these reviews on an individual basis remembering that the standard does not apply to requests/disclosures to or from a health care *provider* or for *treatment* purposes.
3. *Responsible Employees* will not review disclosures/requests authorized by the *individual* or the *individual*'s legal representative for conformance with the *minimum necessary standard* but will review it for conformance with the terms of the authorization.
4. **Hybrid Org** may not use/disclose an entire *medical record* if it is determined, after conversation with the requestor or by established protocol, that the entire *medical record* is not justified as the amount that is reasonably necessary to accomplish the purpose of the use/disclosure.

Restrictions:

See Privacy Policy 16: *Individual Right: Request Restrictions and Alternate Confidential Communications for PHI* for more information regarding restrictions on the communication of *PHI*. These restrictions must be met even in situations in which the *minimum necessary standard* applies.

Requesting Individual Information:
When requesting *PHI* from *covered entities*, **Hybrid Org** will limit any request for information to that which is reasonably necessary to accomplish the purpose for which the request is made. PHI requests made by *providers* for treatment purposes are not covered here, and the minimum necessary standard does not apply to their requests.

Corrective Action:
Upon determination of inappropriate or unauthorized *access* to or disclosure of *PHI* by a *Responsible Employee*, the **Hybrid Org** determines the appropriate corrective action for the misconduct and assesses the matter as a Privacy incident. Please refer to Privacy Policy 1.0: *Privacy Program: General* regarding failure to comply with privacy practices, Privacy Policy 8.0: *Sanctions/Discipline* and Privacy Policy 6.0: *Incident Response and Reporting and Breach Determination* for further details on how to handle such matters.

RELEVANT HIPAA REGULATIONS:
45 CFR 164.502(b)(1) *Minimum Necessary Standard*
45 CFR 164.514(d)(3) *Minimum Necessary Disclosures of Protected Health Information*
45 CFR 164.524(a) *Access to Protected Health Information*

Privacy Policy 4.0 Verification of Identity and Authority

FULL POLICY LANGUAGE:

Policy Purpose:
The purpose of this policy is to ensure the **Hybrid Org** fulfills the *HIPAA* requirement of verification of identify and/or the authority of persons seeking disclosure of an individual's protected health information (*PHI*).

Policy Description:
To ensure that protected health information (*PHI*) is disclosed only to appropriate persons, **Hybrid Org** verifies the identity and authority of a person making a request for the disclosure of *PHI* unless the *individual* has agreed to the disclosure. In addition, **Hybrid Org** obtains from the person seeking disclosure of *PHI*, such documentation, statement, or representation, as may be required under the *HIPAA* Privacy Rule or desired as a best practice (and not prohibited by law), prior to disclosure.

Procedures:
Hybrid Org verifies the identity and confirms the authority of any individual outside of **Hybrid Org** requesting *PHI*.

If documentation, statements, or representations are a condition of disclosure under the Privacy Rule, Hybrid Org will obtain them prior to the disclosure. The details of any oral representation will be recorded in writing by the **Hybrid Org**.

When the Requester is the *Individual*:
When the requester is the *individual*, verification of identity may be accomplished by asking for photo identification (i.e., driver's license), if the request is made in person. If the request is made over the

telephone or in writing, verification may be accomplished by requesting identifying information (i.e., address, telephone number, birth date, and/or *medical record* number) and confirming that this information matches what is in the *individual*'s record.

When the Requester is the *Individual*'s *Personal representative*:
Please also refer to Privacy Policy 11: *Uses and Disclosures of PHI, General Rules* paragraph on *Personal representative*s and Privacy Policy 20: *Minors' Rights* for specifics on *personal representative*s of minors.

When the Requester is the *individual*'s *personal representative*, verification of identity may be accomplished by asking for photo identification (i.e., driver's license). Once identity is established, authority in such situations may be determined by confirming the person is named in the *medical record* as the *individual*'s *personal representative*.

If there is no person listed in the *medical record* as the *individual*'s *personal representative*, authority may be established by the person presenting a copy of a valid power of attorney for health care or a copy of a court order appointing the person guardian (or guardian ad litem) of the *individual*. Authority may also be established by an *individual*'s identification of the person or by a relative (like a parent, spouse, or domestic partner) by providing their identification along with information reflecting their relationship to the *individual*.

When the Requester is a Public Official or Legal Officer:
Please refer to Privacy Policy 22.0: *Uses and Disclosures: Response to Judicial and Administrative Proceedings* for more specifics of responding to requests related to Judicial and Administrative requests. In verifying the identity of a public official or legal officer (i.e., attorneys, judges, law enforcement officers, medical examiners, or coroners), **Hybrid Org'**s *Responsible Employees* may rely on any of the following, if reasonable under the circumstances:

1. A badge or similar official credential.
2. A Bar association listing indicating "active" and "in good standing" status in conjunction with ID (e.g., driver's license).
3. A request on government or law firm letterhead in conjunction with ID.
4. If the person making the request is acting on behalf of a public official, a written statement on government letterhead that the person is acting on behalf of the public official along with ID.

Once identity has been verified, when the public official or legal officer submits the request, whether in person or in writing, *Responsible Employees* presented with, advised of, or who become aware of such requests, will alert their supervisor as soon as possible. The supervisor will then forward the request to the *Privacy Official* of the **Hybrid Org.** Only the *Privacy Official* or their designee may respond to the request unless legal process requires no delay.

The *Privacy Official* or their designee, in consultation with others, including counsel, when assistance is needed, will establish the authority of the public official or legal process.

Hybrid Org may rely on the following, if reliance is reasonable under the circumstances and if approved by a supervisor:

1. A written statement of the legal authority or, if a written statement would be impracticable, an oral statement of such legal authority;

2. A request made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or *administrative tribunal* is presumed to constitute legal authority. Refer to Privacy Policy 22.0: *Uses and Disclosures: Response to Judicial and Administrative Proceedings* for more details on procedures.

If the public official's request is an administrative request, subpoena, or a request related to an investigation, the **Hybrid Org** shall disclose the requested *PHI*, provided the document containing the request, recites:

1. The information sought is relevant to a lawful inquiry, legal proceeding, investigation, or law enforcement activity; and
2. The request is specific and limited in scope, as much as practicable, for the purposes of the inquiry.

When the Request is to Avert a Serious Threat to Health or Safety or in Situations allowing an *Individual* to Agree or Object:

HIPAA verification requirements are met where the Hybrid Org relies on the exercise of professional judgement when disclosing information in situations allowing an *Individual* to agree or object. See Privacy Policy 12.0; *Uses and Disclosures Requiring an Individual Opportunity to Agree or Object* for details of those situations.

HIPAA verification requirements are met where the Hybrid Org acts on a good faith belief in making a disclosure related to averting a serious threat to health or safety. See the paragraph addressing these disclosures in Privacy Policy 14.0: *Uses and Disclosures, No Authorization Required*, for further details on these disclosures**.**

Other Requesters:
Procedures for verifying the identity and/or authority of other unknown requesters of *PHI* will vary according to the circumstances. See Privacy Policy 4.0: *Verification of Identity and Authority* for further details.

When Identity Has Not Been Clearly Established:
Generally, **Hybrid Org's** *Responsible Employees* may rely on required documentation, statements, or representations that, on their face, meet the verification requirements, provided the reliance is reasonable under the circumstances. If there are concerns as to the reliance, staff shall contact the *Privacy Official* or their designee for guidance. See Privacy Policy 4.0: *Verification of Identity and Authority* for further details.

RELEVANT *HIPAA* REGULATIONS:

45 CFR 164.514(h)(1) *Standard Verification Requirements*

Privacy Policy 5.0 Complaints to the Hybrid Org

FULL POLICY LANGUAGE:
Policy Purpose:
To provide an effective process for reporting concerns or complaints about **Hybrid Org's** privacy policies and procedures, **Hybrid Org's** compliance with those policies and procedures, and **Hybrid**

Org's compliance with the *HIPAA* Privacy Rule and the *HIPAA Breach* Notification Rule. To prevent intimidating, threatening, coercing, discriminating against, or retaliating against any *individual* who has exercised a right under *HIPAA* including filing complaints.

Policy Description:

Hybrid Org strives to ensure the privacy of Protected Health Information ("*PHI*"), and to ensure this information is used and disclosed in accordance with all applicable laws and regulations and in conformance with the Privacy Manual. Hybrid Org will honor an *individual*'s right to make complaints concerning **Hybrid Org's** compliance with the *HIPAA* Privacy Rule, its Notice of Privacy Practices and its *HIPAA* privacy policies and procedures. Hybrid Org will honor an *individual*'s right to make complaints concerning the **Hybrid Org's** *breach* notification process and compliance with the *Breach* Notification Rule.

Hybrid Org will also act to prevent anyone from intimidating, threatening, coercing, discriminating against, or retaliating against any *individual* who has exercised their right under *HIPAA* to file complaints with the **Hybrid Org** concerning it's *HIPAA* compliance. Any such act that is reported to **Hybrid Org** will be investigated by the *Privacy Official* or an uninvolved person designated by the **Hybrid Org** and handled under Privacy Policy 8.0: *Sanctions/Discipline* when appropriate.

When a Privacy complaint belongs to the subset of complaints referred to as Privacy Incidents (any attempted or successful unpermitted or unauthorized *access*, use, disclosure, modification, interference or destruction of *unsecured PHI* in any form), **Hybrid Org** will handle the complaint according to Privacy Policy 6.0: *Incident Response and Reporting and Breach Determination*.

Procedures:

Processing a Complaint:

1. Hybrid Org's Notice of Privacy Practices notifies *individuals* (or their *personal representatives*) of their right to complain to Hybrid Org or the Department of Health and Human Services ("*HHS*").
2. Hybrid Org accepts complaints by telephone, mail, or email at Vontier Employment Services, LLC, 5438 Wade Park Blvd., Suite 600, Attn: HIPAA Inquiry/Benefits Department, Raleigh, NC 27607, Phone: (817) 323-1405, email: HIPAA@Vontier.com.
3. *Responsible Employees* should forward complaints received in any manner to the *Privacy Official* at HIPAAInquiry@vontier.com.
4. Upon receipt of any complaint about **Hybrid Org's** privacy policies and procedures, **Hybrid Org's** compliance with those policies and procedures, or **Hybrid Org's** compliance with the *HIPAA* Privacy Rule and the *HIPAA Breach* Notification Rule, the *Privacy Official* shall document the following in a *Complaint Log*:
    a. The date the complaint was received; and
    b. A copy of the written complaint, if any, or a general description of the verbal complaint.
5. Once the complaint is correctly documented in the Complaint Log, the *Privacy Official* shall coordinate with appropriate individuals to determine whether the complaint is a Privacy incident. If it is a Privacy incident the complaint will be handled according to the process in Privacy Policy 6.0: *Incident Response and Reporting and Breach Determination*.
6. If the complaint is not a Privacy incident, the *Privacy Official*, in coordination with other appropriate individuals, including counsel where necessary, shall decide whether an investigation is warranted. If an investigation is warranted, the *Privacy Official* or their designee will conduct the investigation. The **Hybrid Org** will make reasonable efforts to complete the investigation in a timely manner.

7. If the complaint involves an allegation of intimidation, threats, coercion, discrimination against, or retaliation against any *individual* who has exercised their right under *HIPAA* to file complaints with the **Hybrid Org** concerning its *HIPAA* compliance, the complaint will be investigated by the *Privacy Official*, or an uninvolved person designated by the **Hybrid Org.**
8. If any person designated under this policy to investigate, receive or respond to complaints is a party to the action or inactions complained of, Hybrid Org will assign an uninvolved person with appropriate skill and knowledge to review, investigate and respond to the complaint.
9. Upon completion of complaint investigations under this policy, the *Privacy Official* shall:
    a. Document the outcome of the complaint by entering the resolution and any required follow-up actions on the Complaint Log.
    b. Communicate the outcome of the complaint to the person who made the complaint within 30 days from the *Privacy Official*'s receipt of the complaint.
10. If the *Privacy Official* determines that a violation of policy, procedure, the *HIPAA* Privacy Rule, or the *HIPAA Breach* Notification Rule has occurred, the *Privacy Official* shall initiate and coordinate actions as appropriate according to Vontier's Employee Handbook for US Personnel (see Privacy Policy 8.0). **Hybrid Org** will develop and implement a corrective action plan to address the violation and mitigate any consequences of the violation.
11. The *Privacy Official* shall maintain documentation of all complaints received, and the disposition of each, for a period of at least six years.

RELEVANT HIPAA REGULATION:

45 CFR 164.530(a)(d) and (g)*Administrative Requirements: Personnel Designations, Complaints and Refraining from Intimidating or Retaliatory Acts*
45 CFR 164.524(d) *Individual Right: Right to file Complaint Concerning Denial of Access*
45 CFR 164.520(b)(1)(vi) *Notice of Privacy Practice: Complaints*

Privacy Policy 6.0 HIPAA Incident Response and Reporting and Breach Determination

FULL POLICY LANGUAGE:

Policy Purpose:

Hybrid Org takes the privacy, security and integrity of *individuals'* data seriously. **Hybrid Org** also has legal responsibilities to protect *PHI* under *HIPAA*, to identify and respond to suspected incidents, mitigate harm, require its *Responsible Employees* to report incidents, and to determine when there is a reportable *breach* of an *individual*'s *PHI*.

The purpose of this Incident Response and Reporting and *Breach* Determination Policy is to meet **Hybrid Org's** responsibilities and to provide guidance to Hybrid Org *Responsible Employees* regarding recognizing and reporting a privacy or *security incident* involving protected health information. Hybrid Org will review all reported incidents and will follow the procedures set forth to determine if there has been a *Breach* (an acquisition, *access*, use, or disclosure of the Member's *unsecured PHI* in a manner not permitted under *HIPAA*).

Policy Description:

This policy establishes guidelines for Hybrid Org to:

- Require the reporting of suspected privacy and *security incident*s (any attempted or successful unpermitted or unauthorized *access*, use, disclosure, modification, interference or destruction of *unsecured PHI* in any form). All *Responsible Employees* must report, as soon as possible, any suspected incident to the Privacy or Security Official, through the Guard, through the SharePoint portal, or through InfoSec. *Responsible Employees* who fail to

promptly report incidents may be subject to discipline. See Privacy Policy 8.0: *Sanctions/Discipline* for additional details.

- Identify and respond to suspected or known incidents involving the security or privacy of protected health information, including mitigating any harmful effects. Hybrid Org will handle any complaint that is potentially a privacy or *security incident* under this Policy, which also appears in the Security Manual, instead of Privacy Policy 5.0: *Complaints to the Hybrid Org*.
- Determine if there has been a *Breach* of *unsecured PHI* ("*PHI*") after analyzing potential exceptions and performing a risk analysis or requiring any involved *Business associate* to do so and then reviewing their determination, and
- Document the incidents, responses and *Breach* determinations and retain the documentation for at least six years.

Procedures:

Reporting of *Security incidents*: Hybrid Org trains all *Responsible Employees* on *HIPAA* privacy and security requirements. All Hybrid Org *Responsible Employees* must report to Hybrid Org's *Privacy Official*, Security Official, InfoSec, or the Guard as soon as possible after discovering any suspected, known, or potential Privacy or *Security incident*. Supervisors must notify the Privacy and Security Officials immediately upon notification of potential, known or suspected Incidents. Hybrid Org *Responsible Employees* are subject to discipline for failure to promptly report any suspected, known, or potential *Breach* of *unsecured PHI*. Hybrid Org requires *Business associates* to report Privacy and *Security incidents* promptly.

Monitoring for Privacy and *Security incidents*: Hybrid Org's IT and InfoSec departments employ tools and techniques to monitor events, detect attacks and provide identification of unauthorized use of the systems that contain Electronic Protected Health Information (*ePHI*). They also periodically review *access*, integrity, use and disclosure of all *PHI*, in whatever form, to identify any potential *breaches*.

Treatment of Recurring and Expected Unsuccessful HIPAA incidents: Hybrid Org acknowledges the ongoing existence or occurrence of attempted but "Unsuccessful *Security incidents*" including but not limited to, pings, and other broadcast attacks on firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above. As long as no such Unsuccessful *Security incident* results in unauthorized *access*, use or disclosure, inappropriate denial of *access* or harm to the integrity of *ePHI*, they will be reviewed, and the reports kept but Hybrid Org will not undertake a full factual investigation or *breach* determination analysis for each such unsuccessful attempt. Unsuccessful *Security incidents* are reviewed for heightened frequency and considered in the development, implementation of and improvements to safeguards. Hybrid Org performs a thorough analysis of any suspicious circumstances or unusual activity found during reviews.

Perform and Document a Factual Investigation of the Incident: Hybrid Org performs a factual investigation of any reported potential privacy or *security incident*. At a minimum, Hybrid Org seeks information and documentation sufficient to a) perform an analysis of whether there was any attempted or successful *unauthorized access*, use, disclosure, modification, or destruction of information in any form, b) determine if any unsecured information was involved, c) determine if any *PHI* was involved d) determine if any exception to an assumption of a *Breach* of *PHI* exists, e) perform the risk of *PHI* compromise analysis and f) determine the number of *individuals* impacted. Hybrid Org may retain outside resources for the completion of some or all of the investigation, especially if a forensic investigation is desirable.

Should the Privacy or *Security incident* occur through a *business associate*, Hybrid Org may rely on the *Business associate* to conduct an investigation but may also conduct an independent investigation if it so chooses. Hybrid Org must review the *Business associate's* findings and underlying facts prior to deciding on whether or not to rely solely on the *Business associate's* investigation or to perform its own investigation.

Determine Need and Implement Reasonable Mitigation Measures: Following the report or discovery of any HIPAA incident, Hybrid Org assesses whether any immediate or future safeguards or changes to process or practice are required to address the incident or its potential reoccurrence. Hybrid Org determines whether to involve law enforcement on a case-by-case basis. For mitigations specific to *security incidents*, please refer to Security Policy 6 for examples.

Determine if There Was Any Attempted or Successful Unauthorized *Access*, Use, Disclosure, Modification, or Destruction of Information in Any Form: Following a standard procedure and utilizing the HIPAA Breach Risk Assessment Record and *Unsecured PHI* Job Aid (available through the Guard) or similar documentation when applicable, Hybrid Org determines whether a) there was any attempted or successful *access*, use, disclosure, modification or destruction of information, b) whether the information involved was unsecured, c) whether such information was *PHI* or *ePHI*, d) whether such *access*, use, disclosure, modification, or destruction was unauthorized or unpermitted and e) whether any exceptions to a determination of a *breach* is applicable.

Hybrid Org may use the Unsecured PHI Job Aid or a similar standard assessment tool to determine if any information involved in the incident was unsecured.

Hybrid Org determines if the information involved in the attempted or successful unauthorized *access*, use, disclosure, modification, or destruction of information was *PHI*. For example, if the information involved a deceased *individual*, Hybrid Org determines if the *individual* been deceased for more than fifty years.

Hybrid Org determines if *access*, use, disclosure, modification, or destruction was unauthorized or unpermitted by determining if the use or disclosure was authorized or permitted under *HIPAA*. For example, Hybrid Org will determine if it was authorized by the *individual*, required by law, or permitted as incidental.

Determine if there is an Applicable Exception to a *Breach* Determination: As part of its *breach* determination, Hybrid Org refers to the three exceptions listed in paragraph 1 of the definition of *Breach* published in 45 CFR § 164.402 to analyze whether an exception applies. Hybrid Org determines and records its determination as to whether any of these three exceptions applies to the incident:

1.Any unintentional acquisition, *access*, or use of protected health information by a *Responsible Employee* or person acting under the authority of a *covered entity* or a *business associate*, if such acquisition, *access*, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part (Sets forth allowable uses of *PHI*).

2.Any inadvertent disclosure by a person who is authorized to *access* protected health information at a *covered entity* or *business associate* to another person authorized to *access* protected health information at the same *covered entity* or *business associate*, or organized health care arrangement in which the *covered entity* participates, and the information received as a result of such disclosure

is not further used or disclosed in a manner not permitted under subpart E of this part (Part E sets forth allowable uses of *PHI*).

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

If an exception applies, Hybrid Org will record its findings in the incident record and the incident can be closed. If no exception applies, there is a presumption that a *breach* has occurred. Hybrid Org may either perform a risk analysis according to the procedure set forth below or forego performing that analysis and follow the process for notifications under Privacy Policy 7.0: *Breach Notification*.

Perform an Analysis of Risk of Compromise to *unsecured PHI* utilizing the Four Required Factors and Other Pertinent Information: If Hybrid Org has determined that there is a presumption of a *breach*, Hybrid Org may perform a risk of compromise assessment using at least the following four required factors to determine if there is a low probability that *PHI* has been compromised that rebuts the presumption of a *breach*:

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

Hybrid Org may also consider other factors in its analysis that might support a finding of a low probability of risk including but not limited to the time the information may have been accessible or accessed, the likelihood the information was accessed, whether any complaints were received, how difficult or likely *access* was even if there was accessibility and any professional or legal requirements applicable to the person who received the information (does a legal privilege apply, was the person who received the information in healthcare and trained on *HIPAA* privacy requirements). The *HIPAA* Incident Assessment Tool may be useful in completing and documenting the risk of compromise assessment. If the *Breach* occurred through a *business associate*, Hybrid Org may rely on a *business associate* to perform the risk of compromise assessment but must review the findings and underlying facts prior to deciding on whether to perform its own assessment.

Record Keeping: Hybrid Org maintains a *HIPAA* incident log for all reported incidents, regardless of whether they are determined to be *Breach*es. Hybrid Org reviews this log periodically to determine areas that may require additional training. Hybrid Org keeps records concerning all reports of security or privacy incidents, any finding of an exception to the *Breach* definition, all analyses of risk of compromise to *unsecured PHI*, and the factual investigations and documentation supporting the analysis and findings. These records will be kept for a minimum of six years following the conclusion of the *Breach* determination for the incident(s).

Enforcement and Reporting: Hybrid Org's *HIPAA* Privacy and Security Officials and/or their designees, along with the Vontier Benefits Team, are responsible for managing, updating, and enforcing this policy. Violations of this policy must be immediately reported.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.308(a)(6)(i) *Security Incident Procedures*
45 CFR 164.308(a)(6)(ii) *Implementation Specification: Response and Reporting (Required)*
45 CFR 164.530(a)(c)(e)(f) *Administrative Requirements: Personnel Designations, Safeguards, Sanctions and Documentation, Mitigation*
45 CFR 402 *Definitions: Breach*

Privacy Policy 7.0 Breach Notification

FULL POLICY LANGUAGE:

Policy Purpose:

Hybrid Org takes the privacy and integrity of an *individual*'s personal health information seriously. Hybrid Org also has legal responsibilities to protect *PHI* under *HIPAA*, to determine when there is a reportable *breach* of an *individual*'s *PHI* and to make appropriate and timely notifications following a *breach*.

The purpose of this *Breach* Notification Policy is to meet Hybrid Org's responsibilities and to provide guidance to Hybrid Org *Responsible Employees* regarding making required notifications when a *Breach* determination has been made under Privacy Policy 7.0: *Breach Determination*.

This policy establishes guidelines for Hybrid Org to:

- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to *individual*s impacted by a *Breach*,
- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to federal and state authorities if required by the details of the *Breach* determination,
- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate notifications to media if the findings of the *Breach* determination require them;
- Determine when and if appropriate substitute notice is allowed and to use that substitute notice when appropriate; and
- Document compliance with the requirements of *Breach* notifications.

Policy Description:

This policy establishes guidelines for Hybrid Org to:

- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate timely notifications to *individual*s impacted by a *Breach*;
- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate timely notifications to federal and state authorities if required by the details of the *Breach* determination including reporting of *breach*es involving less than 500 *individual*s in a single state or geographic region to *HHS* electronically on an annual basis by March 1 (or February 29th in a Leap year) of the year following the *Breach*;
- Make, or assure the appropriate *Covered entity* or *Business associate* makes, appropriate timely notifications to media if the findings of the *Breach* determination require them;
- Determine when and if appropriate substitute notice is allowed and to use that substitute notice if required or desired;
- Ascertain and meet any more stringent applicable contractual notification requirements; and
- Document compliance with the requirements of this policy.

Following the determination of a *breach* under Privacy Policy 9: *HIPAA incident Reporting and Response and Breach Determination* **Hybrid Org** will determine what external notifications are required or should be made (i.e., Secretary of Department of Health & Human Services (*HHS*), media outlets, law enforcement officials, etc.), develop appropriate content for the notices, reports and postings, and communicate each notification, report or positing according to the procedures and requirements set forth below.

Procedures:

Privacy and Security Officials Shall Direct all Notifications but may appropriately Delegate Activities

With input from others at their discretion, Hybrid Org's Privacy and Security Officials will direct all activities required under this policy including the wording of any *Individual* Notices, *HHS* filings, communications required by contract, Media notices, and scripts (including escalation processes) for any telephone inquiries. Legal representation will be utilized if desired by the Privacy or Security Official or at the direction of anyone on the senior leadership team of the Hybrid Org. The Privacy and Security Official may delegate responsibilities as appropriate but remain responsible for the implementation of *Breach* Notification Policy requirements. This delegation includes allowing either another responsible *Covered entity* or a responsible *Business associate* to make the notifications. Hybrid Org remains responsible for assuring all requirements have been met by the delegated entity or individual. For responsibilities of *Business associates*, please refer to Privacy Policy 9.0: *Business associates* for more information.

Hybrid Org will determine notification requirements based on the findings of the *Breach* Incident Investigation. Hybrid Org will use the number of *Individual*s involved to determine appropriate notifications and timing.

Individual Notification: If the number of *individual*s impacted by a *breach* is known to be less than 500, Hybrid Org will follow the notification Procedures set forth below for the timing and content of *Individual* Notification and Notification to *HHS*.

500 or More: If the number of *individual*s affected by the *Breach* is known to be 500 residents of a State or jurisdiction, Hybrid Org will provide notification to Prominent media outlets serving the State and regional area where the impacted *individual*s reside and follow the notification Procedures set forth below for the timing and content of Media Notice, *HHS* and Notification for *Breach*es Affecting more than 500 *individual*s.

If the number of *individual*s is uncertain, Hybrid Org must use reasonable efforts to estimate the number of affected *individual*s and document its methods. Hybrid Org shall use this estimate to determine the number of *individual*s affected for determining appropriate notification procedures. Should further information or investigation prove the estimate to be incorrect, Hybrid Org must update any previous notifications or reports made using that estimate if the method or content of the Notice is materially different due to the change.

Details of Appropriate Notice, Timing, Content and Means appear below the summary chart.

IF	Notification To	Timing*	Content	Means of Notice
Number of *Individual*s	Each person individually	Without unreasonable delay and in no	In plain language	In writing by first class mail or by email if the

impacted is less than 500		case later than 60 days following discovery of *breach*	A. A brief *breach* description, including date and the date of B. types of *unsecured PHI* that were involved C. steps the *individual* should take to protect themselves D. what the Hybrid Org is doing to investigate, mitigate harm to *individual*s, and to protect against further *Breach*es; and E. Contact procedures	affected *individual* has consented to such notice. Additional notice in urgent situations, it may do so by telephone or other means in addition to the written notice Substitute notice**
	HHS	no later than 60 days after the end of the calendar year in which the *Breach*es were discovered (March 1 or February 29th in a leap year).	In addition to content required for *individual* notice, Information Required on Current *HHS* report includes Entity Contact, BA Contact if Occurred at BA, Number of *individual*s impacted, safeguards placed prior to *breach*, mitigation efforts, safeguards placed after *breach*, number of *individual*s impacted	Completion of online form on the *HHS* website
Number of *Individuals* Impacted is greater than 500 in any State or jurisdiction	Prominent Media Outlet serving the areas where impacted *individuals* reside	without unreasonable delay and in no case later than 60 days following the discovery of a *Breach*	In plain language: A. A brief *breach* description, including date and the date of B. types of *unsecured PHI* that were involved C. steps the *individual* should take to protect themselves D. what the Hybrid Org is doing to investigate, mitigate harm to *individuals*, and to protect against further *Breach*es; and E. Contact procedures	Contact media and provide information to be included in publication
	HHS	without unreasonable delay and in no case later than 60 days following the	In addition to content required for media notice, Information Required on Current *HHS* report includes Entity Contact, BA Contact if Occurred at BA, Number of	Completion of online form on the *HHS* website

		discovery of a *Breach*	*individuals* impacted, safeguards placed prior to *breach*, mitigation efforts, safeguards placed after *breach*, number of *individual*s impacted	

*Subject to Law Enforcement requests for delay
**Substitute notice may be used in some situations for *individuals*, see policy for details.

Timing

Hybrid Org will provide *Individual* notice without unreasonable delay and in no case later than 60 days following the discovery of a *Breach*. The Hybrid Org may also provide additional notice in urgent situations because of possible imminent misuse of the *PHI*.

Hybrid Org will provide Media Notice, when required, without unreasonable delay and in no case later than 60 days following the discovery of a *Breach*.

Hybrid Org will provide *HHS* notice by completing a web report form on the following timeline: If 500 or more individual residents of a State or jurisdiction are affected, Hybrid Org will complete the *HHS* notification without unreasonable delay and in no case later than 60 days following the discovery of a *Breach*. If fewer than 500 *individual*s are affected, Hybrid Org will notify *HHS* of each *Breach* no later than 60 days after the end of the calendar year in which the *Breach*es were discovered (March 1 or February 29th in a leap year).

Discovery of *Breach*

A *breach* of *PHI* shall be treated as "discovered" as of the first day the *breach* is known to the **Hybrid Org**, or, by exercising reasonable diligence would have been known to the **Hybrid Org** (includes *breach*es by **Hybrid Org's** *Business associates*). The **Hybrid Org** shall be deemed to have knowledge of a *breach* if such *breach* is known or if by exercising reasonable diligence would have been known, to any person, other than the person committing the *breach*, who is a *Responsible Employee* or an *agent* of the Hybrid Org (i.e., a *Business associate* acting as an *agent* of the **Hybrid Org**).

Delays in timing permitted: Law Enforcement Delay

When Hybrid Org is notified by a law enforcement official that a notification, notice or posting required for a *Breach* would either impede a criminal investigation or damage national security, Hybrid Org may delay the notification, notice or posting for a) a period of time specified by the law enforcement official in writing or b) for the requested amount of time not to exceed 30 days from the date of an oral request for delay from a law enforcement official. Hybrid Org will extend the original 30-day delay imposed by an oral request if a law enforcement official makes a later request in writing prior to the expiration of the initial delay request. Any such oral or written request must be documented by Hybrid Org and the record preserved. *Responsible Employees* should also refer to Privacy Policy 4: *Verification of Identity and Authority* when processing any law enforcement request for delay.

Content and Means of Notifications and Postings

At a minimum the content of reports, notifications and notices required by law for *breach*es of the privacy or security of *PHI* in any form must include the information set forth below and must be communicated by the means indicated:

Individual Notice: Means of Communication

In writing by first class mail or by email if the affected *individual* has consented to such notice. If the Hybrid Org desires to send additional notice in urgent situations, it may do so by telephone or other means in addition to the written notice but not as a substitute for it.

Substitute *Individual* Notice

When Hybrid Org has insufficient contact information for ten or greater affected *individual*s, Hybrid Org will give notice by posting notice for 90 days on the company website or by publication in major print or broadcast media in the area where the affected *individual*s likely reside.

When Hybrid Org has insufficient contact information for fewer than ten affected *individual*s it may give notice to those *individual*s by alternative written notice, by telephone or other reasonable means.

***Individual* Notice: Content**

1. A brief description of what happened, including the date of the *Breach* and the date of the discovery of the *Breach*, if known;
2. A description of the types of *unsecured PHI* that were involved in the *Breach* (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps the *individual* should take to protect themselves from potential harm resulting from the *Breach*;
4. A brief description of what the **Hybrid Org** is doing to investigate the *Breach*, to mitigate harm to *individual*s, and to protect against further *Breach*es; and
5. Contact procedures for *individual*s to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

Media Notice Means of Communication and Content

For Media Notices the following information should be included and the Notice must include enough information for an *individual* to determine whether their information may have been disclosed, what they should do if it was and who to contact for more information:

1. A brief description of what happened, including the date of the *Breach* and the date of the discovery of the *Breach*, if known;
2. A description of the types of *unsecured PHI* that were involved in the *Breach* (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps the *individual* should take to protect themselves from potential harm resulting from the *Breach*;
4. A brief description of what the **Hybrid Org** is doing to investigate the *Breach*, to mitigate harm to *individual*s, and to protect against further *Breach*es; and

5. Contact procedures for *individual*s to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

Means of Notifying *HHS*

For a *Breach* Affecting 500 or More *individual*s Hybrid Org will timely complete a Notice utilizing the form on the *HHS* website: (https://*OCR*portal.hhs.gov/*OCR*/*breach*/wizard_*breach*.jsf?faces-redirect=true).

For a *Breach* Affecting less than 500 *Individual*s Hybrid Org will timely file (within 60 days of the end of the calendar year in which the *Breach occurred*) a Notice utilizing the form on the *HHS* website (https://*OCR*portal.hhs.gov/*OCR*/*breach*/wizard_*breach*.jsf?faces-redirect=true).

Reliance on Others to Provide Notification

Hybrid Org will determine any contractual obligations related to the *PHI*. If allowable, Hybrid Org may choose to rely upon notifications given by a *Business associate* for the *Breach* notifications required. Hybrid Org will request copies of any notifications to its *individual*s, the public and *HHS* if Hybrid Org's *individual*'s information was *breach*ed.

Record Keeping

Hybrid Org keeps records concerning all notifications, notices and postings made separately for each *Breach* reported. This includes any reports, notices or postings made by any other party on which Hybrid Org relied for its own notice to *individual*s, agencies, authorities, or media. These records are be kept for a minimum of six years following the provision of the notice, report or posting.

RELEVANT HIPAA REGULATIONS:
45 CFR 164.404 *Notification to Individuals*
45 CFR 164.406 *Notification to the Media*
45 CFR 164.408 *Notification to the Secretary*
45 CFR 164.410 *Notification by a Business Associate*
45 CFR 164.412 *Law Enforcement Delay*
45 CFR 164.414 *Administrative Requirements and Burden of Proof*
45 CFR 164.530 *Administrative Requirements*

Privacy Policy 8.0 Sanctions/Discipline

FULL POLICY LANGUAGE:

Policy Purpose:

To ensure that appropriate sanctions will be applied to *Responsible Employees* who violate the requirements of the *HIPAA* Privacy Rule, **Hybrid Org's** *HIPAA* privacy policies and procedures, the *HIPAA Breach* Notification Rule and/or **Hybrid Org's** *HIPAA Breach* Notification Rule policies and procedures.

Policy Description:

It is **Hybrid Org's** policy to impose sanctions, as applicable, for violations of **Hybrid Org's** policies and procedures regarding *Responsible Employee HIPAA* compliance. **Hybrid Org** utilizes the directives of the Vontier Employee Handbook for US Employees to determine if a sanction is appropriate and documents all sanctions. The *Privacy Official* is ultimately responsible for the

determination of appropriate sanctions and may involve human resources in any decision. In deciding upon the appropriate sanction, **Hybrid Org** may review the severity of the violation, the impact of the violation, and the *Responsible Employee's* work history. The *Privacy Official*, in his or her discretion, may review the sanction decision at the request of a *Responsible Employee.*

Hybrid Org will not impose discipline against any *Responsible Employee* or *Business associate* for disclosing *PHI*, if the person believes in good faith either that **Hybrid Org** has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care or services provided by **Hybrid Org** potentially endanger one or more *individual*s, workers, or the public; **and** the disclosure is either to a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct of **Hybrid Org.**

Procedures:

Sanctions:

Responsible Employees who violate Hybrid Org's privacy policy and procedures may be subject to sanctions per the Vontier Employee Handbook for US Employees. Following the report or discovery of a *HIPAA* incident, the *Privacy Official*, in conjunction with the Benefits Team and Human Resources team when appropriate, may impose sanctions against any *Responsible Employee* who was found to have violated the requirements of the *HIPAA* Privacy Rule, **Hybrid Org's** *HIPAA* privacy policies and procedures, the *HIPAA Breach* Notification Rule and/or **Hybrid Org's** *HIPAA Breach* Determination/Notification Rule policies and procedures.

Upon receipt or report of an allegation that an *individual* has been subjected to intimidation or retaliation, the *Privacy Official* shall investigate, and upon conclusion of the investigation, shall impose appropriate sanctions. See Privacy Policy 1.0: *HIPAA Privacy Program: General* for a discussion of prohibited intimidation and retaliation.

Fair and Consistent Discipline

The *Privacy Official* shall consistently apply corrective disciplinary action when warranted, up to and including termination of employment or contracts. Whenever appropriate, progressive discipline will be applied. Sanctions imposed will be consistent, and proportional with the severity of the offense with like violations under similar fact patterns treated equally.

Facts and Circumstances that May be Considered in Making Disciplinary Decisions

Hybrid Org will consider the type and severity of the violation, factors that mitigate or increase the appropriate sanction and any other pertinent facts relative to the violation at issue.

Type of Offense	**Examples**
Willful Intentional Violation	Sale of *PHI*, Identity theft
Violation with Harmful Intent	Malice, disclosure of a condition with an intent to harm or embarrass; Disclosure of a Mental Health condition
Deliberate Violation without harmful intent (Curiosity)	Looking up a friend's *personal information*
Failure to Follow Policies and Procedures	Violation due to poor job performance such as not seeking appropriate authorization before releasing records; failure to send messages through secure portals or secure email/Kiteworks
Accidental or Inadvertent Violations	Violations due to human error such as misdirecting an electronic communication due to a typo

Factors to consider that Might Mitigate or Increase Appropriate Sanction
Violation included sensitive information, e.g., *Records included Mental health Condition, Substance Abuse Records*
High volume of data impacted, e.g. *A entire record containing extensive PHI was impacted rather than one or two data points*
High number of *individuals* impacted
Breach resulted from violation
Hybrid Org incurred significant expense as a result of the violation, e.g, *Hybrid Org bore the expense of an extensive investigation and breach notification*
Harm to an individual resulted from the violation
Responsible Employee was not forthcoming or honest during investigation
Responsible Employee reported the incident themselves
History of Performance Issues for Individual
Failure of Training, e.g., *Individual had not been offered all training before violation occurred*
Action taken at request of individual in authority
Training Understood but ignored
Long Job Performance, exemplary employee

Examples of Appropriate Types of Discipline to Consider

Hybrid Org may impose appropriate sanctions for violations. The penalty should be more stringent for repeat offenses and intentional or malicious violations. Sanctions and discipline up to and including termination of employment or contracts may be appropriate even for first violations. Hybrid Org considers the follow as appropriate sanctions:

Verbal or Written Reprimand
Retraining on Privacy/security awareness
Retraining on privacy/security policies and procedures
Retraining on Proper Use of Forms
Letter of Reprimand
Probationary status
Suspension
Unpaid Leave
Final Warning
Longer term Suspension
Termination of Employment or Contract

Appeals:

1. In the event that a sanction triggers any process of appeal under an applicable **Hybrid Org** disciplinary policy and procedure, the *Responsible Employee* is entitled to file an appeal. The *Privacy Official* or other appropriate individual shall review the appeal, which shall be in writing, and shall render a decision upon such appeal.
2. In the event that the party hearing the appeal is not authorized by **Hybrid Org** or *HIPAA* regulations to *access PHI*, the identity of the *individual* whose privacy rights were violated shall be removed to the extent feasible or, if that is not possible, other measures must be taken to ensure *HIPAA* compliance prior to providing the party with *PHI*.

Documentation of Disciplinary Actions:

1. **Hybrid Org** shall document all disciplinary action, including:
    a. All information about the nature of the violation;
    b. The names and roles of the parties who played a role in determining the disciplinary action;
    c. The facts and circumstances considered in determining the disciplinary action (without regard to whether such considerations were relied upon in determining the disciplinary action);
    d. The discipline imposed (including lack of discipline);
    e. The nature of the appeals process used, if any, and the results thereof; and
    f. The actions taken in order to enforce the discipline.
2. Such documentation shall be retained in accordance with **Hybrid Org's** document retention policies, and, in any event, for no less than six years.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.530(e) *Sanctions*

Privacy Policy 9.0 Business Associates

FULL POLICY LANGUAGE:

Policy Purpose:

The purpose of this policy is to meet **Hybrid Org's** responsibility to determine whether a vendor is a *business associate* as defined by the *HIPAA* regulations and to provide rules for creation, content, maintenance, and termination of *business associate agreement*s that establish protections for the privacy and accessibility of protected health information created, received, maintained, or transmitted on **Hybrid Org's** behalf and meet the requirements of the Privacy Rule.

Policy Description:

It is the policy of the Hybrid Org to determine which of its vendors are *business associates*, to enter into *Business associate agreement*s containing all the required elements to protect the privacy of health information, to provide rules for creation, maintenance, and termination of *Business associate agreement*s, and to provide for rules regarding the use and disclosure of information and the reporting of uses or disclosures not provided for in the *Business associate agreement*.

A *business associate* is an individual or entity that provides a service, performs a function, or performs an activity on behalf of a *covered entity* that involves the creation, receipt, maintenance or transmission of protected health information, including but not limited to claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, individual safety activities, billing, benefit management, practice management, repricing, legal representation and accounting. *Business associates* do not include *members* of the **Hybrid Org's** *workforce*. A *Business associate agreement* is a legally binding contract, in which, the *business associate* provides, in writing, satisfactory assurances that it will appropriately safeguard the information it creates, receives, maintains or transmits in carrying out specified functions or activities for a *covered entity* as well as agreeing to provide *access* and *amendment* to records, and reporting of *breach*es and incidents. **Hybrid Org** may only disclose protected health information (*PHI*) to a *business associate* after a valid *business associate agreement* is in place. Examples of business associates are bswift, United Healthcare and Cigna Dental.

Procedures:

***Business associate* Determination:**
Hybrid Org shall inventory all outside business and service vendors to determine if they are *business associates*. For a vendor to be considered a *business associate*, the following requirements must be met:

- The vendor/business' staff *members* are not *members* of **Hybrid Org's** *workforce*;
- The vendor/business is performing a function, service or activity on behalf of the **Hybrid Org**; and
- That "something" involves the *access* to, creation, receipt, maintenance or transmission of *PHI*.

To make the *business associate* determination, **Hybrid Org** inventories all existing business and service vendors to determine if they are *business associates*. It also makes such a determination for any new vendors engaged by Hybrid Org prior to entering into an agreement for services, function or activity with the vendor.

Hybrid Org enters into *Business associate agreement*s for all vendors identified as *Business associates* unless the circumstances discussed below in Other Requirements for Contracts and other Arrangements apply.

***Business Associate* Contracts/Agreements:**
If an entity is determined to be a *business associate*, then the Hybrid Org must require a *business associate agreement* that provides in writing satisfactory assurances that it will appropriately safeguard the information it receives, uses, or discloses in carrying out the specified functions or activities.

The satisfactory assurances obtained from the *business associate* must, at a minimum, contain the provisions specified in the Privacy Rule, provisions that:

1. Establish the permitted and required uses and disclosures of protected health information by the *business associate* and not allow the *business associate* to further use or disclose information in manner that would violate the Privacy Rule;
2. Provide that the *business associate* will not use or further disclose the information other than as permitted or required by the contract or as required by law;
3. Require the *business associate* to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the *HIPAA* Security Rule regarding electronic protected health information, including administrative, technical and physical safeguards;
4. Require the *business associate* to train its *workforce* on the *HIPAA* Security Rule, and on the provisions of the *HIPAA* Privacy Rule with which *Business associate* must comply in the performance of the agreement with the *covered entity;*
5. Require the *business associate* to timely report to the *covered entity* any use or disclosure of the information not provided for by its contract of which it becomes aware, including *breach*es of *unsecured PHI*;
6. Ensure that any subcontractors of *business associate* that create, receive, maintain or transmit protected health information on behalf of the *business associate* agree to the same restrictions and condition that apply to the *business associate* with respect to such information;

7. Require the *business associate* to disclose protected health information as specified in its contract to satisfy **Hybrid Org's** obligation with respect to *individual*s' requests for *access* or copies of their protected health information;
8. Make protected health information available for *amendment* and incorporate any *amendment*s as required or when appropriate, if allowed under the 45 CFR 164.526;
9. Make available the information required for an *accounting of disclosures*;
10. To the extent the *business associate* is to carry out **Hybrid Org's** obligation(s) covered under the Privacy Rule, the agreement must require the *business associate* to comply with the requirements that apply to the *covered entity* in the performance of the obligation;
11. Require the *business associate* to make available to *HHS* its internal practices, books, and records relating to the use and disclosure of protected health information received from, created, or received by the *business associate* on behalf of **Hybrid Org** for purposes of *HHS* determining **Hybrid Org's** compliance with the *HIPAA* Privacy Rule;
12. At termination of the contract, if feasible, require the *business associate* to return or destroy all protected health information received from, created, or received by the *business associate* on behalf of **Hybrid Org** that it still maintains in any form and retain no copies of such information, or, if destruction is not feasible, extend all of the protections of the contract to the information and limit further use and disclosures of such information to those purposes that make return or destruction of the information infeasible; and
13. Authorize termination of the contract by the **Hybrid Org** if the *business associate* violates a material term of the contract as determined by the Hybrid Org. This term may be omitted if it is inconsistent with statutory obligations of either the Hybrid Org or its *business associate*.

Other requirements for Contracts and Other Arrangements

If the Hybrid Org and the *business associate* enter into a Data Use Agreement that meets the requirements set forth at 45 CFR 164. 514(e)(4) and 164.314(a)(1), if applicable, the Hybrid Org is in compliance with the Privacy rule if it only discloses a *limited data set* to the *business associate* for them to carry out a healthcare operation function.

In the Event of Material *Breach* or Violation or a Pattern or Practice that violates the *Business associate agreement*:

If **Hybrid Org** knows of a material *breach* or violation by the *business associate* of the contract or agreement, the **Hybrid Org** is required to ensure that *business associate* takes reasonable steps to cure the *breach* or end the violation. If such steps are unsuccessful, the **Hybrid Org** must terminate the contract or agreement. If termination of the contract or agreement is not feasible, the **Hybrid Org** must report the problem to the Secretary of the Department of Health and Human Services (*HHS*).

Responsible Employees shall immediately notify the **Hybrid Org's** *Privacy Official* if and when they learn that a *business associate* may have *breach*ed or violated its *business associate agreement*.

A *business associate* of **Hybrid Org** may use or disclose *PHI* only as permitted or required by its *business associate agreement* with the **Hybrid Org**.

1. A *business associate* may not use or disclose *PHI* in a manner that would violate the Privacy Rule, if done by the **Hybrid Org**, except:
    a. If the *business associate* contract permits the business to use and disclose protected health information for the proper management and administration of the *business associate*; or

   b. If such uses or disclosures are lawfully permitted by the *business associate agreement*.
2. A *business associate* is required to disclose *PHI*:
   a. When required by the *HHS* Secretary to investigate or determine the *business associate's* compliance with *HIPAA*.
   b. To the **Hybrid Org**, if the *PHI* is the subject of a request for *access* and is maintained in electronic *designated record set*s. Under such circumstances, if an *individual* requests an electronic copy of such information, the *business associate* must provide the **Hybrid Org** with *access* to the *designated record set*s, so that the **Hybrid Org** can provide the *individual* (or the *individual*'s designee) with the requested *access*.

RELEVANT HIPAA REGULATIONS:

45 CFR 160.103 *Business Associate Definition*
45 CFR 164.502(a)(3)-(4) *Permitted and Required Uses and Disclosures; Business Associates*
45 CFR 164.504(e) *Standard Business Associate Contracts*

Privacy Policy 10.0 Notice of Privacy Practices

FULL POLICY LANGUAGE:

Policy Purpose:

*Individual*s are entitled to adequate notice of the uses and disclosures of protected health information and of their rights and Hybrid Org's responsibilities with respect to *PHI* unless an exception applies. The Privacy Rule requires **Hybrid Org** to describe its privacy practices in plain English, in a document called a Notice of Privacy Practices ("Notice").

Policy Description:

Hybrid Org makes its Notice available to all *individual*s on its SharePoint site or through US mail, by request. The Notice contains permitted uses and disclosures; uses and disclosures that require an opportunity for them to agree or object; uses and disclosures that require an authorization; whether the **Hybrid Org** intends to use or disclose information for marketing, facility directories or *fundraising*; the *individual*'s rights to *access*, *amendment*, and limitations on sharing; the **Hybrid Org's** responsibilities; a way to make complaints; contact details for further information; and an effective date.

Revisions to the Notice of Privacy Practices:

1. The **Hybrid Org** revises and distributes its Notice whenever there is a material change to privacy practices, including practices regarding *PHI* uses and disclosures, *individual*'s rights, and **Hybrid Org** legal duties, or other privacy practices stated in the Notice.
2. **Hybrid Org** makes any revised Notice available on its SharePoint site and through US mail, by request.

Record Retention:

All versions of the **Hybrid Org** approved Notice of Privacy Practices are archived and maintained by the *Privacy Official* for a period no less than six (6) years from the date of creation or the date when it was last in effect, whichever is later.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.520 *Notice of Privacy Practices for protected health information*

Privacy Policy 11.0 Uses and Disclosures: General Rules

FULL POLICY LANGUAGE:

Policy Purpose:

To outline the general rules for when and how **Hybrid Org** can use or disclose *PHI*.

Policy Description:

It is the policy of this **Hybrid Org** to only use or disclose protected health information as permitted or required under the Privacy Rule and rules regarding compliance with the Privacy rule. *Responsible Employees* are trained on the circumstances in which use, or disclosure of *PHI* is permitted or required. If in question, they should seek clarification before sharing information.

Hybrid Org will not use or disclose information in circumstances where use and disclosure is allowed unless all the administrative requirements applicable to that use or disclosure (examples include agreement of the *individual*, authorization, or confirmation of a legal requirement to disclose) have been met.

Procedures:

Permitted Uses and Disclosures:

Hybrid Org *may* (i.e., is permitted under law) use or disclose protected health information as follows:

1. To the *individual*.
2. To its own *workforce* and other parties, for the purposes of *treatment*, *payment*, or *health care operations* of the Hybrid Org (see Privacy Policy 13.0: *Uses and Disclosures: No Authorization or. Right to Agree or Object Required* paragraphs on use of *PHI* for *Treatment*, *Payment* and *Health care operations*)
3. Incident to a use or disclosure that is otherwise permitted, provided **Hybrid Org** complies with the requirements of this Policy 11.0: *General Rules for Uses and Disclosures*; Privacy Policy on *Minimum Necessary Standard* (See Privacy Policy 3.0: *Minimum Necessary Standard*) and the requirements of Privacy Policy 2.0: *Administrative, Technical and Physical Safeguards of PHI* and any other policy that applies in the specific circumstances.
4. Pursuant to, and in compliance with, a valid written authorization (see Privacy Policy 15.0: *Individual Right: Access to Protected Health Information* and Privacy Policy 13.0 *Uses and Disclosures: Authorization Required and Requirements for Valid Authorization* for details). Use of genetic information for underwriting purposes remains prohibited.
5. Pursuant to an agreement under, or as otherwise permitted by, Privacy Policy 16.0: *Individual Right: Request Restrictions and Alternate Confidential Communications*. When **Hybrid Org** agrees to a restriction pursuant to Privacy Policy 16.0: *Individual Right: Request Restrictions and Alternate Confidential Communications*, **Hybrid Org** may not use *PHI* covered by the restriction in violation of that restriction.
6. As permitted by any applicable rule or regulation.

Required Uses and Disclosures:

Hybrid Org *must* (i.e., is required to, under the law) and will disclose *PHI*:

1. To an *individual*, pursuant to that *individual*'s request under the Privacy Rule Right of *Access* Standard (45 CFR 164.524), or the Accounting of *PHI* Disclosures Standard (45 CFR 164.528). See Privacy Policy 15.0: *Individual's Right to Access Protected Health Information* and Privacy Policy 18.0: *Individual Right: Accounting of disclosures* for further details.

2. When required by the *HHS* Secretary to investigate or determine **Hybrid Org's** compliance with *HIPAA* and the Privacy Rule. (45 CFR 160.310).

Prohibited Uses and Disclosures:
Hybrid Org is prohibited from using and disclosing *PHI*, as follows:

Prohibited: Sale of Protected Health Information

Hybrid Org may not and will not sell protected health information. For further details about valid authorizations for use of *PHI* for the marketing of information and what is included and excluded from *HIPAA*'s definition of marketing of *PHI*, refer to the paragraphs on marketing within Privacy Policy 13.0: *Uses and Disclosures: Authorization Required and Requirements for Valid Authorization*.

Prohibited: Use and Disclosure of Genetic Information for Underwriting Purposes

Health plans: Hybrid Org will not use or disclose *PHI* that is genetic information for underwriting purposes. Underwriting purposes include rules for, or determination of, eligibility for, or determination of, benefits under a health plan or policy; computation of premium amounts; the application of a pre-existing exclusion; and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits. Underwriting does not include determinations of medical appropriateness for *individual*s seeking a benefit under a plan, coverage or policy.

Uses and Disclosures: Agreed Upon Restriction
Hybrid Org will not use or disclose information in violation of a restriction it has agreed to unless required to do so (for example, by a valid subpoena or the need to avert harm to the public or an *individual*). For further details on **Hybrid Org's** policy and procedure concerning requested restrictions see Privacy Policy 16.0: *Individual Right: Request Privacy Restrictions and alternate Confidential Communications* for *PHI*.

De-Identified *PHI*: Creation, Use and Disclosures:
1. **Hybrid Org** may use *PHI* to create information that is not *individually identifiable health information* or disclose protected health information to a *business associate* for the purpose of de-identification.
2. If Hybrid Org decides to de-identify information, it will do so in accordance with standard implementation specifications for de-identification under 45 CFR 164.514(a) and 45 CFR 164.514(b).

Disclosures to *Business associates* (See above for Use and Disclosure *by Business associates* and also Privacy Policy 9.0: *Business Associates*)

Deceased *Individuals*:
The *HIPAA* Privacy Rule applies to the *PHI* of a deceased *individual* for a period of 50 years following the person's death. During the 50-year period of protection, the Privacy Rule generally protects a decedent's health information to the same extent the Rule protects the health information of living *individuals*.

The Privacy Rule includes a number of special disclosure provisions relevant to deceased *individuals*. The following disclosures may be made within the 50-year period following the individual's death:

1. To alert law enforcement to the death of the *individual*, when there is a suspicion that death resulted from criminal conduct.
2. To coroners or medical examiners and funeral directors.
3. For *research* that is solely on the protected health information of decedents.
4. For entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation.
5. To a family *member* or other person who was involved in the *individual*'s health care or *payment* for care prior to the *individual*'s death, unless doing so is inconsistent with any prior expressed preference of the deceased *individual* that is known to **Hybrid Org**.

For disclosure of *PHI* of a deceased person that is not covered under those enumerated above, **Hybrid Org** will obtain written consent from an authorized representative for disclosure to be permitted. Refer to the paragraph on deceased *individual*'s *personal representative*s below to determine who is authorized.

***Personal representatives*:**

Hybrid Org will treat a *personal representative* as the *individual* for purposes of the Privacy Rule with some exceptions to this general rule regarding unemancipated minors and circumstances involving suspected or known abuse, neglect and endangerment. When deciding how to use and share a minor's *PHI*, *Responsible Employees* must first refer to Privacy Policy 20.0: *Minors' Rights* for more specific direction. For *personal representative*s of deceased *individual*s see last paragraph below.

Hybrid Org may decide not to treat an *individual* as a *personal representative* in situations of known or suspected violence, abuse, neglect or endangerment, even if other laws dictate that it is appropriate or required to treat an *individual* as a *personal representative*. For the **Hybrid Org** to elect *not to treat* a person as a *personal representative*, *Responsible Employees* must document that:

1. Hybrid Org, exercising professional judgment, decides it is not in the best interest of the *individual* to do so ***and***
2. Hybrid Org has a reasonable belief that ***either:***
    a. the *individual* has been or may be subjected to domestic violence, abuse or neglect by that person; or
    b. treating the person as the *individual*'s *personal representative* will or could endanger the *individual*.

Confidential Communications:

Hybrid Org complies with the applicable requirements of 45 CFR 164.522(b) in communicating *PHI*. Hybrid Org permits *individual*s to request, and accommodates reasonable requests by *individuals* to receive communications of *PHI* by alternative means or at alternative locations. See Privacy 16.0**:** *Individual Right: Request Restrictions and Alternate Confidential Communications* for *PHI* for more details on how Hybrid Org handles such requests.

Uses and Disclosures: More Stringent Federal or State Law

Hybrid Org complies with privacy and confidentiality requirements, including administrative requirements such as obtaining specific *individual* authorizations, from sources other than HIPAA.

HIPAA does not preempt, and accordingly **Hybrid Org** follows, stricter federal and state requirements applicable to an *individual's PHI*. Examples of where stricter requirements are often present include state mental health record protections (in addition to HIPAA's strict psychotherapy record requirements), substance use disorder (SUD) records, including sharing for treatment purposes (see federal SAMSHA guidance), rules regarding public health activities, rules regarding gender reassignment and rules specific to deceased individuals and minors.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.502 *Uses and Disclosures of Protected Health Information: General Rules*
45 CFR 164.501 *Definitions*
45 CFR 160.203 *General Rule and exceptions*

Privacy Policy 12.0 Uses and Disclosures Requiring Individual an Opportunity to Agree or Object

FULL POLICY LANGUAGE:

Policy Purpose:

To meet Hybrid Org's responsibility under several circumstances, to only use or disclosure *PHI* after an *individual* has been given the opportunity to agree or to prohibit or restrict the use or disclosure, and to inform *Responsible Employees* of the situations under which an *individual* must be given an opportunity to agree or object and how to meet the requirements.

Policy Description:

Under several circumstances, before **Hybrid Org** may use or disclose an *individual*'s *PHI*, the *individual* must be given an opportunity to agree or object to the use or disclosure:

1. use and disclosure of *PHI* by the Hybrid Org for purposes of a *directory*,
2. disclosure of *PHI* to a person that is directly relevant to that person's involvement with an *individual*'s care including *payment* for that care,
3. limited disclosure for notification of an *individual*'s location, general condition, or death,
4. uses and disclosures for disaster relief purposes, and
5. uses and disclosures when an *individual* is deceased (prior prohibition on disclosures must be honored).

It is the policy of the **Hybrid Org** that it will meet its responsibility to provide *individual*s the right to agree or object to uses and disclosures as required. Under each of these circumstances there are additional administrative requirements that must be met such as what to do if the *individual* is not present, when it is appropriate to exercise professional judgment and what is allowed in emergency circumstances that may not be allowed in the absence of an emergency. Special requirements that might apply in situations involving minors or other requirements like disclosures made pursuant to legal process may override the rights of an *individual* to agree or object. For details on such requirements please see the various Privacy Policies addressing those circumstances: Privacy Policy 20: *Minors' Rights*; Privacy Policy 22.0: *Uses and Disclosures: Response to Judicial and Administrative Proceedings*: Privacy Policy 11.0: *Uses and Disclosures: General Rules*.

Any *Responsible Employee* who is unsure of appropriate use or disclosure should seek direction prior to making a disclosure. *Responsible Employees* should follow the procedures below.

Procedures:

Uses and Disclosures Requiring an Opportunity for the *Individual* to Agree or to Object:

The **Hybrid Org** may orally inform the *individual* of and obtain the *individual*'s oral agreement or objection to a use or disclosure permitted by this section. *Responsible Employees* should note any oral objection or agreement in the *individual*'s record.

If an *individual* expresses a desire to prohibit the use or disclosure, Hybrid Org will record that objection in the record and abide by that request. If the *individual* desires to restrict the disclosure in some way, the Hybrid Org will record that restriction in the *individual*'s record and abide by that request. *Responsible Employees* will review any objections or prohibitions in the record or ask the *individual* (if they are available) before using or disclosing information in the circumstances defined above.

*Individual*s may change their decision. For any use or disclosure made after the *individual* has changed their decision, Hybrid Org will abide by any new restrictions or prohibitions or any new agreement to a use or disclosure with an understanding that there may be a slight administrative delay in implementing some changes. If a *Responsible Employee* anticipates a delay, they will notify the *individual* of said possibility.

Uses and Disclosures for Involvement in the *Individual*'s Care and Notification Purposes:
Permitted uses and disclosures to those involved in the *individual*'s *payment* for their care and for notification purposes:

1. The **Hybrid Org** may disclose to a family *member*, other relative, or a close personal friend of the *individual*, or any other person identified by the *individual*, the *PHI* directly relevant to such person's involvement with the *individual*'s health care or *payment* related to the *individual*'s health care.
2. The **Hybrid Org** may use or disclose *PHI* to notify or assist in the notification of (including identifying or locating), a family *member*, a *personal representative* of the *individual*, or another person responsible for the care of the *individual* of the *individual*'s location, general condition, or death.

Limited Use or Disclosure: If the *individual* is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the *individual*'s incapacity or an emergency circumstance, the **Hybrid Org** may disclose information using professional judgment in some circumstances and may also use knowledge of common practices in others.

Uses and Disclosures for Disaster Relief Purposes: The **Hybrid Org** may use or disclose *PHI* to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities. The uses or disclosures must only be to notify or assist in the notification of (including identifying or locating), a family *member*, a *personal representative* of the *individual*, or another person responsible for the care of the *individual* of the *individual*'s location, general condition, or death. Any such disclosure must respect the *individual*'s right to agree or object to such disclosure, including a) respecting any request for restricted use made prior to an *individual*'s death and b) following the process for use and disclosure for notification purposes when 1) the *individual* is present and 2) when the *individual* is not present as set forth above.

Uses and disclosures when the *individual* is deceased: If the *individual* is deceased, the **Hybrid Org** may disclose to a family *member*, or other persons identified in this section who were involved in the *individual*'s care or *payment* for health care prior to the *individual*'s death, *PHI* of the

individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the *individual* that is known to the **Hybrid Org**.

RELEVANT HIPAA REGULATIONS:
45 CFR 164.510 *Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object*

Privacy Policy 13.0 Uses and Disclosures: Individual Authorization Required and Requirements for a Valid Authorization

FULL POLICY LANGUAGE:

Policy Purpose:

Hybrid Org will obtain and require valid written *individual* authorization before it uses or discloses information in the circumstances described in this policy and as required under the Privacy Rule.

Policy Description:

Generally, **Hybrid Org** may not use or disclose *PHI* without a valid written authorization from the *individual* who is the subject of the information, unless otherwise allowed under the Privacy Rule. When the *individual* provides a valid authorization, Hybrid Org's use and disclosure of the information must be consistent with the authorization. *Responsible Employees* must be familiar with the requirements of a valid authorization and the situations which require that authorization be obtained prior to use or disclosure of information and must follow the terms of the authorizations that are in place. See Privacy Policy 19.0: *Use and Disclosure: No Authorization or Right to Agree or Object* for more detail on situations in which an authorization is not required. A sample Authorization is available and can be requested through HIPAAinquiry@vontier.com.

Hybrid Org allows revocation of authorizations in writing with some minor exceptions as further detailed below. Hybrid Org will provide *individual*s with a copy of their authorizations. Hybrid Org will use and accept only valid authorization forms written in plain language which contain all the core elements and required statements for an authorization and will limit the use of compound authorizations to circumstances where they are allowed as detailed below. The **Hybrid Org** will also document and retain any signed authorization.

Hybrid Org will not condition the provision of *treatment*, *payment*, enrollment in a health plan, or eligibility for benefits on the provision of an *individual*'s authorization except in limited circumstances as allowed under the Privacy Rule and further described below.

Hybrid Org will meet the requirements for authorizations related to the sale of *PHI* and communications for marketing purposes.

Procedures:

Use only Valid Authorization Forms: Hybrid Org will use and accept only valid written authorization forms meeting the authorization requirements below. Hybrid Org will not accept any authorizations that include a defect. Hybrid Org will only use and accept compound authorizations in situations allowed under the Privacy Rule as described below in the Compound Authorization section.

Authorization Requirements: A valid authorization under *HIPAA* must be written in plain language and contain at a minimum the 6 core elements defined in the Privacy Rule and at least 3 required statements. A fourth statement is required if the authorization relates to the use and

disclosure of *PHI* for marketing purposes. The content of this fourth statement is specific to the marketing of *PHI*. Hybrid Org requires that all authorizations that it uses or accepts contain all the required elements and statements.

Responsible Employees will be aware of these validity requirements and not use or disclose information under an authorization that is not valid. If a *Responsible Employee* has questions about the validity of any specific authorization or form, they should seek further information.

The Privacy Official will periodically review authorization forms used or accepted by Hybrid Org on a regular basis to assure they are valid and will review any new authorization form to be used by *Responsible Employees* to obtain authorizations before they are made available for use.

Core Elements and Requirements:
Generally, each authorization must contain a description of the information to disclose, who is authorized to disclose it, who is authorized to receive it, the purpose for the disclosure (or notation that it is at *individual*'s request), when it expires, and a signature. These core elements are set forth in more detail below.

Core Elements: A valid authorization will contain at least the following elements (but may contain additional information so long as it does not create an inconsistency in the document):

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
3. The name or other specific identification of the person(s), or class of persons, to whom the **Hybrid Org** may make the requested use or disclosure;
4. A description of each purpose of the requested use or disclosure. The statement "at the request of the *individual*" is a sufficient description of the purpose when an *individual* initiates the authorization and does not, or elects not to, provide a statement of the purpose;
5. An expiration date or an expiration event that relates to the *individual* or the purpose of the use or disclosure. The statement "end of the *research* study," "none," or similar language is sufficient if the authorization is for a use or disclosure of *PHI* for *research*, including for the creation and maintenance of a *research* database or *research* repository; and
6. Signature of the *individual* and date. If the authorization is signed by a *personal representative* of the *individual*, a description of such representative's authority to act for the *individual* must also be provided.

Required Statements
In addition to the core elements, authorizations must contain at least three statements. The general topics are an *individual*'s ability to revoke the authorization in writing including exceptions to that right; whether there is a prohibition on the conditioning of *treatment*, *payment*, enrollment or eligibility for benefits on the authorization and, when there is no prohibition, the consequences for the *individual* if they refuse to sign; and the potential that information will be redisclosed by the recipient without protection if the *individual* signs the authorization. The statements required are further detailed below:

Three Statements to be Included in All Authorizations:
Statements must be adequate to place the *individual* on notice of all of the following:

1. The *individual*'s right to revoke the authorization in writing, and either:

   a. A description of how the *individual* may revoke the authorization and any exceptions to that right (Please see below for details on exceptions to the right to revoke); or
   b. A referral to the Notice of Privacy Practices if a description of how to revoke and the exceptions to that right are covered in that Notice of Privacy Practices.
2. The ability or inability to condition *treatment*, *payment*, enrollment or eligibility for benefits on the authorization, by stating either:
   a. The **Hybrid Org** (or other *covered entity* if reviewing an authorization from a different entity) may not condition *treatment*, *payment*, enrollment, or eligibility for benefits on whether the *individual* signs the authorization when the prohibition on conditioning of authorizations applies (please see below for details on when this prohibition applies); or
   b. The consequences to the *individual* of a refusal to sign the authorization when the prohibition does not apply (i.e., for *research*, health plan eligibility, underwriting purposes, and risk rating determinations) - the **Hybrid Org** or the *covered entity* from whom **Hybrid Org** is accepting an authorization, can condition *treatment*, enrollment in a health plan, or eligibility for benefits on failure to obtain such authorization; and
3. The potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer be protected by *HIPAA* privacy rules.

Additional Authorization Statement Requirements for Marketing of *PHI*:
For any authorization related to the sale of *PHI* or the use or disclosure of *PHI* for marketing purposes, a fourth statement must be included for the authorization to be valid.

Defective Authorizations: An authorization is not valid, and the **Hybrid Org** will not use or accept it if the document submitted has any of the following defects:
1. It is expired: the expiration date has passed, or the expiration event is known by the **Hybrid Org** to have occurred;
2. It is incomplete: the authorization has not been filled out completely, with respect to an element described by this policy, if applicable;
3. It is revoked: the authorization is known by the **Hybrid Org** to have been revoked;
4. The authorization is defective, it is an invalid compound authorization or it conditions *treatment*, *payment*, enrollment or eligibility for benefits on the authorization inappropriately or without the correct statement regarding that condition; and
5. Any material information in the authorization is known by the **Hybrid Org** to be false.

Prohibition on Conditioning of Authorizations with Exceptions
The **Hybrid Org** will not condition *treatment*, *payment*, or enrollment in a health plan, or eligibility for benefits on the provision of an authorization, except in the following circumstances allowed under the Privacy Rule:
1. The **Hybrid Org,** only when acting in the capacity of a health plan, may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan *prior to* an *individual*'s enrollment in the health plan, if:
   a. The authorization sought is for the health plan's eligibility or enrollment determinations relating to the *individual*, or for its underwriting or risk rating determinations; or
   b. The authorization is not for a use or disclosure of *psychotherapy notes*.

2. The **Hybrid Org** may require an authorization for release of information to a third party before providing health care that is solely for the purpose of creating *PHI* for disclosure to a third party.

Revocation of Authorizations
An *individual* may revoke an authorization at any time, provided that the revocation is in writing, and **Hybrid Org** will respect that revocation except to the extent that:
1. The **Hybrid Org** has taken action in reliance thereon; and
2. If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy, or the policy itself.

Circumstances in Which an Authorization is Specifically Required under the Privacy Rule

The Privacy rule contains special provisions related to authorizations and the sale of *PHI* in all circumstances and for the use or disclosure of Psychotherapy records, and the use or disclosure of *PHI* for marketing purposes, in most circumstances. Hybrid Org will require authorizations in all instances where it is required as further described below and in Privacy Policy 19.0: *Psychotherapy notes.*

***Psychotherapy notes*: Hybrid Org** utilizes an Authorization for the use or disclosure of *psychotherapy notes* specific to the *psychotherapy notes* and may not combine the authorization with any other consent or authorization except for another authorization for the use or disclosure of *psychotherapy notes*.

For the details on what *psychotherapy notes* are, who may *access* them, the limited circumstances in which they can be released with an authorization, and releases that are allowed without obtaining an *individual* authorization, refer to Privacy Policy 19.0: *Psychotherapy notes* which details the appropriate *treatment* of these records.

Marketing: Hybrid Org may use or disclose *PHI* for certain marketing purposes and for broader marketing purposes with authorization as set forth below.

Authorization to Use or Disclose *PHI* for Marketing Purposes:
1. The **Hybrid Org** shall obtain written authorization for any use or disclosure of *PHI* for marketing, except if the communication is in the form of:
    a. Face-to-face communication with the *individual*;
    b. A promotional gift of nominal value provided by the **Hybrid Org**.
    c. communications only about government or government sponsored programs; or
    d. communications promoting health in general and not promoting a product or service or particular *provider*.
2. If the marketing involves the **Hybrid Org's** receiving direct or indirect remuneration from a third party, written authorization is required. If the marketing activity involves remuneration, Hybrid Org will reflect that remuneration in the authorization.

What is Marketing under the Privacy Rule? Hybrid Org will make determinations about what activities it undertakes that fall within the Privacy Rule's definition of marketing. No *Responsible Employee* shall engage in any activity that might be marketing before determining whether it falls within this definition to assure that any necessary authorizations are in place prior to the use or disclosure of *PHI* for which an authorization is required.

Any activity is considered "marketing "under the Privacy Rule when it is a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service UNLESS it is specifically excluded from the definition. An activity can but does not have to involve remuneration to be considered marketing. If the activity is marketing and involves remuneration, Hybrid Org will reflect that remuneration in the authorization.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.508 *Uses and Disclosures for Which an Authorization is Required*
45 CFR 501 *Definitions*

Privacy Policy 14.0 Uses and Disclosures: No Authorization or Right to Agree or Object Required

FULL POLICY LANGUAGE:

Policy Purpose:

To set forth rules regarding when **Hybrid Org** may use or disclose *individual* protected health information (*PHI*) without first having to a) obtain written authorization or b) allowing the *individual* an opportunity to agree or object. To set forth requirements for when the Hybrid Org may be required to inform the *individual* of the use or disclosure and the *individual* may agree to the use or disclosure. To set forth the parameters for when the Hybrid Org may use and disclose *PHI* for *treatment*, *payment* and *health care operations*.

Policy Description:

Under several circumstances, the *HIPAA* Privacy Rule permits **Hybrid Org** to use or disclose *PHI* without written authorization or an opportunity to agree or object. Generally, written authorization or an opportunity to agree or object are *not* required when a use or disclosure is for *treatment*, *payment*, or healthcare operations purposes. In addition, a written authorization or an opportunity to agree or object are generally *not* needed when a law *requires* that **Hybrid Org** use or disclose certain *PHI*.

Procedures:

Use and Disclosure for *Treatment*, *Payment* and *Health care operations*

Each *Responsible Employee* should be familiar with what activities are included in *treatment*, *payment* and *health care operations* under the Privacy Rule. Also frequently referred to as TPO, it is very important to understand the scope of what is covered.

What is TPO under the Privacy Rule?

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

***Payment*:** Activities undertaken by a health care *provider* or health plan to obtain or provide reimbursement for the provision of health care.

Examples of *payment* activities include:

- eligibility of coverage determination,
- billing,

- claims management,
- collection activities,
- medical necessity determinations,
- risk adjustments,
- utilization review including precertification, preauthorization, concurrent and retrospective review of services, and
- disclosures to consumer reporting agencies (limited to specified identifying information about the *individual*, his or her *payment* history, and identifying information about the **Hybrid Org**).

Healthcare Operations: Any of the following activities of a *covered entity* to the extent that the activities are related to a covered function:

1. Quality assessment and improvement activities (including outcome evaluation and clinical guideline development); individual safety; population-based activities related to improving health or reducing health care costs, protocol development, case management and care coordination, contacting health care *providers* and recipients with information about *treatment* alternatives, related activities that do not include *treatment*;
2. Reviewing the competence, qualifications, performance of health care professionals, health plan performance, conducting health care training programs for students, trainees or practitioners under supervision for practice and improvement of skills; training of non-health care professionals, accreditation, certification, licensing, or credentialing;
3. Underwriting (excluding any use of genetic information), enrollment, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, ceding, securing or placing a contract for reinsurance of healthcare claim risks;
4. conducting or arranging for medical review, legal services, and auditing functions including fraud and abuse detection and compliance programs;
5. business planning and development including formulary development and administration, development or improvement of *payment* or coverage policies;
6. business management and general administrative activities of the entity which include but are not limited to:
    a. Management activities relating to implementation of and compliance with the Privacy Rule;
    b. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
    c. Resolution of internal grievances;
    d. The sale, transfer, merger, or consolidation of all or part of the *covered entity* with another *covered entity*, or an entity that following such activity will become a *covered entity* and due diligence related to such activity; and
    e. Consistent with the applicable requirements of creating de-identified health information or a *limited data set* and *fundraising* for the benefit of the *covered entity*.

Hybrid Org May Seek Consent for TPO Uses and Disclosures: While Hybrid Org may request an *individual*'s consent for the use of *PHI* for *treatment*, *payment* and *health care operations*, it may not condition the provision of services or insurance on the *individual* granting consent. **Hybrid Org** does not *require* consent for the use of *PHI* for *treatment*, *payment* and operations. The **Hybrid Org** may make an exception for this when such consent is specifically required by other legal requirements like in cases for *research* consents. Any consent provided by an *individual* for **Hybrid**

Org's use of *PHI* for TPO purposes will not be treated as an authorization and the consent does not permit otherwise prohibited sharing of *PHI*.

If an *individual* is asked for consent but declines to provide it, **Hybrid Org** may still utilize their *PHI* for TPO purposes unless otherwise prohibited by another provision of the Privacy Rule.

Hybrid Org's Uses and Disclosures for *Treatment Payment* and *Health care operations*
Hybrid Org permits use or disclosure of protected health information for *treatment*, *payment*, or *health care operations* as set forth below, provided that such use or disclosure is consistent with other applicable requirements of the Privacy Rule.

Hybrid Org permits use or disclose of protected health information:

1. for Hybrid Org's own *treatment*, *payment*, or *health care operations*.
2. for *treatment* activities of a health care *provider*.
3. to another *covered entity* or a health care *provider* for the *payment* activities of the entity that receives the information.
4. to another *covered entity* for *health care operations* activities of the entity that receives the information, if each entity either has or had a relationship with the *individual* who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:
    a. For a purpose listed in paragraph (1) or (2) of the definition of *health care operations* above; or
    b. For the purpose of health care fraud and abuse detection or compliance.

Other Uses and Disclosures Which Do Not Require Authorizations or Opportunities to Agree or Object prior to Hybrid Org's Use or Disclosure of *PHI*

For each of the following topics on use and disclosure listed below, Hybrid Org *Responsible Employees* will use and disclose *PHI* without the need for obtaining a valid authorization or providing an *individual* the opportunity to agree or object following the parameters detailed for each topic.

Uses and Disclosures Required by law
Uses and Disclosures for Public Health Activities
Disclosures About Victims of Abuse, Neglect, or Domestic Violence
Uses and Disclosures for Health Oversight Activities
Uses and Disclosures for Judicial and Administrative Proceedings (See Privacy Policy 22.0)
Uses and Disclosures for Law Enforcement Purposes
Uses and Disclosures About Decedents
Uses and Disclosures for *Research* Purposes
Uses and Disclosures to Avert a Serious Threat to Health or Safety
Uses and Disclosures for Specialized Government Functions
Uses and Disclosures for Workers Compensation (See Privacy Policy 24.0)
Permitted Disclosures by Whistleblower
Permitted Disclosures by *Responsible Employee* Crime Victims
Permitted Disclosures Military and Veterans Activities

Uses and Disclosures Required by Law:

1. **Hybrid Org** will use or disclose *PHI* to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.
2. **Hybrid Org** will follow the specific *HIPAA* parameters for disclosure related to:
    a. Disclosures about victims of abuse, neglect, or domestic violence;
    b. Disclosures for judicial and administrative proceedings; and
    c. Victims of a crime.

Uses and Disclosures for Public Health Activities: The **Hybrid Org** may disclose *PHI* related to public health activities to:

1. A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including but not limited to, the mandatory reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority; and
2. A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.
3. A person subject to the jurisdiction of the Food and Drug Administration ("FDA") with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety, or effectiveness of such FDA-regulated product or activity. Such purposes include:
    a. To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;
    b. To track FDA-regulated products;
    c. To enable product recalls, repairs, replacement, or lookback (including locating and notifying *individual*s who have received products that have been recalled, withdrawn, or are the subject of lookback); or
    d. To conduct post-marketing surveillance.
4. A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if **Hybrid Org** or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.
5. An employer, about an *individual* who is a *member* of the *workforce* of the employer, if:
    a. **Hybrid Org** is the ***Responsible Employee's*** health care *provider* who provides health care to the *individual* at the request of the employer:
        i. To conduct an evaluation relating to medical surveillance of the workplace; or
        ii. To evaluate whether the *individual* has a work-related illness or injury.
    b. The *PHI* that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;
    c. The employer needs such findings in order to comply with its obligations under OSHA, MSHA, or under State law having a similar purpose to record such illness or injury, or to carry out responsibilities for workplace medical surveillance; or
    d. The covered health care *provider* provides written notice to the *individual* that *PHI* relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:
        i. By giving a copy of the notice to the *individual* at the time the health care is provided; or

ii. If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

6. A school, about an *individual* who is a student or prospective student at the school, if:
    a. The *PHI* that is disclosed is limited to proof of immunization;
    b. The school is required by state or other law to have such proof of immunization prior to admitting the *individual*; and
    c. **Hybrid Org** obtains and documents the agreement to the disclosure from either:
        i. A parent, guardian, or other person acting *in loco parentis* of the *individual*, if the *individual* is an unemancipated minor; or
        ii. The *individual*, if the *individual* is an adult or emancipated minor.

Disclosures About Victims of Abuse, Neglect, or Domestic Violence:

1. The **Hybrid Org** may disclose *PHI* about an *individual* whom the **Hybrid Org** reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency authorized by law to receive reports of such abuse, neglect, or domestic violence:
    a. To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;
    b. If the *individual* agrees to the disclosure; or
    c. To the extent the disclosure is expressly authorized by statute or regulation, and:
        i. The Hybrid Org, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the *individual* or other potential victims; or
        ii. If the *individual* is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the *PHI* for which disclosure is sought is not intended to be used against the *individual* and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the *individual* is able to agree to the disclosure.
2. When a disclosure about victims of abuse, neglect, or domestic violence is made, the **Hybrid Org** must promptly inform the *individual* that such a report has been or will be made, except if:
    a. The **Hybrid Org**, in the exercise of professional judgment, believes that informing the *individual* would place the *individual* at risk of serious harm; or
    b. The **Hybrid Org** would be informing a *personal representative* and the **Hybrid Org** reasonably believes the *personal representative* is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the *individual* as determined by the **Hybrid Org**, in the exercise of professional judgment.

Uses and Disclosures for Health Oversight Activities:

1. The **Hybrid Org** may disclose *PHI* to a health oversight agency for oversight activities authorized by law, including: audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:
    a. The healthcare system;
    b. Government benefits programs for which health information is relevant to beneficiary eligibility;

   c. Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
   d. Entities subject to civil rights laws for which health information is necessary for determining compliance.
2. "Health oversight activities," for purposes of (1) above, do not include an investigation or other activity in which the *individual* is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:
   a. The receipt of healthcare;
   b. A claim for public benefits related to health; or
   c. Qualification for, or receipt of, public benefits or services when a individual's health is integral to the claim for public benefits or services.
3. Notwithstanding (2) immediately above, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of this policy.
4. If the **Hybrid Org** also is a health oversight agency, the **Hybrid Org** may use *PHI* for health oversight activities as permitted by this policy.

Use and Disclosure for Law Enforcement Purposes
Hybrid Org will follow these requirements for the release of *PHI* for law enforcement purposes via court orders, court-ordered warrant, a judicial or grand jury subpoena, or summons including considerations for administrative and civil investigative demands.

Standard: Disclosures for law enforcement purposes. Hybrid Org may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs 1 through 6 below are met, as applicable.

1. ***Permitted disclosures: Pursuant to process and as otherwise required by law.*** A *covered entity* may disclose protected health information:
   a. As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject disclosure of abuse, neglect or domestic violence or if the victim agrees to the disclosure of this section; or
   b. In compliance with and as limited by the relevant requirements of:
      i. A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;
      ii. A grand jury subpoena; or
      iii. An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:
         1. The information sought is relevant and material to a legitimate law enforcement inquiry;
         2. The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
         3. *De-identified information* could not reasonably be used. See Also Privacy Policy 22.0: *Uses and Disclosures: Response to Judicial and Administrative Proceedings*.
2. ***Permitted disclosures: Limited information for identification and location purposes.*** Except for disclosures required by law as permitted by paragraph 1 above, **Hybrid Org** may

disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

a. **Hybrid Org** will disclose only the following information:
    i. Name and address;
    ii. Date and place of birth;
    iii. Social security number;
    iv. ABO blood type and rh factor;
    v. Type of injury;
    vi. Date and time of *treatment*;
    vii. Date and time of death, if applicable; and
    viii. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.
    ix. Except as permitted by paragraph 2(i)above, the *covered entity* may not disclose for the purposes of identification or location under this paragraph any protected health information related to the *individual*'s DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

3. ***Permitted disclosure: Victims of a crime.*** Except for disclosures required by law as permitted by paragraph 1 above, **Hybrid Org** may disclose protected health information in response to a law enforcement official's request for such information about an *individual* who is or is suspected to be a victim of a crime, other than disclosures that are subject to disclosures for public health activities or disclosures regarding victims of abuse, neglect or domestic violence, if:
    a. The *individual* agrees to the disclosure; or
    b. The *covered entity* is unable to obtain the *individual*'s agreement because of incapacity or other emergency circumstance, provided that:
        i. The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
        ii. The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the *individual* is able to agree to the disclosure; and
        iii. The disclosure is in the best interests of the *individual* as determined by the Hybrid Org, in the exercise of professional judgment.

Uses and Disclosures About Decedents:

1. Coroners and medical examiners: The **Hybrid Org** may disclose *PHI* to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A *Covered entity* that also performs the duties of a coroner or medical examiner may use *PHI* for the purposes described in this paragraph.
2. The **Hybrid Org** may disclose *PHI* to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If it is necessary for funeral directors to carry out their duties, the **Hybrid Org** may disclose the *PHI* prior to, and in reasonable anticipation of, the *individual*'s death.
3. The **Hybrid Org** may use or disclose *PHI* to organ procurement Hybrid Orgs or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation.

Uses and Disclosures About Decedents:

1. Coroners and medical examiners: The **Hybrid Org** may disclose *PHI* to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A *Covered entity* that also performs the duties of a coroner or medical examiner may use *PHI* for the purposes described in this paragraph.
2. The **Hybrid Org** may disclose *PHI* to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If it is necessary for funeral directors to carry out their duties, the **Hybrid Org** may disclose the *PHI* prior to, and in reasonable anticipation of, the *individual*'s death.
3. The **Hybrid Org** may use or disclose *PHI* to organ procurement Hybrid Orgs or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation of facilitating organ, eye, or tissue donation and transplantation.

Uses and Disclosures for *Research* Purposes:

1. The **Hybrid Org** may use or disclose *PHI* for *research*, regardless of the source of funding of the *research*, provided that:
    a. The **Hybrid Org** obtains documentation that an alteration to or waiver, in whole or in part, of the *individual* authorization for use or disclosure of *PHI* has been approved by either:
        i. An *Institutional Review Board* (*IRB*); or
        ii. A privacy board that:
            a. Has *members* with varying backgrounds and appropriate professional competency as necessary to review the effect of the *research* protocol on the *individual*'s privacy rights and related interests;
            b. Includes at least one *member* who is not affiliated with the **Hybrid Org**, not affiliated with any entity conducting or sponsoring the *research*, and not related to any person who is affiliated with any of such entities; and
            c. Does not have any *member* participating in a review of any project in which the *member* has a conflict of interest.
    b. The **Hybrid Org** obtains from the *researche*r:
        i. Representation that the use or disclosure sought is solely for *research* on the *PHI* of decedents;
        ii. Documentation, at the request of the **Hybrid Org**, of the death of such *individual*s; and
        iii. Representation that the *PHI* for which use or disclosure is sought is necessary for the *research* purposes.

Uses and Disclosures to Avert a Serious Threat to Health or Safety:

1. The **Hybrid Org** may, consistent with applicable law and standards of ethical conduct, use or disclose *PHI* if the **Hybrid Org**, in good faith, believes that the use or disclosure:
    a. Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public;
    b. Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or
    c. Is necessary for law enforcement authorities to identify or apprehend an *individual*:
        i. Because of a statement by an *individual* admitting participation in a violent crime that the **Hybrid Org** reasonably believes may have caused serious physical harm to the victim; and

ii. Where it appears from all the circumstances that the *individual* has escaped from a correctional institution or from lawful custody.

2. A use or disclosure pursuant to this policy may not be made if the information described is learned by the **Hybrid Org:**
    a. Over the course of *treatment*, counseling, or therapy to affect the propensity to commit the criminal conduct that is the basis for the disclosure under this policy; or
    b. Through a request by the *individual* to initiate or to be referred for *treatment*, counseling, or therapy described in the above paragraph.
3. A disclosure made pursuant to (1)(a)(i) above shall contain a statement that *PHI* is necessary for law enforcement to apprehend or identify an *individual* because of a statement by an *individual* admitting participation in a violent crime that the *covered entity* reasonably believes may have caused serious harm to the victim, AND the following information: name and address; date and place of birth; social security number; ABO blood type and rhesus factor; type of injury; date and time of *treatment*; date and time of death, if applicable; and a description of distinguishing physical characteristics, such as height, weight, gender, hair, and eye color.
4. The **Hybrid Org**, when using or disclosing *PHI*, is presumed to have acted in good faith if the belief is based upon the **Hybrid Org's** actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

Uses and Disclosures for Specialized Government Functions: Hybrid Org may use and disclose an *individual*'s protected health information (*PHI*) without an *individual*'s written authorization for the following specialized government functions:

- Military and veterans' activities
- National security and intelligence activities
- Protective services for the President and others
- Medical suitability determinations
- Correctional institutions and other law enforcement custodial situations

Under the Privacy Rule "*whistleblower* exception," *Responsible Employees* and their *business associates*, have the right to disclose *PHI* if they believe in good faith that another *Responsible Employee* or *business associate* has engaged in conduct that is unlawful or otherwise violates professional standards *Responsible Employees* may also report that services or conditions provided by a *member* of the *workforce*, a department, or a *business associate*, are endangering one or more participants, workers, or the public.

Permitted Disclosures by Whistleblower:

1. **Hybrid Org's** *Responsible Employees* and *business associates* may make *whistleblower* disclosures of an *individual*'s *PHI* without the *individual*'s written authorization.
2. **Hybrid Org** will not impose any sanctions upon and will not take any intimidating or retaliatory actions against *members* of **Hybrid Org's** *workforce* and **Hybrid Org's** *Business associates* who make Whistleblower Disclosures related to **Hybrid Org's** handling of *PHI* and compliance with *HIPAA*.
3. **Hybrid Org** does not violate *HIPAA* if a *member* of its *workforce* or its *business associate* makes a *whistleblower* disclosure in compliance with the requirements of this policy.
4. Under the *HIPAA whistleblower* exception, **Hybrid Org** is not considered to have violated the *HIPAA* Privacy Rule if a *member* of its *workforce* or a *business associate*

discloses protected health information (*PHI*), provided that the requirements of (a), (b), and (c) below, are met:

a. The *Responsible Employee* believes, in good faith, that:
    i. The **Hybrid Org** has engaged in unlawful conduct; or
    ii. The **Hybrid Org** has engaged in conduct that otherwise violates professional or clinical standards; or
    iii. The care, services, or conditions provided by the **Hybrid Org** potentially endanger individuals, workers, or the public.
b. The *PHI* "*whistleblower*" disclosures listed in (1) through (3) above are made to:
    i. An appropriate healthcare accreditation Hybrid Org for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the **Hybrid Org**; **or**
    ii. A health oversight agency or public health authority that has the authority to investigate or oversee the relevant conduct or conditions of the **Hybrid Org**; **or**
    iii. An attorney retained by or on behalf of the *Responsible Employee* or *business associate* for the purpose of determining the legal options of the *Responsible Employee* or *business associate* with regard to the conduct alleged to be improper.

Limitation on Disclosures: Disclosures can only be made if the Responsible Employee has a good faith belief that improper conduct has taken place. Broadly speaking, "good faith belief" means a belief with a reasonable basis in fact. Generally, a person is not acting in good faith if he or she knows or should have known that he or she is making a malicious, false, or frivolous allegation or complaint.

Permitted Disclosures by *Responsible Employee* Crime Victims:

1. A *Responsible Employee* who is a victim of a criminal act has the right to disclose *PHI* to law enforcement officials. Such a disclosure will not constitute a violation of the Privacy Rule by the **Hybrid Org** if the following conditions apply:
    a. The *PHI* disclosed is about the suspected perpetrator of the criminal act; and
    b. The *PHI* disclosed is limited to the following information:
        i. Name and address
        ii. Date and place of birth
        iii. Social Security Number
        iv. ABO blood type and rh (rhesus) factor
        v. Type of injury
        vi. Date and time of *treatment*
        vii. Date and time of death, if applicable; and
        viii. A description of distinguishing physical characteristics.
2. If a *Responsible Employee* considers himself or herself a *workforce* crime victim, he/she should immediately notify the *HIPAA Privacy Official*, who shall advise the *Responsible Employee* as to what *PHI* (see paragraph (1)) may be disclosed to law enforcement.

Permitted Disclosures: Military and Veterans Activities.

1. Armed Forces Personnel: **Hybrid Org** may disclose to military authorities the *PHI* of *individuals* who are *members* of the armed forces for purposes that appropriate military

command authorities have deemed necessary to ensure proper execution of the military mission.

2. Before the military authority may seek the information, the military authority must publish a notice in the Federal Register that sets forth both the name of the appropriate military command authorities, **and** the purposes for which the *PHI* may be used or disclosed.
3. Foreign Military Personnel: **Hybrid Org** may use or disclose to the appropriate military authority the *PHI* of *individual*s who are foreign military personnel for the same purposes for which **Hybrid Org** may use or disclose *PHI* regarding Armed Forces Personnel as described above.
4. National Security and Intelligence Activities: **Hybrid Org** may disclose *PHI* to authorized federal officials as necessary to conduct lawful intelligence, counterintelligence, and other national security activities authorized by the National Security Act (50 U.S.C. § 401, et. seq.) and implementing authority (i.e., Executive Order 12333).
5. Protective Services for the President and Others: **Hybrid Org** may disclose an *individual*'s *PHI* to authorized federal officials for the provision of protective services to the President of the United States or other persons authorized by 18 U.S.C. § 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. § 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. §§ 871 (Threats Against the President and Successors to the Presidency) and 879 (Threats Against Former Presidents and Others).
6. Correctional Institutions and Other Law Enforcement Custodial Situations: **Hybrid Org** may disclose an *individual*'s *PHI* to a correctional institution or a law enforcement official who has lawful custody of an inmate or other individual if the correctional institution or law enforcement official represents that such *PHI* is necessary for:
    a. The provision of healthcare to the *individual*;
    b. The health and safety of such *individual* or another inmate;
    c. The health and safety of the officers, *Responsible Employees*, or others at the correctional institution;
    d. The health and safety of such *individual* and officers or other persons responsible for the transporting of inmates or their transfer from one institutional facility or setting to another; or
    e. The administration and maintenance of safety, security, and good order of the correctional institution.

The *PHI* of an *individual* who has been released on parole, probation, supervised release, or who is otherwise no longer in lawful custody, may not be used or disclosed.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.501 *Definitions: Healthcare Operations*
45 CFR 164.512 *Uses and Disclosures for which an Authorization or Opportunity to Agree or Object is Not Required*
45 CFR 164.506 *Uses and Disclosures to Carry Out Treatment, Payment, or Health Care Operations*

Privacy Policy 15.0. Individual Right: Access to Protected Health Information

FULL POLICY LANGUAGE:

Policy Purpose:

It is the policy of the **Hybrid Org** to honor an *individual*'s right to *access*, inspect, and obtain a copy of their *PHI* contained in the *designated record set* and to charge only allowable fees for such *access*.

Policy Description:

This policy describes **Hybrid Org's** responsibility for providing *access* to a *designated record set* to *individuals* for as long as the record is maintained and the procedures for ensuring *individuals*' timely rights to *access*, inspect and copy their protected health information and seek review of some denials of *access*. Additionally, the policy establishes the requirements for determining and charging reasonable fees related to *access* requests by *individuals*.

Procedures:

Accessing and Inspecting *PHI*: Timing and Process

1. An *individual* may to *access* and inspect their *PHI*. Whenever possible, this request should be made in writing and documented.
2. The *Responsible Employee* who receives the request should direct it the *Privacy Official* to help make a determination prior to allowing or denying *access*.
3. When *access* is granted, the **Hybrid Org** will provide *access* to the requested *PHI* and furnish a copy (if requested) within a reasonable time but no later than 30 days from the date of the request unless the Hybrid Org is not able to provide *access* within 30 days. See below for the requirements on the form and fees for copies.
4. Where it cannot provide *access* within the 30-day time limit, before the 30 days expire, Hybrid Org will provide the *individual* a written notice of the reasons for the delay and include a date when *access* will be available. Hybrid Org will respond to all requests for *access* within 60 days of the *individual*'s request. A second extension beyond 60 days is not available.
5. The **Hybrid Org** documents and retains the *Designated record sets* containing the *PHI* that is subject to *access*. The **Hybrid Org** documents and retains the titles of persons or offices responsible for receiving and processing requests for *access*. These records are maintained for a minimum of six years form the date of creation or the date it was last in effect.

When *Access*, Inspection and/or Copy Request is Granted:

1. *Individual* and the **Hybrid Org** will arrange a mutually convenient time and place for the *individual* to inspect and/or obtain a copy of the requested *PHI* within the *designated record set*. Inspection and/or copying may be carried out on site at the **Hybrid Org** with staff assistance if necessary.
2. The individual may choose to inspect the *PHI*, copy it, or both, in the form or format requested. If the *PHI* is not readily producible in the requested form or format, the **Hybrid Org** must provide the individual with a readable hard copy form, or other form or format as agreed to by the **Hybrid Org** and the *individual*.
    a. If the *individual* chooses to receive a copy of the *PHI*, the **Hybrid Org** may offer to provide copying services. The individual may request that this copy be mailed.
    b. If the *individual* chooses to copy their own information, the **Hybrid Org** may supervise the process to ensure that the integrity of the individual record is maintained.
3. Whenever the *PHI* in the *designated record set* is maintained electronically, if the *individual* requests an electronic copy, **Hybrid Org** will provide *access* in the electronic form and format requested unless it is not readily producible that way. If it is not readily producible in the requested format, **Hybrid Org** and the *individual* will agree to a different readable electronic format for production.
4. Upon prior approval by the individual, the **Hybrid Org** may provide a summary of the requested *PHI* and charge an agreed upon fee (must not exceed the fees allowed – see fee section below).

5. If, upon inspection of the *PHI*, the individual believes the *PHI* is inaccurate or incomplete, the individual has the right to request an *amendment* to the *PHI*. The **Hybrid Org** shall process requests for *amendment* as outlined in Privacy Policy 17.0: *Individual Right: Request Amendment to Designated record set*.

Fees: Hybrid Org may charge a reasonable cost-based fee for the production of copies (including electronic copies) or a summary of *PHI* pursuant to the request of an *individual* (or their *personal representative*) for their own personal use. **Hybrid Org** may decide to waive such fees. For electronic record requests, **Hybrid Org** may decide to charge a flat fee in lieu of a cost-based fee.

Such fees may only include the actual or average cost of:

1. Labor for copying the protected health information, whether in paper or electronic form;
2. Supplies for creating the paper copy if paper is requested;
3. Electronic media if the *individual* requests an electronic copy be provided on portable media;
4. Postage when the *individual* requests that the phi or summary be mailed; and
5. Preparation of a Summary or Explanation of the *PHI* when the *individual* was informed in advance and agreed to the stated fee.

Such fees may *not* include:

1. costs associated with verification; documentation; searching for, handling, or retrieving the *PHI*; processing the request; maintaining systems; or recouping capital for data *access*, storage, or infrastructure, even if such costs are authorized by State law.
2. Fees established by state law where such fees are in excess of that allowed under *HIPAA*. State laws typically permit *providers* to charge a per-page copy fee, of up to a certain dollar value, or to charge a flat fee of up to a certain amount for the entire *medical record*. These fees are untethered to the actual costs of reproduction and can be in excess of that allowed under *HIPAA*.
3. Costs for providing, releasing, or delivering *medical record*s or copies of *medical record*s, where the request is for the purpose of supporting the application, claim, or appeal for any government benefit or program requested by the relevant government entity or at the *individual*'s request.

Flat Fee

Hybrid Org, in its discretion, may charge *individual*s a flat fee for all requests for electronic copies of *PHI* maintained electronically, provided the fee does not exceed $6.50 (or the then approved fee, if it increases), inclusive of all labor, supplies, and any applicable postage. **Hybrid Org** may charge this fee in lieu of going through the process of calculating actual or average allowable costs for requests for electronic copies of *PHI*.

***Access*, Inspection, and/or Copy Request is Denied in Whole or in Part:**

The **Hybrid Org** will deny *access* to any *PHI* without the opportunity for review if it contains:

1. *Psychotherapy notes* (See Privacy Policy 19.0: *Psychotherapy notes* for further details); or
2. Information compiled in reasonable anticipation of, or for use in, civil, criminal, or administrative action or proceeding.

If any part of the *designated record set* is separate from *psychotherapy notes* or information compiled in anticipation of legal proceedings, Hybrid Org shall allow *access* to that part of the record.

The Hybrid Org May Deny *Access* without Providing the *Individual* an Opportunity for Review, in the Following Circumstances:

1. When **Hybrid Org** is acting under the direction of a Correctional Institution and may deny an inmate's request if it were to jeopardize the health, safety, security, custody, or rehabilitation of the *individual*, other inmates, or any other person at the correctional institution.
2. When *PHI* created in the course of *research* that is still in progress, provided the *individual* has agreed to the denial of *access* when consenting to participating in the *research* that includes *treatment*, and the covered health care *provider* had informed the *individual* that the right of *access* would be reinstated upon completion of the *research*.
3. When *PHI* in the *designated record set* was obtained under promise of confidentiality from someone other than a healthcare *provider* and giving *access* would reveal the source of the information.
4. An *individual*'s *access* to *PHI* that is contained in records that are subject to the Privacy Act (also known as the Freedom of Information Act) may be denied, if the denial of *access* under the Privacy Act would meet the requirements of that law.

The Hybrid Org May Deny *Access* but will Provide the Opportunity for Review of Denials in the following Circumstances:

1. When a licensed healthcare professional (exercising their professional judgment) has determined that the *access* requested is reasonably likely to endanger the life or physical safety of the *individual* or another person.
2. When the *PHI* makes reference to another person (unless that person is a healthcare *provider*) and a licensed healthcare professional has determined in exercise of professional judgment, that the *access* requested is reasonably likely to cause substantial harm to the person.
3. When request for *access* is made by a *personal representative* of an *individual* and a licensed healthcare professional has determined in exercise of professional judgment that providing *access* to that representative can reasonably be expected to cause substantial harm to the *individual* or another person.

Denials of *Access*: Timing, form, and Review: If the **Hybrid Org** denies *access* in whole or in part in any of the circumstances described above, the following requirements apply:

Making Other information Accessible: The Hybrid Org will give the *individual access* to the protected health information that is not excluded under the denial to the extent that it is possible to separate the information for which the **Hybrid Org** has a basis for denial.

Denials will be in writing:
The **Hybrid Org** must provide a written denial in plain language to the *individual*. The denial must contain the following elements:

1. The basis for the denial;
2. A statement of the *individual*'s review rights for reviewable denials; and
3. A description of how the *individual* may complain to the **Hybrid Org** or to the Secretary of Health and Human Services (*HHS*) including at a minimum the title and telephone number of the *individual* designated to handle complaints for the **Hybrid Org**.

Other Responsibilities When *Access* is Denied:

1. If *access* is denied because the **Hybrid Org** does not maintain the *PHI* that is the subject of the request, and the **Hybrid Org** knows where that *PHI* is maintained, the **Hybrid Org** must inform the *individual* where to direct the request for *access*.
2. If *access* is denied under a situation where that denial may be reviewed, an *individual* has the right to have the denial reviewed by a licensed healthcare professional who is designated by the **Hybrid Org** to act as a reviewing official. Hybrid Org will designate a licensed professional to review the original *access* decision. The reviewing professional must be someone who did not participate in the original decision to deny *access*.
3. The individual must initiate the review of a denial by making a request for review to the **Hybrid Org**. If the individual has requested a review, the **Hybrid Org** must provide or deny *access* in accordance with the determination of the reviewing professional, who will make the determination within a reasonable period of time.
4. The **Hybrid Org** will promptly provide written notice to the *individual* of the determination of the reviewing professional and also act promptly on the reviewer's decision if they have granted *access*.

RELEVANT *HIPAA* REGULATIONS:

45 CFR 164.524 *Access of Individuals to Protected Health Information*

Privacy Policy 16.0 Individual Right: to Request Restrictions and Alternate Confidential Communications

FULL POLICY LANGUAGE:

Policy Purpose:

This policy covers how **Hybrid Org** assesses and when it will honor an *individual*'s request to restrict how and when their *PHI* is used or disclosed, and requests for communication of *PHI* by alternative means or at an alternate location.

Policy Description:

Hybrid Org permits an *individual* to request restrictions of uses and disclosures for *treatment*, *payment*, healthcare operations and disclosures to family *members*, relatives, close friends or others identified by the *individual* for involvement in the *individual*'s care and notifications and must agree to restrictions in some circumstances involving *payment*. All granted restrictions must be fully documented for six years and adhered to if agreed except in emergency circumstances or as otherwise required by law.

Hybrid Org may also terminate restrictions previously agreed to if (1) the *individual* agrees to or requests the termination in writing, (2) the *individual* orally agrees to the termination and the oral agreement is documented, or (3) a *Covered entity* informs the *individual* it is terminating an agreement to a restriction, (under circumstance 3, termination is only effective with respect to *PHI* created or received after it has informed the *individual*).

Hybrid Org, when considering the request for restriction, may consider its own need for *access* to *PHI* for *treatment* purposes.

Hybrid Org will also honor an *individual*'s right to receive confidential communications at alternative locations or by alternative means from a health plan when an *individual* would be endangered or from a *provider* where the request is reasonable. A *Covered entity provider* may

require that the request meet the following criteria: (1) be reasonable with respect to the administrative burden, (2) be in writing, (3) specify an alternative address or other method of contact, and, where relevant, provides information on how *payment*s should be handled.

Procedures:

Response to Request for Restriction:

1. Hybrid Org will notify *individual*s of the right to request restrictions on the use and disclosure of *PHI* and that the request needs to be in writing in **Hybrid Org's** Notice of Privacy Practices.
2. The *Privacy Official* will manage requests for restrictions. All documentation associated with the request shall be placed in the *individual*'s *medical record*.
3. The Hybrid Org will provide an *individual* with a *Request to Restrict Use and Disclosure of Protected Health Information* form ("Request to Restrict" form) if an *individual* asks to make a restriction.
4. The *individual* must complete and sign the form. The *Privacy Official* and/or his or her designee may assist the *individual* in completing the form, if necessary.
5. Once the request has been completed, the *Privacy Official* will review it, in consultation with other **Hybrid Org** staff, to determine the feasibility of the request.
6. Hybrid Org will agree to all requests related to restrictions about communicating *PHI* to a health plan when the following criteria are met:
    a. The disclosure is for the purpose of carrying out *payment* or *health care operations* and is not required by law; *and*
    b. The protected health information pertains solely to a health care item or service for which the *individual*, or a person (other than the health plan) on behalf of the *individual*, has paid the **Hybrid Org** in full.
7. Whether requests are allowed or denied, the *Privacy Official* will provide a written response to the *individual* and place a copy in their *medical record*.

Accepted Requests for Restrictions:

1. **Hybrid Org** will abide by the terms of any accepted restrictions with the following exceptions:
    a. **Hybrid Org** may use the restricted *PHI*, or may disclose such information to a healthcare *provider*, *if* (1) the *individual* is in need of emergency *treatment*, **and** (2) the restricted *PHI* is needed to provide that *treatment*. In this instance, **Hybrid Org** will release the *PHI*, but shall ask the emergency *treatment provider* to not further disclose or use the *PHI*.
    b. **Hybrid Org** may disclose the information to the individual who requested the restriction.
    c. **Hybrid Org** may use and disclose the restricted *PHI* when legally required to do so under the *HIPAA* Privacy Rule.
2. Upon accepting the restriction, the *Privacy Official* will notify appropriate staff of the restriction.
3. The *Privacy Official* will document the restriction on the Request to Restrict form, provide the individual with a copy, and maintain the original in the individual's *medical record*. This notation on the form can suffice for communicating the decision.

Termination of Restriction with *Individual*'s Agreement:

1. **Hybrid Org** may terminate the accepted restriction if the *individual* agrees to such termination in writing, **or** the *individual* agrees to the termination orally, and such oral agreement is documented by **Hybrid Org**.
2. **Hybrid Org** will notify appropriate staff of such termination. The *Privacy Official* shall document the *individual*'s agreement to the termination on the Request to Restrict form, provide the *individual* with a copy, and maintain the documentation in the *individual*'s record.
3. Termination of a restriction with the *individual*'s agreement is effective for all *PHI* created, maintained or received by **Hybrid Org**.

Termination of Restriction Without *Individual*'s Agreement:

1. **Hybrid Org** may terminate the restriction without the *individual*'s agreement if the **Hybrid Org** informs the individual that the restriction is being terminated.
2. Such termination will only be effective with respect to *PHI* created or received after **Hybrid Org** has informed the *individual* that it is terminating the restriction. The **Hybrid Org** must continue to abide by the restriction with respect to all *PHI* created or received before it informed the *individual* of the restriction.
3. If **Hybrid Org** informs the *individual* by mail that it is terminating the restriction, **Hybrid Org** will send it via certified mail, return receipt requested. **Hybrid Org** will maintain a copy of the notification and the return receipt. **Hybrid Org** may only terminate the restriction upon confirmation that the *individual* has received the notification.
4. If **Hybrid Org** informs the *individual* in person that it is terminating the restriction, **Hybrid Org** will ensure that the *individual* signs and dates the notification of termination. **Hybrid Org** may alternatively document that the *individual* was notified on the *Request to Restrict* form.
5. If **Hybrid Org** informs the *individual* by telephone of the termination of the restriction, the **Hybrid Org** shall document this action and will also send the *individual* a letter via certified mail, return receipt requested. **Hybrid Org** may deem such termination to be effective as of the date it informs the resident by telephone.

Confidential Communication by Alternative Means or at Alternate Location

*Individual*s may request communication of *PHI* by alternative means or at an alternate location. **Hybrid Org** will review and respond to such requests in accordance with the below procedures.

Response to Requests for Alternative Means of Communication:

1. Individuals shall be notified of the right to request communication by alternative means or at alternative locations in **Hybrid Org's** Notice of Privacy Practices. See Privacy Policy 10; *Notice of Privacy Practices*.
2. **Hybrid Org's** *Privacy Official* shall oversee and manage requests to receive communications by alternative means.
3. **Hybrid Org** requires *individual*s make a written request for communication by alternative means or at alternate location.
4. When an *individual* inquires about the right to request the **Hybrid Org** communicate with him or her, or his or her *personal representative*, by some alternate means, **Hybrid Org** shall provide them with a *Request for Communications by Alternative Means* ("Request for Communications") form. No request shall be evaluated until the request form has been completed and signed by the *individual* or their *personal representative*.

5. **Hybrid Org,** *if acting as a health plan*, may require that requests be accompanied by a statement that disclosure of *PHI* could endanger the *individual*. (The statement may be oral or written. *Responsible Employees* can ask *individuals* if disclosure of *PHI* could put them in danger, or *individuals* can fill out a request form that contains a checkbox question about possible endangerment due to *PHI* disclosure). Hybrid Org will not require an *individual* to give details of the perceived endangerment.
6. Hybrid Org, *when acting as a provider*, will have the *Privacy Official* promptly review the completed *Request for Communications* form to determine if the request is reasonable.
    a. **Hybrid Org** *will not* require an explanation for the request.
    b. **Hybrid Org** will not base its decision on the perceived merits (i.e., whether individual has a "good reason" for making the request) of the request.
    c. **Hybrid Org** will accommodate a request that it determines is reasonable (administratively feasible). Examples of reasonable requests include:
        i. The use of a sealed envelope rather than a postcard.
        ii. Receiving mail at a P.O. Box or office rather than a home address.
        iii. That telephone reminders only be communicated to an office or cell number.
7. The *Privacy Official* will complete the Response section of the Request for Communications form to inform the individual of the **Hybrid Org's** decision and may suggest different forms of alternate communications for requests that have been found not to be administratively feasible.
8. If the **Hybrid Org** grants an *individual*'s request, the decision must be documented by maintaining a written or electronic record of the action taken.
9. The *Privacy Official* shall maintain all requests and responses in the appropriate location in the *individual*'s *medical record* and *Responsible Employees* must review the record when communicating with the *individual*.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.502(c) *Uses and Disclosures of PHI Subject to an Agreed Upon Restriction*
45 CFR 164.502(h) *Confidential Communications*
45 CFR 164.522 *Rights to Request Privacy Protection for Protected Health Information*

Privacy Policy 17.0 Individual Right: Request Amendment of Designated record set

FULL POLICY LANGUAGE:

Policy Purpose:

It is the policy of **Hybrid Org** to honor an *individual*'s right to request an *amendment* or correction to their protected health information held in their *designated record set*, establish a process to review, deny, allow, and implement *amendments* and reflect requests for *amendments* in our records, and to notify others known by the **Hybrid Org** to have the information in their records.

Responsible Employees, *business associates*, and other healthcare *providers* must all comply with this policy.

Policy Description:

The *HIPAA* Privacy Rule grants *individuals* the right to *amend* or supplement their own protected health information, for as long as a *covered entity* (**Hybrid Org**) maintains the *PHI* in a *designated record set*. The right to *amend* includes the right to correction of errors, and the right to supplement an existing record with additional *PHI*. A *designated record set* is a group of records maintained by

or for **Hybrid Org,** which includes billing records, *medical record*s, and other records **Hybrid Org** uses to make decisions about *individual*s.

Hybrid Org has established a process to review, allow, deny, and reflect *amendment*s and requests for *amendment*s in the *designated record set*.

Procedures:

Requests to be in Writing:
Individual requests for *amendment* of protected health information shall be made in writing to **Hybrid Org** and clearly identify the information to be *amend*ed, as well as the reasons for the *amendment* and the content of the *amendment*.

Responding to a Request for *Amendment* or Notification of an *Amendment*:
Timing:
Hybrid Org acts on an *individual*'s request for *amendment* no later than 60 days after it receives the request. The deadline may be extended up to 30 days if **Hybrid Org** provides the *individual* with a written statement of the reasons for delay and the date by which **Hybrid Org** will fulfill his or her request before the expiration of the sixty days. The final response must be provided no later than 90 days from the date of the request.

Hybrid Org will promptly act upon a notice of an *amendment* for records in its *designated record set* received from another *covered entity*.

Implementation of *Amendment*: Notice from Another *Covered entity*
Upon receipt of notice from another *covered entity* of an *amendment* to records authored by that *covered entity* but also held in **Hybrid Org's** records, **Hybrid Org will** identify the information in the *designated record set* to be *amend*ed and clearly reflect the *amendment* in the *designated record set* for as long as it is held by the **Hybrid Org** and whenever it is shared by the **Hybrid Org.** Additionally, **Hybrid Org** will inform its *business associates*, that may use or rely on the *individual*'s *designated record set*, of the *amendment*, so that they may make the necessary revisions based on the *amendment*.

Review *Amendment* Request:
Privacy Official or their designee will be responsible for reviewing all requests for *amendment*s in a timely manner and in accordance with the guidelines below. Reviewer will involve clinical resources as necessary and the author of the record when appropriate.

It may be determined that a further review of the individual's request for *amendment* could be aided by the participation of an uninvolved third party. For purposes of this policy, an uninvolved third party will be defined as an individual who has not been involved in the original review of the request. This individual should be in a leadership position which, for the purposes of this policy, includes (but is not limited to) risk management Officials and executive leaders.

Allowing Request for *Amendment*:
If **Hybrid Org** approves the request for *amendment*, **Hybrid Org** must timely inform the *individual* that the request to *amend* has been accepted, and then make the appropriate *amendment*, reflecting it in the *designated record set* as well as timely notifying others known by the **Hybrid Org** to have the information in their records.

If **the request is granted,** after review and approval by the individual responsible for the entry to

be *amend*ed, **Hybrid Org** must:

- Insert the *amendment* or provide a link within the *designated record set* to the *amendment* at the site of the information that is the subject of the request for *amendment*;
- Inform the *individual* that the *amendment* is accepted;
- Obtain the *individual*'s identification of, and agreement to, have the **Hybrid Org** notify the relevant persons with whom the *amendment* needs to be shared. These persons include:
    - Persons identified by the *individual* as having received protected health information about the *individual* and needing the *amendment*; and
    - Persons, including *business associates*, that the **Hybrid Org** knows have the protected health information that is the subject of the *amendment* and that may have relied, or could foreseeably rely, on such information to the detriment of the *individual*.

Hybrid Org must then provide the *amendment* to both entities identified by the *individual*, and other entities known to have received the erroneous information.

Denial of Request for *Amendment*:
Hybrid Org may deny an *individual*'s request for *amendment* only *when the reviewer* determines that the information or record:

1. Was not created by **Hybrid Org**, unless the originator of the protected health information is no longer available to make the *amendment*;
2. Is not part of a *designated record set*;
3. Would not be available for inspection (under the Privacy Rule "right of *access*" standard) See Privacy Policy 15, *Right to Access* for further details; or
4. Is accurate and complete.

If **Hybrid Org** denies an *individual*'s request, it must give the *individual* a timely, written denial, which includes:

1. The basis for the denial;
2. The *individual*'s right to submit a written statement disagreeing with the denial and how to exercise that right;
3. A statement that the *individual* can request that **Hybrid Org** include the *individual*'s request and the denial with any future disclosures of the information (so long as the *individual* does not file a statement of disagreement – see below for process when one is filed); and
4. A description of how the *individual* can file a complaint with **Hybrid Org** or the Secretary of the Department of Health and Human Services (*HHS*).

Statements of Disagreement:
If **Hybrid Org** denies all or part of a requested *amendment*, **Hybrid Org** must permit the *individual* to submit a written statement disagreeing with the denial of all or part of the requested *amendment*, and the basis of such disagreement. **Hybrid Org** may reasonably limit the length of such statement.

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

Recordkeeping for Disputed *Amendments*:
Hybrid Org must, as appropriate, identify the record or protected health information in the *designated record set* that is the subject of the disputed *amendment* and append or otherwise link the *individual*'s request for an *amendment*, **Hybrid Org's** denial of the request, the *individual*'s statement of disagreement, if any, and **Hybrid Org's** entity's rebuttal, if any, to the *designated record set*.

Documentation:
Hybrid Org must document the titles for the persons or offices responsible for receiving and processing requests for *amendments* and retain the documentation as required by the *HIPAA* Privacy Rule for at least six years.

RELEVANT *HIPAA* REGULATIONS:

45 CFR 164.528 *Accounting of Disclosures of Protected Health Information*

Privacy Policy 18.0 Individual Right: Accounting of Disclosures

FULL POLICY LANGUAGE:

Policy Purpose:
The purpose of this policy is to ensure *individuals* can receive an *accounting of disclosures* of their protected health information.

Policy Description:
Hybrid Org, upon an *individual*'s request, will provide the *individual* with an accounting of certain disclosures of *PHI*. This policy details the required content of an *accounting of disclosures* that should include at least the following information: all non-excluded disclosures, including those made by a *business associate*, for a period not to exceed six years (can be for a shorter time at the request of the *Individual*). It must also include details like the date, name of entity/person receiving the phi, their address (if known), brief description of the disclosed information, and a copy of the request or a statement of reason for disclosure. For instances of multiple disclosures to same entity, the details may be limited to the first disclosure and a list of frequency or number of disclosures made during the accounting period and the date of the last disclosure. *Research* disclosures should also be included with details of the *research* and disclosures and an offer to help contact the *researcher* if desired. *Privacy Official* will handle all requests for *accounting of disclosures* and may delegate the responsibility at his or her discretion.

Disclosures Not to Be Included in an Accounting: In response to a request for an *accounting of disclosures*, **Hybrid Org** will exclude the following disclosures:

1. made for *treatment*, *payment*, and healthcare operations;
2. to the *individual* themself;
3. made incident to another allowed or required disclosure;
4. made pursuant to a valid authorization;
5. for facility directories, to those involved in the *individual*'s care or those involved in their care and those made for notification purposes, including identifying and locating a family member;
6. for national security or intelligence purposes;
7. made to law enforcement or correctional institutions with lawful custody of an inmate;

8. made as a part of a *limited data set*;
9. to which a valid request for delayed accounting by law enforcement or a health oversight agency is in place and has not expired; and
10. made more than six years prior to the date of the request for an accounting.

Required Disclosures: In response to a request for an *accounting of disclosures*, **Hybrid Org** will include disclosures:

1. made as required by law (i.e., reporting of certain wounds);
2. made for public health activities;
3. made for health oversight activities;
4. made to report victims of abuse, neglect, and domestic violence;
5. made for judicial and administrative proceedings;
6. made for *research* conducted under an *Institutional Review Board* (*IRB*) Waiver of Authorization;
7. made to avert a serious threat to the health and safety of the *individual*, or to the public;
8. made for certain specialized government functions (i.e., military and veterans affairs; medical suitability determinations); and
9. made for workers' compensation purposes.

Required Tracking: Hybrid Org will maintain and track the following information for disclosures that could be included in an accounting:

1. The date of disclosure;
2. The name of the *individual* or entity who received the information and their address, if known;
3. A brief description of the protected health information disclosed; and
4. A brief statement of the purpose of the disclosure.

Multiple disclosures to the same party for a single purpose may have a summary entry. A summary entry includes all information for the first disclosure, the frequency with which disclosures were made, and the date of the last disclosure.

Hybrid Org will maintain summary information for all public health authority reviews of its entire record set, or the portion of the entire record set that was made available for review but need not reflect these reviews in each individual record that may have been accessed. **Hybrid Org** will maintain these summaries in a way that makes it easy to reflect them in any *accounting of disclosures* for *individuals*.

Procedures:

Processing the Request:

1. All requests for an *accounting of disclosures* must be submitted, in writing, to the **Hybrid Org**.
2. The **Hybrid Org** must retain this request, retain a copy of the written account to be provided to the individual, and maintain a record of the name/departments responsible for the completion of the accounting, or of the *Privacy Official* if it was not delegated.
3. *Individuals* may authorize in writing that the *accounting of disclosures* be released to another individual or entity. The request must clearly identify all information required to carry out the request (name, address, phone number, etc.).

4. The **Hybrid Org** must retain all requests, maintain a copy of the written account to be provided to the third party, and maintain a record of the name/departments responsible for the completion of the accounting, or of the *Privacy Official* if it was not delegated.

Gathering the Necessary Information: Upon receipt of a completed request for *accounting of disclosures* form, the **Hybrid Org** will gather the requested information by:

1. Querying all systems and searching any records not in electronic form that contain disclosures that are not excluded from *accounting of disclosures*;
2. Obtaining a Disclosure Report from all departments that maintain such reports; or
3. Contacting *business associates*, as necessary, to request any pertinent disclosures made by or through them to include in the accounting.

Preparing the *Accounting of disclosures*: Accountings of disclosures shall be prepared by **Hybrid Org** following the protocol listed for each type of disclosure:

1. For each individual item on the *accounting of disclosures* **Hybrid Org** will include:
    a. The date the disclosure was made;
    b. The name of the entity or person receiving the *PHI*, and, if known, the address of such entity or person (to the extent revealing this information does not violate the *HIPAA* regulations);
    c. A brief description of the *PHI* that was disclosed; and
    d. A brief description of the purpose of the disclosure; OR
    e. For multiple disclosures to the same person or entity for the same purpose during the accounting period, A summary entry includes all information for the first disclosure, the frequency with which disclosures were made, and the date of the last disclosure.

2. Hybrid Org need not note in each individual record when it discloses all its records or a portion of its records that included the *individual* for public authority oversight activities, but these disclosures must be included in the *accounting of disclosures* with a summary of the dates the records were made available, the entity and/or person who may have reviewed the record and a brief description of the purpose of the disclosure.

Sending the Accounting and Timing:

1. In accordance with the *HIPAA* regulations, **Hybrid Org** will provide the *individual* with an accounting within 60 days after receipt of the request.
2. If the accounting cannot be completed within 60 days after receipt of the request, prior to the expiration of the 60 days, **Hybrid Org** will provide the *individual* with a written statement of the reason for the delay and the expected completion date. Only one extension of time, 30 days maximum, per request is permitted.
3. In no event will **Hybrid Org** provide the *individual* with the accounting later than 90 days from the date of the request.
4. The **Hybrid Org** will provide an accounting for a period of time of up to six years prior to the date of the request, unless the *individual* specifies a shorter time frame.
5. **Hybrid Org** must provide an accounting to the *individual* at no charge for the first request made during any twelve-month period.
6. A reasonable fee can be charged for any additional requests made during a twelve-month period, *provided* that the *individual* is informed of the fee in advance and given an opportunity to withdraw or modify the request.

Maintaining Records of Accountings Provided:

Hybrid Org must maintain all information subject to an accounting for at least six years, or longer (if required by **Hybrid Org's** state).

Hybrid Org must maintain written requests for an accounting provided to an *individual* for at least six years from the date it was created, or longer (if required by **Hybrid Org's** state).

Hybrid Org must maintain the titles and names of the people responsible for receiving and processing accounting requests for a period of at least six years, or longer (if required by **Hybrid Org's** state).

RELEVANT *HIPAA* REGULATIONS:

45 CFR 164.528 *Accounting of Disclosures of Protected Health Information*

Privacy Policy 19.0 Uses and Disclosures: Psychotherapy notes

FULL POLICY LANGUAGE:

Policy Purpose:

To ensure *Responsible Employees* understand the distinction between *psychotherapy notes* and other mental health records, the mental health practitioner/individual privilege that applies to *psychotherapy notes* in most states, and the requirement that these notes be separated from the *designated record set* to receive heightened protections. To assure that Hybrid Org follows all requirements for use and disclosure of *psychotherapy notes* in the limited circumstances where it is allowed.

Policy Description:

This policy describes how **Hybrid Org** is to respond to requests for *psychotherapy notes*; the distinction between *psychotherapy notes* and other mental health records; the mental health practitioner/individual privilege that applies to *psychotherapy notes*; and the requirement that these notes be separated from the *designated record set* to receive heightened protections. The Policy also describes the processes Hybrid Org follows to assure that it meets all requirements for use and disclosure of *psychotherapy notes* in the limited circumstances where it is allowed.

Procedures:

What are *Psychotherapy notes*? Hybrid Org treat notes recorded in any medium by a health care *provider* who is a mental health practitioner documenting or analyzing the contents of a conversation during a during a private counseling session or a group, joint, or family counseling session that are separated from the rest of the *medical record* as *psychotherapy notes*.

Separation from *Designated record set*: Hybrid Org will provide a means for recording any *Psychotherapy notes* in its possession separately from the *designated record set* in order to preserve the heightened privacy afforded these records. This separation may be electronic or physical.

What is not included in *Psychotherapy notes* even though it is related to psychotherapy?

Hybrid Org will not consider the following as *psychotherapy notes*: medication prescription and monitoring, session start and stop times, modalities and frequency of *treatment*, clinical test results, or summary information on diagnosis, functional status, *treatment* plan, symptoms, prognosis and progress to date. Hybrid Org will consider this content part of the mental health record and recognizes that heightened privacy requirements may apply because it is sensitive *PHI* under most state laws.

***Psychotherapy notes* and the Mental Health Practitioner/Individual Privilege**: If there is a practitioner/individual privilege that attaches to *psychotherapy notes* under applicable state law, **Hybrid Org** will honor that privilege and require that the privilege be validly waived in any situation in which another law does not take priority over this privilege.

Use of Legal Counsel: Hybrid Org will seek legal counsel when it is unsure of how to proceed prior to releasing *psychotherapy notes*.

Limitations on Use and Disclosure of *Psychotherapy notes* for *Treatment*: *Psychotherapy notes* are treated differently from other mental health information both because they contain particularly sensitive information and because they are the personal notes of the therapist that typically are not required or useful for *treatment*, *payment*, or *health care operations* purposes, other than by the mental health professional who created the notes. Accordingly, **Hybrid Org** follows the rule that only the originator of the *psychotherapy notes* may *access* those notes for the *treatment* of the *individual* to which they apply unless the privilege has been waived and a valid authorization has been signed by the *individual*.

Individual *Access* to *Psychotherapy notes*: Even though the individual has a right to *access* most health information, the individual does not have a right to *access psychotherapy notes*. Therefore, the **Hybrid Org** is not required to fulfill an individual's request for *access* to *psychotherapy notes*. However, the **Hybrid Org** will inform the individual of this limitation in response to a request for *access*.

Individual Authorization Required: In most circumstances, the **Hybrid Org's** *Responsible Employees* must obtain an individual's written authorization for any use or disclosure of *psychotherapy notes*. If there is a concern that a request for disclosure is unnecessary or excessive, the **Hybrid Org** may ask the individual if the authorization for disclosure is consistent with his or her wishes.

Hybrid Org utilizes an Authorization for the use or disclosure of *psychotherapy notes* specific to the *psychotherapy notes* and may not combine the authorization with any other consent or authorization with the exception of another authorization for the use or disclosure of *psychotherapy notes*.

Individual Authorization *Not* Required: The **Hybrid Org** is not required to obtain an authorization for the following uses or disclosures of *psychotherapy notes*, when use or disclosure is necessary to:

1. To carry out the following *treatment*, *payment*, or *health care operations*:
    a. Use by the originator of the *psychotherapy notes* for *treatment*; or
    b. Use by the author of the notes or the **Hybrid Org** to defend the author, the Hybrid Org or another *member* of Hybrid Org's *workforce* in a legal action or other proceeding brought by the *individual* who is the subject of the notes. Such use is not

allowed in response to a legal action brought by anyone other than the *individual* who is the subject of the notes.

2. To respond to the federal Department of Health and Human Services (*HHS*) to determine the **Hybrid Org's** compliance with *HIPAA* privacy rules;
3. To comply with the law;
4. To assist in health oversight activities regarding the originator of the *psychotherapy notes*;
5. To help coroners/medical examiners in the examination of deceased persons; and
6. To prevent or lessen a serious and imminent threat to the health or safety of a person or the public. Hybrid Org will only make such disclosures when necessary in the professional judgement of the author of the notes and when made to a person reasonably able to prevent or lessen the threat. **Hybrid Org** will follow state law in determining whether such disclosures are mandatory or permissive.

RELEVANT *HIPAA* REGULATIONS:

45 CFR 164.508(a)(2) *Uses and Disclosures for Which an Authorization is Required: Psychotherapy notes*

Privacy Policy 20.0 Minors' Rights

FULL POLICY LANGUAGE:

Policy Purpose:

To set forth **Hybrid Org's** requirements surrounding *access* to an unemancipated minor's records and *PHI*.

Policy Description:

This policy describes circumstances in which Hybrid Org requires minors to *access* their *PHI* through a *personal representative*, and when minors may *access* their *PHI* directly with or without the approval or knowledge of parents, guardians or *personal representative*s. It also describes the circumstances in which Hybrid Org requires a minor's approval for parents, guardians and *personal representative*s to *access* a minor's record.

This policy further describes the circumstances under which **Hybrid Org** *must* provide minors with *access* to their *PHI*; when **Hybrid Org** *may* do so; and when **Hybrid Org** *may not* do so.

Procedures: Exercising *HIPAA* rights and *Access* to Minor's *PHI*

When Parents guardians or other persons acting as in loco parentis or as *Personal representative*

Although generally, Hybrid Org may regard a parent, guardian or other person acting in loco parentis of a minor child as what the *HIPAA* Privacy Rule *personal representative*, there are also number of situations where that the **Hybrid Org** may not do so.

Because parents, guardians and those acting in loco parentis do not have unfettered rights to act as *personal representative*s, Hybrid Org will determine their rights on a case-by-case basis. Hybrid Org will honor a parent who is a *personal representative* exercise of a minor's *HIPAA* Privacy Rule rights with respect to protected health information (*PHI*) and other *HIPAA* rights like the signing of authorizations, consistently with state and other laws in the following circumstances:

1. If a *personal representative* has the authority to act on behalf an emancipated minor in making decisions related to healthcare, **Hybrid Org** must treat that person as a *personal representative*, with respect to *PHI* unless otherwise prohibited (see discussion below regarding abuse, neglect and endangerment); and
2. If, under applicable law, a parent, guardian, or other person acting *in loco parentis* has the authority to act on behalf of an unemancipated minor in making decisions related to healthcare, **Hybrid Org** must treat that person as a *personal representative* with respect to *PHI* relevant to such personal representation unless otherwise prohibited (see discussion below regarding abuse, neglect and endangerment).

Honoring the Minor's authority to Act: The Hybrid Org may not treat another person as a representative of the unemancipated minor, and must honor the minor's authority to act as an *individual* with respect to *PHI* pertaining to health care services, if under federal, state or other applicable law, including case law:

1. The minor consents to such healthcare services; *no other consent is required by law*, regardless of whether the consent of another person has been obtained; and the minor has not requested that person be treated as the *personal representative*;
2. The minor may lawfully obtain such health care services without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or when
3. A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between **Hybrid Org** and the minor with respect to such healthcare service.

What Role Does State and other Federal Law Play? The *HIPAA* Privacy Rule does not contravene state or other federal laws that expressly address the ability of parents to obtain health information about minors.

For example, regardless of whether a parent is the *personal representative* of a minor child, the *HIPAA* Privacy Rule permits a *covered entity* to disclose to a parent, or provide the parent with *access* to, a minor child's protected health information, *when and to the extent* it is permitted or required by state law.

Likewise, the *HIPAA* Privacy Rule prohibits **Hybrid Org** from disclosing a minor child's protected health information to a parent, or providing a parent with *access* to such information, when and to the extent it is prohibited under state or federal law.

Situations involving Endangerment Domestic Violence, abuse or Neglect: When **Hybrid Org** reasonably believes that an *individual*, including an unemancipated minor, has been or may be subjected to domestic violence, abuse, or neglect by the *personal representative*, or that treating a person as an *individual*'s *personal representative* could endanger the *individual*, **Hybrid Org** may choose not to treat that person as the *individual's personal representative,* if in the exercise of professional judgment, doing so would not be in the best interests of the *individual*. See the paragraph discussing *personal representative*s in Privacy Policy 17.0: *Uses and Disclosures: General Rules* for more detail.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.502(g) *Personal Representatives, Adults and Emancipated Minors*

Privacy Policy 21.0 Use of Social Media

FULL POLICY LANGUAGE:

Policy Purpose:

To provide rules for acceptable social media use.

Policy Description:

This policy outlines the safeguards *Responsible Employees* must follow to ensure that their use of social media does not result in unauthorized disclosure of *PHI*.

Procedures:

The following principles apply to professional use of social media on behalf of **Hybrid Org**, as well as personal use of social media when referencing the **Hybrid Org** or anyone served by them.

***Individual* Privacy** (*individual*s include persons served, beneficiaries and insureds and the term is further defined in the Glossary)**:**

1. Posting an *individual*'s information, commentary, or photographs on professional or personal social media sites requires written authorization from the *individual*.
2. If any photos, audio recordings, or video-recordings, contain images or recordings of more than one *individual*, written authorization from all *individual*s those individuals must also be obtained.
3. *Responsible Employees* who suspect unauthorized disclosure of an *individual*'s information via social media, or any suspected unauthorized live streaming, photographing, filming, or recording, shall promptly report such suspicions to the *Privacy Official*.

Interacting with *Individual*s on Social Media

1. *Responsible Employees* may not connect with *individual*s or their family *members* using social media.
2. *Responsible Employees* should not accept "Friend" requests from *individual*s on social media sites such as Facebook, nor should *Responsible Employees* send such requests.

RELEVANT HIPAA REGULATION:

45 CFR 164.530(c) *Privacy Safeguards*

Privacy Policy 22.0 Uses and Disclosures: Response to Judicial and Administrative Proceedings

FULL POLICY LANGUAGE:

Policy Purpose:

To establish rules for how **Hybrid Org** will respond to requests for disclosure of *PHI* in the course of judicial or administrative proceedings through judicial or administrative orders, subpoenas, discovery requests, or other lawful process, that is not accompanied by an order of a court or *administrative tribunal*. **Hybrid Org** will cooperate with courts and with counsel to provide lawfully sought *PHI*, while simultaneously ensuring protection of *individual* privacy.

Policy Description:

Hybrid Org may receive requests to disclose *PHI* in the course of judicial or administrative proceedings. Requests can be in the form of a subpoena, court order, request for discovery, or other

lawful process not accompanied by an order of a court or an *administrative tribunal*. This policy outlines how to handle disclosures of *medical record*s and other health information for purposes of judicial and administrative hearings. In the absence of an actual order but with lawful process (for example a subpoena or discovery request), **Hybrid Org** will determine if there is satisfactory assurance that the *individual* received appropriate notice and a chance to respond or to provide notice prior to releasing protected health information. **Hybrid Org** may determine if there are grounds for objection to a judicial or administrative order prior to responding, especially where the request seems overly broad or irrelevant.

Procedures:

Disclosing *PHI* in Response to a Court or Administrative Order:

If the **Hybrid Org** receives an order from a court or administrative judge requiring **Hybrid Org** to disclose protected health information, **Hybrid Org** may only release that *PHI* which the order expressly authorizes disclosure.

If the Hybrid Org believes the order may be overbroad, irrelevant or objectionable on other legal grounds, the *Privacy Official*, working with legal counsel, may review any such order to determine whether **Hybrid Org** will object to the order on any lawful basis. If the Hybrid Org concludes that an objection to the order is required, such objection shall be filed in accordance with applicable state or federal law and filing deadlines. The objection shall be documented.

Disclosing *PHI* in Response to a Subpoena, Discovery Request, or Other Lawful Process Other Than a Court Order:

1. The **Hybrid Org** may release *PHI* in response to a subpoena, discovery request, or other lawful process, that is not accompanied by a court order, as follows:
    a. The **Hybrid Org** may release *PHI* if it receives *written* "satisfactory assurance" from the party requesting the information that reasonable efforts have been made by the requesting party to ensure that the individual who is the subject of the *PHI* has been given notice of the request. Receipt of "Satisfactory assurance" that the requesting party has made a good faith effort to notify the *individual* of the request for is met where the requesting party provides the **Hybrid Org** a *written statement and supporting documentation* demonstrating that:
        i. The requesting party has made a good faith attempt to provide written notice to the *individual* (if the *individual*'s location is unknown, documentation showing that a notice was mailed to their last known address shall be provided by the requesting party);
        ii. The requesting party provided notice to the *individual* containing enough information to allow the *individual* to make an informed objection to the court or *administrative tribunal* regarding the release of their *PHI*; and
        iii. The time for the *individual* to raise objections to the court or *administrative tribunal* has passed, and, either no objections were filed, **or** all objections filed by the *individual* have been resolved and the disclosures being sought are consistent with the court's resolution.

2. The **Hybrid Org** may release *PHI* to a requesting party if it receives ***written*** satisfactory assurance from the requesting party that reasonable efforts have been made by such party to secure a *qualified protective order*. A *qualified protective order* is an order of a court or *administrative tribunal* or a stipulation by the parties to the proceeding, that prohibits the parties from using or disclosing *PHI* for any purpose other than the proceeding for which the information was requested. A qualified protective order requires the parties to return the *PHI* (including all copies made) to **Hybrid Org** at the end of the proceeding.

"Satisfactory assurance" in this instance means that the **Hybrid Org** has received from the requesting party a written statement, along with supporting documentation, demonstrating that:

a. The parties to the dispute giving rise to the request for *PHI* have *agreed* to a qualified protective order and have presented it to a court or *administrative tribunal* with jurisdiction over the dispute; or
b. The requesting party has asked for a qualified protective order from such court or *administrative tribunal*.

3. The **Hybrid Org** may release *PHI* to a requesting party even without satisfactory assurance from that party if the **Hybrid Org** either:
    a. Makes reasonable efforts to provide notice to the *individual* about releasing their *PHI*, so long as the notice meets all of the following requirements:
        i. The notice is written and given to the *individual* (if the *individual*'s location is unknown, **Hybrid Org** should establish documentation showing that a notice was mailed to their last known address);
        ii. The notice contained enough information to allow the *individual* to make an informed objection to the court or *administrative tribunal* regarding the release of their *PHI*; and
        iii. The time for the *individual* to raise objections to the court or *administrative tribunal* has lapsed and either no objections were filed, or all objections filed by the *individual* have been resolved and the disclosures being sought are consistent with the court's resolution.
    b. Seeks a qualified protective order from the court or *administrative tribunal* or convinces the parties to stipulate to such order.

RELEVANT *HIPAA* REGULATIONS:

45 CFR164.512(e) *Use and Disclosure of Protected Health Information for Judicial and Administrative Proceedings*

Privacy Policy 23.0 Uses and Disclosures: Fundraising

FULL POLICY LANGUAGE:

Policy Purpose:

To ensure **Hybrid Org conducts any** *fundraising* activities consistent with the Privacy Rule.

Policy Description:

Hybrid Org does not currently engage in fundraising.

If Hybrid Org opts to engage in fundraising for itself or a third party, **Hybrid Org** will notify *individuals* in its Notice of Privacy Practices of same. All *fundraising* materials must describe how an *individual* can opt out of receiving future *fundraising* communications.

RELEVANT HIPAA REGULATIONS:

45 CFR 164.514(f)(2) *Uses and Disclosures for Fundraising & Implementation Specifications: Fundraising Requirements*
45 CFR 164.501 *Definitions*

Privacy Policy 24.0 Uses and Disclosures: Worker's Compensation

FULL POLICY LANGUAGE:

Policy Purpose:

To provide rules for use or disclosure of *PHI* for workers compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

Policy Description:

HHS guidance makes clear that the Privacy Rule recognizes legitimate needs for insurers and other entities involved in the worker's compensation system to be allowed *access* to an *individual*'s *PHI* when authorized by state or other law. These laws may vary significantly so the Privacy Rule permits disclosure of *PHI* for worker's compensation purposes in a number of ways including allowing disclosures without an *individual*'s authorization, allowing disclosures with an *individual*'s authorization, and requiring the application of the *minimum necessary standard* for worker's compensation disclosures.

Disclosures made for Worker's Compensation related *medical record*s without an *individual*'s authorization. The Privacy Rule permits **Hybrid Org** to, and the **Hybrid Org** will disclose protected health information to workers' compensation insurers, State administrators, employers, and other persons or entities involved in workers' compensation systems, without the *individual*'s authorization:

1. When such release is authorized by and to the extent necessary to comply with laws relating to workers' compensation or similar programs established by law that provide benefits for work-related injuries or illness without regard to fault. This includes programs established by the Black Lung Benefits Act, the Federal Employees' Compensation Act, the Longshore and Harbor Workers' Compensation Act, and the Energy Employees' Occupational Illness Compensation Program Act. See 45 CFR 164.512(l).
2. To the extent the disclosure is required by State or other law. The disclosure must comply with and be limited to what the law requires. See 45 CFR 164.512(a) for specific limitations.
3. For purposes of obtaining *payment* for any health care provided to the injured or ill worker. Hybrid Orgs' Use and Disclosure requirements for *payment* must be followed.

Disclosures made to Entities and People involved in addressing Worker's Compensation related claims and conditions with an *Individual*'s Authorization: An *individual* may also authorize the Hybrid Org to release their *PHI* to worker's compensation insurers and others involved in worker's compensation systems. For release under such an authorization, the authorization must be valid and meet the requirements set forth in Privacy Policy 13: *Uses and Disclosures for which an Authorization is Required*. concerning the validity of an authorization. Hybrid Org will not release information beyond the authorization except as otherwise required and to the extent necessary to comply with laws related to worker's compensation and similar programs.

Examples of when an *individual*'s authorization may be required are releases of *PHI* that are not reasonably related to the condition for which they are claiming worker's compensation and are beyond the requirements of the laws applying to record release for worker's compensation purposes.

Application of the *Minimum Necessary Standard* to Disclosures for Worker's Compensation Purposes: Hybrid Org may share information for worker's compensation purposes to the full extent authorized by the state or other law and will limit the information to the minimum necessary

to meet the legal requirements. Hybrid Org will reasonably rely on a state worker's compensation official or other public official's representations that the information requested is the minimum necessary for the intended purpose. Hybrid Org will also limit the information shared for receiving *payment* for services performed related to a worker's compensation claim to the minimum necessary for that purpose.

Procedures:

1. After receipt of written request from an *individual*, employer, state board of workers compensation, or workers compensation insurance carrier for the employer, **Hybrid Org** shall release, within a reasonable amount of time and no later than required by the applicable legal requirements, copies of *medical record*s or verbal communications, that reasonably relate to the work injury in compliance with the *minimum necessary standard* and with the law requiring the disclosure. If Hybrid Org finds that is routinely making such disclosures, it may develop a standard protocol to be used for meeting the Minimum Necessary standard for worker's compensation *payment* disclosures.
2. Requests for copies of *medical record*s, which extend beyond the scope of the work-related injury and the reach of the applicable law, need to be accompanied by a valid written authorization from the *individual*.
3. **Hybrid Org** shall furnish legible duplicates of written material requested by *individual*s, employers, insurance carriers, and state boards of workers compensation. Certified copies shall be furnished upon request.
4. **Hybrid Org** will follow this same process for the release of *PHI* for *Responsible Employees* who have filed a claim under worker's compensation or related laws for on-the-job related injuries or conditions**.**

RELEVANT *HIPAA* REGULATIONS:

45 CFR 164.512(l) *Uses and Disclosures for which an Authorization or Opportunity to Agree or Object is Not Required: Worker's Compensation*

Privacy Policy 25.0 Uses and Disclosures: Limited Data Set and Data Use Agreements

FULL POLICY LANGUAGE:

Policy Purpose:

To establish the process for creating a Limited Data Set, as well as the purposes for and circumstances under which a Limited Data Set may be disclosed and to describe the process for creating the Data Use Agreement that to be signed before sharing a Limited Data Set.

Policy Description:

This policy defines a *limited data set*; sets forth appropriate uses for *limited data set*s; requires that a data use agreement meeting the defined criteria be in place between the parties; requires that the **Hybrid Org** adhere to applicable data use agreements and monitor the recipient's use of the data set for patterns of activity or practices in violation of the data use agreement; and requires **Hybrid Org** to end sharing of the data set and report to *HHS* if any violations are not reasonably cured.

Under *HIPAA*, a *limited data set* is a set of identifiable healthcare information. The *HIPAA* Privacy Rule permits **Hybrid Org** to share a *limited data set* with certain entities for *research* purposes, public health activities, and healthcare operations, without having to obtain prior written individual authorization, *if* certain conditions are satisfied.

Since a *limited data set* is still identifiable protected health information, a *limited data set* may only be shared by **Hybrid Org** with entities that have signed a data use agreement with **Hybrid Org**. A data use agreement allows **Hybrid Org** to obtain satisfactory assurances that the *PHI* will only be used for specific purposes; that the *PHI* will not be disclosed by the entity with which it is shared; and that the *HIPAA* Privacy Rule requirements will be observed.

Procedures:

Limited Data Set:

1. **Hybrid Org** may disclose a Limited Data Set (*PHI* with certain identifiers removed) to a requesting party only if the disclosure is for purposes of *research*, public health, or *health care operations*.
2. To create a Limited Data Set, the **Hybrid Org** (or its *Business associate*) shall remove the following identifiers from existing *PHI* of the *individual*, and of relatives, employers, or household members of the *individual*:
    a. Names;
    b. Street addresses (other than town, city, state and zip code);
    c. Telephone numbers;
    d. Fax numbers;
    e. Email addresses;
    f. Social Security numbers;
    g. Medical records numbers;
    h. Health plan beneficiary numbers;
    i. Account numbers;
    j. Certificate/ license numbers;
    k. Vehicle identifiers and serial numbers, including license plates;
    l. Device identifiers and serial numbers;
    m. URLs;
    n. IP address numbers;
    o. Biometric identifiers (including finger and voice prints); and
    p. Full face photos (or comparable images).
3. The health information that may remain in the Limited Data Set – in the information disclosed – includes:
    a. Dates, including admission dates, discharge dates, service dates, date of birth, and date of death;
    b. City, state, and five digit or more zip code; and
    c. Age (in years, months, days, or hours)
4. Only authorized **Hybrid Org** *Responsible Employees*, or authorized *business associates*, may create a Limited Data Set.
5. If a *business associate* creates the Limited Data Set, **Hybrid Org** must have enter into a *business associate agreement* before the *business associate* can have *access* to the *PHI* or create the limited Data Set.

Data Use Agreement:

1. **Hybrid Org** may use or disclose a Limited Data Set, only if **Hybrid Org** first obtains a signed, written Data Use Agreement (DUA) from the person/entity to whom the Limited Data Set is to be disclosed.
2. **Hybrid Org** will enter into a DUA before there is any use or disclosure of a Limited Data Set to an outside party. **Hybrid Org** will abide by the terms of the DUAs and assure that all of its DUAs:

a. Establish the permitted uses and disclosures of such information by the Limited Data Set recipient. The DUA may not authorize the Limited Data Set recipient to use or further disclose the information in a manner that would violate *HIPAA* privacy requirements, if done by the **Hybrid Org**;
b. Establish who is permitted to use or receive the Limited Data Set; and
c. Provide that the Limited Data Set recipient will:
    i. Not use or further disclose the information other than as permitted by the DUA or as otherwise required by law;
    ii. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the DUA; and
    iv. Ensure that any *agent*s to whom it provides the Limited Data Set agree to the same restrictions and conditions that apply to the Limited Data Set recipient with respect to such information.

3. Noncompliance by Limited Data Set Recipient: If at any time **Hybrid Org** becomes aware that a recipient of a Limited Data Set has undertaken a pattern of activity or practice that constitutes a material *breach* or violation of the Data Use Agreement, then **Hybrid Org** shall take reasonable steps to cure the *breach* or end the violation. If the *breach* cannot be cured or the violation ended, then **Hybrid Org** must cease all disclosures of the Limited Data Set to the recipient and report the problem to the Secretary of the Department of Health and Human Services.
4. Minimum Necessary and Accounting for Disclosures: The minimum necessary and accounting for disclosures rules do not apply to *PHI* disclosed as part of a Limited Data Set.

RELEVANT *HIPAA* REGULATION 45 CFR 164.514(e) *Limited Data Set and Data Use Agreement*

Privacy Policy 26.0 Guidelines for Specific Transactions/Minimum Necessary Standard

The following generally describes regular transactions performed by Responsible Employees. Guidelines for uses and disclosures of PHI by Business Associates will be documented by the Business Associates, as appropriate.

Human Resources, Compensation, and Benefits Departments

Responsible Employees in the Human Resources Department, including the Compensation and Benefits Department, may create and receive PHI from Individuals who have questions about their Health Plan benefits and from Business Associates (as permitted under this Policy). A Responsible Employee in the Human Resources Department may use or disclose PHI as follows:

DESCRIPTION OF HEALTH INFORMATION	REASON FOR USE/DISCLOSURE	PROTOCOLS	MINIMUM NECESSARY PHI
Disclosure of Health Plan enrollment and disenrollment information	Disclosure of Individual's enrollment PHI, such as to direct an Individual to the correct claims' administrator, HMO, or insurer	Verify identity of requestor by asking for participant's date of birth or social security number. (If requestor is Personal Representative, also verify Personal Representative's identity with appropriate documentation.)	No limit – disclosure of Individual's own PHI
	Disclosure of a dependent family member's enrollment PHI to a Covered Participant, such as to direct the Covered Participant to the correct claims' administrator, HMO, or insurer	Verify requestor is involved with dependent's health care or payment for health care by requiring requestor to explain relationship and supply claim related information (*e.g.*, social security number or date of birth, treatment date, provider's name, amount charged, etc.). Check participant's or covered dependent's benefits profile to determine whether he or she has requested confidential communication or has objected to the sharing of PHI with friends or family members. If so, refuse to disclose information.	Name and contact information for appropriate administrator, HMO, or insurer for relevant Health Plan

DESCRIPTION OF HEALTH INFORMATION	REASON FOR USE/DISCLOSURE	PROTOCOLS	MINIMUM NECESSARY PHI
	Disclosure of a minor child's enrollment PHI to a parent or guardian, such as to direct the parent or guardian to the correct claims administrator, HMO, or insurer	Verify requestor is involved with dependent's health care or payment for health care by requiring requestor to explain relationship and supply claim related information (*e.g.*, social security number or date of birth, treatment date, provider's name, amount charged, etc.). Check participant's or covered dependent's benefit profile to determine whether he or she has requested confidential communication or has objected to the sharing of PHI with friends or family members. If so, refuse to disclose information.	Name and contact information for appropriate administrator, HMO, or insurer for relevant Health Plan
Claims-related medical information	Use of PHI obtained from an Individual and disclosure to/from the appropriate claims administrator, HMO, or insurer to assist the Individual with a claim or coverage issue	Refer Individual to appropriate claims administrator.	Varies, but must be limited to one Individual and only the relevant Health Plan(s) and the particular claim.
	Use of PHI obtained from an Individual and disclosure to/from the internal claims review board responsible for reviewing a claim for benefits under final appeal	Compile PHI from Individual and/or third-party administrator and present to Employee Benefits Committee for review.	Varies, but typically limited to the Employee Benefits Committee and relevant information on a particular claim appeal.

The Hybrid Org has delegated claims processing responsibilities to its Business Associates. However, Responsible Employees with Health Plan oversight responsibilities may assist Individuals with claims or eligibility questions and problems. In such cases, the Responsible Employee may not access, use or disclose PHI to assist with claims processing activities relating to any non-Health Plan unless the Individual has provided a proper Authorization. The Responsible Employee may access, use or disclose only the Minimum Necessary PHI and will request from the Individual only the Minimum Necessary PHI needed to resolve the claim.

The Employee Benefits Committee has retained the right to a final appeal for benefit claims. In such cases, the Employee Benefits Committee shall access, use or disclose only the Minimum Necessary PHI and will request from the Individual on the Minimum Necessary PHI needed to review the appeal.

Routine Disclosures to Business Associates

The following table sets forth the Routine Transactions by a Health Plan to a Business Associate. All of the Transactions listed below have been determined to comply with the Minimum Necessary requirement. If, after referring to the tables below, a Responsible Employee is unsure about whether or what PHI can be disclosed to a Business Associate, the Responsible Employee should reach out for further guidance.

BUSINESS ASSOCIATE RECEIVING PHI	REASON FOR DISCLOSURE	MINIMUM NECESSARY PROVIDED	RESPONSIBLE EMPLOYEES SENDING PHI	FREQUENCY
Auditors	Audit of Medical program	Individual medical and prescription drug benefits, enrollment, and eligibility data	Director, Compensation & Benefits; Benefits Manager; or Benefits Administrator	Annually
Prescription Benefit Manager for prescription drug benefits	To confirm eligibility for benefits	Individual prescription drug benefits, enrollment, and eligibility data	Director, Compensation & Benefits; Benefits Manager; or Benefits Administrator	Weekly
Third Party Administrator for self-funded health benefits	To confirm eligibility for benefits	Individual medical benefit, enrollment, and eligibility data	Director, Compensation & Benefits; Benefits Manager; or Benefits Administrator	Weekly
Third Party Administrator for self-funded dental benefits	To confirm eligibility for benefits	Individual medical benefit, enrollment, and eligibility data	Director, Compensation & Benefits; Benefits Manager; or Benefits Administrator	Weekly
COBRA/FSA Administrator	To confirm eligibility for benefits	Individual enrollment and eligibility data	Director, Compensation & Benefits; Benefits Manager; or Benefits Administrator	Weekly

BUSINESS ASSOCIATE RECEIVING PHI	REASON FOR DISCLOSURE	MINIMUM NECESSARY PROVIDED	RESPONSIBLE EMPLOYEES SENDING PHI	FREQUENCY
Broker	To place or obtain insurance coverage or administrative services	Individuals' eligibility and claim data	Director, Compensation & Benefits; Benefits Manager; or Benefits Administrator	Annually, or as necessary when hiring a new provider
EAP	To confirm eligibility for benefits	Individual's eligibility and enrollment data	Director, Compensation & Benefits; Benefits Manager; or Benefits Administrator	Quarterly

Employee Benefits Committee

The Employee Benefits Committee may use or disclose Minimum Necessary PHI to make final claims determinations on appeal. As necessary, the committee may disclose Minimum Necessary PHI to a Business Associate, such as an outside medical expert, for advice or independent review.

Information Systems/IT

A Responsible Employee in Information Security or IT may use and disclose PHI for purposes of supporting the security and infrastructure of the HIPAA privacy program, assisting the Security Official in his/her duties, responding to security incidents, providing breach response assistance, and as otherwise necessary to comply with the Privacy and Security Rules. The Responsible Employee will use and disclose only the Minimum Necessary PHI to perform his or her job function.

Quality Assessment/Internal Audits

A Responsible Employee with quality assessment responsibilities may access, use or disclose PHI for purposes of performing certain internal audit functions, including, but not limited to, the following: Monitoring compliance of vendors and business associates; quality control purposes; compliance audits, including compliance with this Policy; and any other purpose as delegated by the Privacy or Security Officials.

In all cases, the Responsible Employee will use only the Minimum Necessary PHI to perform his or her job function.

Legal/Compliance Departments

Responsible Employees in the Legal and Compliance Departments may use the Minimum Necessary PHI for purposes of investigating, defending, or advising the Health Plan with regard to Payment or Health Care Operations activity, a violation or potential violation of this Policy, or any other similar Health Plan-related matter. Responsible Employees in the Legal Department must not use PHI for

non-Health Plan-related purposes, such as an employment law matter, without a proper Authorization or as otherwise permitted.

GLOSSARY

Access: Means the ability or the means necessary to retrieve, view, hear, read, write, modify, or communicate records, data or information or otherwise use any system resource.

Accounting of disclosures of PHI: A report that describes a *covered entity*'s disclosures (including those by its *business associates*) of *PHI* other than those disclosures that are excluded from the requirement like those for *treatment*, *payment*, and *health care operations*; those made with written individual authorization; and certain other disclosures.

Administrative safeguards: Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of *privacy and security measures* to protect protected health information and 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.

Administrative tribunal: An officially appointed or elected individual or judge or group of those individuals or judges, including those appointed by administrative agencies who conduct hearings and exercise judgment over specific issues.

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

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

Agent: An *agent* of the **Hybrid Org** is determined in accordance with federal common law of agency. The **Hybrid Org** is liable for the acts of its *agent*s. An agency relationship exists if the **Hybrid Org** has the right or authority to control the *agent*'s conduct in the course of performing a service on behalf of the **Hybrid Org** (i.e., give interim instructions, direct the performance of the service).

Alternative communications: Information or communications delivered to individuals in a manner different than the **Hybrid Org's** normal practice. For example, individuals may ask for delivery at an alternative address, phone number, or post office box.

Amend/Amendment: The correction of *PHI* or the addition of *PHI* to existing *PHI* contained in a *designated record set*.

Authorization: An *individual*'s written statement of agreement to the use or disclosure of protected health information when that statement includes all required elements.

Breach: The acquisition, *access*, use, or disclosure of protected health information in a manner not permitted which compromises the security or privacy of the protected health information.

Business associate: A person or entity who, 1) is not a *member* of the **Hybrid Org's** *workforce* and, 2) provides a service, performs a function, or performs an activity on behalf of the Health Plan that involves the creation, receipt, maintenance or transmission of protected health information, including but not limited to claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, benefit management, repricing, and other professional services. A Business Associate includes all employees

of the Business Associate who perform or assist in the performance of functions on behalf of the Health Plan.

Business associate agreement: Under the *HIPAA* Privacy and Security Rules, a *business associate agreement* ("BAA") is a legally binding contract entered into by and between a *covered entity* and a *business associate*. Among other things, the agreement must contain satisfactory assurances by the *business associate* that the *business associate* will appropriately safeguard protected health information.

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

Compliancy Group: Software provider for the HIPAA tool "The Guard".

Covered entity: A health plan; a health care clearinghouse; or a health care *provider* who stores or transmits protected health information in connection with a *HIPAA* transaction.

Data aggregation: The act of a *business associate* combining protected health information from multiple *covered entities* in order "to permit data analyses that relate to the *health care operations* of the respective *covered entities*."

De-Identified health information: Health information that does not identify an *individual*, and that does not contain information that can identify or link the information to the *individual* to whom the information belongs.

Designated record set: A group of records maintained by or for a *Covered entity* that is: a) medical and billing records maintained by or for a covered health care *provider* entity; b) enrollment, *payment*, claims, adjudication, and case or medical management record systems maintained by or for a health plan; or c) records used in whole or in part to make Health-plan related decisions.

Disclosure: The release, transfer, provision of *access* to, or divulging in any manner *PHI* to outside the entity holding the information.

Electronic Protected Health Information (ePHI): Any protected health information (PHI) that is created, stored, transmitted, or received in any electronic format or media.

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

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

Facility directory: A directory of **Hybrid Org's** staff.

Fundraising: An organized campaign designed to reach out to certain segments of the population to raise monies.

Genetic Information: With respect to any Individual, information about such Individual's genetic tests; the genetic tests of family members of such Individual; and the manifestation of a disease or disorder in family members of such Individual. Such term includes any request for, or receipt of, genetic

services, or participation in clinical research which includes genetic services, by such Individual or any family member of such Individual but shall not include information about the sex or age of any Individual.

Health care component: A component or a combination of components of a hybrid entity designated by the hybrid entity in accordance with Sec. 164.105(a)(2)(iii)(D).

Health Care Operations: Any of the following activities to the extent that they are related to a Covered Entity's covered functions:

1) Conducting quality assessment and improvement activities; population-based activities related to health improvement, reduction of health care costs, case management and care coordination; contacting health care providers and patients regarding treatment alternatives; and related functions that do not include treatment;
2) Reviewing competence or qualifications of health care professionals and evaluating provider and health plan performance;
3) Underwriting, enrollment, premium rating, and other activities that relate 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); provided, however, that Genetic Information may not be used or disclosed for Underwriting purposes;
4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
5) Business planning and development, such as cost-management and planning-related analysis related to managing and operating the Covered Entity, and development or improvement of coverage policies;
6) Business management and general administrative activities, including, but not limited to: (i) management activities related to implementation of and compliance with the requirements of the Privacy Rule; (ii) customer service, including the provision of data analyses for policy holders, plan sponsors, or others, provided that PHI is not disclosed to such entities; (iii) resolution of internal grievances; (iv) due diligence related to the sale, transfer, merger, or consolidation of all or part of the Health Plan with another Covered Entity, or an entity that, following such activity, will become a Covered Entity; and (v) consistent with applicable requirements of the Privacy Rule, creating De-identified Information or a limited data set; and
7) Communications to describe a health-related product or service that is covered by the Health Plan, including communications about a provider network, or the replacement or enhancement of the Health Plan, or health-related products or services available only to a Health Plan enrollee that add value to, but are not part of, the benefits; and communications for case management or care coordination and treatment alternatives, unless such communication is Marketing. Notwithstanding the foregoing, a communication shall be considered a Health Care Operation if the communication:
    a. is made by the Covered Entity, and the Covered Entity obtains an Authorization from the recipient of the communication, with respect to such communication; or
    b. is made by a Business Associate on behalf of the Covered Entity and the communication is consistent with the written contract between such Business Associate and Covered Entity.

Health Plan: The health care benefit programs offered under the Plan which are subject to HIPAA, including the medical, dental, vision, prescription drug, employee assistance, family planning, and health/flexible spending account programs. Current providers are listed in **Appendix 2**.

HHS: Stands for the Department of Health and Human Services. This agency is charged with the development, statement, and implementation of the *HIPAA* Privacy Rule.

Health Insurance Portability and Accountability Act (HIPAA): Federal legislation passed in 1996, as *amend*ed and updated from time to time, that regulates privacy and security of *individually identifiable health information*.

HIPAA Privacy Rule: The *HIPAA* Privacy Rule regulates the use and disclosure of protected health information. The *HIPAA* Privacy Rule gives *individual*s the right to *access* their protected information; the right to request that this information be *amend*ed; and the right to an accounting of how their *PHI* has been disclosed. The Privacy Rule prescribes measures that must be taken to ensure *PHI* is protected from unauthorized *access*. The Privacy Rule also requires *covered entities* to develop and use Notices of Privacy Practices, which outline how *covered entities* will use or disclose the *PHI* of *individual*s. The Privacy Rule also outlines when individual written authorization to use or disclose *PHI* is required, and when it is not required. In addition, the Privacy Rule outlines those circumstances under which *PHI* must be disclosed, and those circumstances under which it may not be disclosed.

Hybrid entity: A hybrid entity means a single legal entity:

1. that is a covered entity;
2. whose business activities include both covered and non-covered functions; and
3. that designates health care components in accordance with 45 CFR Section 105(a)(2)(iii)(D).

Hybrid Org: Vontier Employment Services, LLC, its parent companies, subsidiaries, affiliates and participating OpCos under common control or ownership as defined in 45 CFR Section 164.105 (b) as related to activities governed by HIPAA only. The list of OpCos participating in Vontier Benefits is **Appendix 1**.

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.

Individual: A person covered by the Health Plan, or a decedent previously covered by the Health Plan, who is the subject of the PHI.

Individually identifiable health information: A subset of health information, including demographic information that:

1. Is created or received by a healthcare *provider*, health plan, employer or healthcare clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an *individual*; the provision of healthcare to the *individual*; or the *payment* for the provision of health care for the *individual*; and
3. That identifies the *individual* or might reasonably be used to identify the *individual*.

Institutional Review Board (IRB): In reference to a *research* project, a board that is designated to review and approve proposed *research*, and the process by which the investigator intends to secure the informed authorization of *research* subjects.

Integrity: This describes the property that data or information has not been altered or destroyed in an unauthorized manner.

Kiteworks: A software program that provides for secure transmissions of ePHI through end-to-end encryption.

Limited Data Set: A set of identifiable healthcare information that the *HIPAA* Privacy Rule permits *covered entities* to share with certain entities for *research* purposes, public health activities, and healthcare operations without obtaining prior authorization from individuals, if certain conditions are met including the exclusion of *HIPAA* specified direct identifiers of the *individual*, or of relatives, employers or household members of the *individual*.

Malicious software: Software, for example, a virus, designed to damage or disrupt a system.

Marketing: The provision of information about a product or service that encourages recipients of the communication to purchase or use the product or service. However, the following items are excluded from the definition of marketing for purposes of this policy manual:

a) communications about a drug currently prescribed for an individual unless the covered entity sending it is reimbursed in excess of the cost of the communication;
b) unless the *covered entity* making the communication receives remuneration, communications for *treatment* and *health care operations* of the following types are not marketing: For *treatment* of an *individual* by a health care *provider*, including case management or care coordination for the *individual*, or to direct or recommend alternative *treatment*s, therapies, health care *providers*, or settings of care to the *individual*;
c) To describe a health-related product or service (or *payment* for such product or service) that is provided by, or included in a plan of benefits of, the *covered entity* making the communication, including communications about: the entities participating in a health care *provider* network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or
d) For case management or care coordination, contacting of *individual*s with information about *treatment* alternatives, and related functions to the extent these activities do not fall within the definition of *treatment*.

Medical Record: documents, notes, forms, and test results that collectively document health and healthcare services for an *individual* including but not limited to medical history, care or *treatment*s received, medications prescribed or taken, test results, diagnosis and prognosis. *Psychotherapy notes* are excluded from the definition of *medical record* as are peer review documents when they are covered by a legal privilege.

Minimum Necessary Standard: The use of reasonable efforts to limit the use or disclosure of *PHI* to the minimum necessary to accomplish the intended purpose.

Notice of Privacy Practices: A document required by the *HIPAA* Privacy Rule. The Notice of Privacy Practices provides *individual*s with information on how an Hybrid Org will use or disclose their *PHI*, what the Hybrid Org's responsibilities are, and what *individual*s' rights are with respect to that *PHI*.

Office for Civil Rights (*OCR*): The branch within the Department of Health and Human Services that enforces *HIPAA*.

Opt-out: To make a choice to be excluded from communications or practices.

Payment: Activities: 1) undertaken by a health care provider or health plan to obtain or provide reimbursement for the provision of health care; and 2) activities undertaken by a health plan to obtain premiums or to determine the full extent of its coverage and benefit provision under the health plan. Activities for *payment* include eligibility of coverage determination, billing, claims management, collection activities, medical necessity determinations, risk adjustments, utilization review including precertification, preauthorization, concurrent and retrospective review of services, and specified disclosures to consumer reporting agencies. In no event shall Genetic Information be used or disclosed for Underwriting Purposes.

Password: Confidential *authentication* information composed of a string of characters.

Personal representative: One who, under law, has the authority to act on behalf of an *individual* in making decisions related to health care or in exercising the *individual*'s rights related to their protected health information. A Personal representative is entitled to act on behalf of an individual under this Policy. *Personal representative*s' rights are limited in certain circumstances.

Physical safeguards: Physical measures, policies, and procedures to protect a covered entity's or business associate's electronic *information system*s and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Privacy Breach: Any unauthorized or unpermitted *access*, use, disclosure, modification, or destruction of *unsecured PHI* in any form.

Privacy incident: Any attempted or successful unpermitted or unauthorized *access*, use, disclosure, modification, interference or destruction of *unsecured PHI* in any form.

Privacy Officer: **Hybrid Org's** designated *individual* who is responsible for overall compliance with the *HIPAA* Privacy Rule and for development and implementation of *HIPAA* policies and procedures.

Protected Health Information (PHI): *PHI* is *individually identifiable health information* that is created, received, transmitted, or maintained by a *covered entity* or *business associate* in any form or medium. *PHI* excludes information regarding persons deceased for more than 50 years, information in education records (which are protected by other laws) and information in employment records held by a *covered entity* in its role as an employer. It includes genetic and demographic information.

Privacy Rule: The HIPAA security standards and implementation specifications at CFR Parts 160 and 164 (subparts A and C).

Provider: A *provider* of medical or health services, and any other person or entity who furnishes, bills for, or is paid for health care in the normal course of business.

Psychotherapy notes: Notes recorded in any medium by a mental health professional documenting or analyzing the contents of a conversation during a counseling session that are separated from the rest of the *medical record*. *Psychotherapy notes* do not include medication prescription and monitoring, session start and stop times, modalities and frequency of *treatment*, clinical test results, or summary information on diagnosis, functional status, *treatment* plan, symptoms, prognosis, and progress to date.

Research: A systematic investigation designed to develop or contribute to generalized knowledge. *Research* is conducted through development, testing, and evaluation.

Responsible Employee: Vontier employee (including, for purposes of this Policy a contract, temporary, or leased employee) whose duties (i) require that the employee have access to PHI to perform administrative functions on behalf of the Health Plan, or (ii) make it likely that he or she will receive or have access to PHI on behalf of the Health Plan. Persons designated as Responsible Employees are described in the Policy and a current list is attached as **Appendix 3.** Any other Vontier employee, not so designated, who creates, discloses, or receives PHI on behalf of the Health Plan is treated as a Responsible Employee under the Policy, even though his or her duties do not (or are not expected to) include creating, disclosing, or receiving PHI.

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

Security incident: A *HIPAA security incident* is an attempt (which can be successful or not) to do something unauthorized. The "something" that is unauthorized, is an unauthorized *access*, use, disclosure, modification, destruction, or interference with *ePHI*.

Security measures: Encompasses all of the administrative, physical, and *technical safeguards* in an *information system*.

Security Rule: The HIPAA security standards and implementation specifications at CFR Parts 160 and 164 (subparts A and C).

Technical safeguards: The technology and the policy and procedures for its use that protect electronic protected health information and control *Access* to it.

The Guard: Compliancy Group's software program for HIPAA compliance.

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

Unsecured PHI: *PHI* that is not been rendered unusable, unreadable, or indecipherable to unauthorized *individual*s though the use of a technology or methodology specified by the *HHS* Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

Use: To share, employ, apply, utilize, examine, or analyze *individually identifiable health information*.

User: A person or entity with authorized *Access*.

Whistleblower: An *individual* who reveals wrongdoing within a Hybrid Org to the public, government agencies, or to those in positions of authority.

Workstation: An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

[SIGNATURES ON NEXT PAGE]

Executed and effective on 2/12/2024.

VONTIER EMPLOYMENT SERVICES, LLC

Signature: Courtney Kamlet

Name: Courtney Kamlet

Title: VP, Group GC & Corporate Secretary

Date: 2/12/2024

PRIVACY OFFICIAL

Signature: Srikant Mikkilineni

Name: Srikant Mikkilineni

Title: Senior Counsel, Global Privacy and Data Protection

Date: 2/12/2024

APPENDICES AS OF 2/12/2024

Appendix 1. Companies participating in Vontier Benefits

- ANGI
- DRB
- EVolve
- Gilbarco Veeder-Root
- Invenco by GVR
- Matco Tools Corporation
- Teletrac Navman
- Vontier

Appendix 2. 2024 Healthcare Benefit Providers

Vendor Name	Type	Contact	Website
bswift	Plan Administrator	877-927-9438	bswift.com
Cigna Dental	Dental	800-244-6224	mycigna.com
CVS Caremark	Pharmacy	888-964-0034	caremark.com
Health Advocate	Personal Benefits Consultant	866-799-2731	healthadvocate.com/members
Health Equity	FSA/HSA	877-924-3967	healthequity.com
Maven Clinic	Fertility and Family Building	mavenclinic.com/join/Vontier	mavenclinic.com
United HealthCare Services	Medical	833-805-7672	myuhc.com
Vision Service Plan	Vision	800-877-7195	vsp.com

Appendix 3. Responsible Employees

Last Name	First Name	Email	Job Title	Supervisor
Alf	Brittany	brittany.alf@angienergy.com	Sr. People and Culture Business Partner	Nicole Baird
Anderson	Joey	joey.anderson@gilbarco.com	Sr. People and Culture Business Partner	Caitlin Newsholme
Anderson	Trish	trish.anderson@veeder.com	People & Culture Business Partner	Hannah Lewis
Ankney	Megan	m.ankney@drb.com	Senior Payroll Analyst	Christi McReynolds
Bailey	Bi'Anca	bi'anca.bailey@teletracnavman.com	People & Culture Business Partner	Kim McCormick
Brushaber	Mariah	m.brushaber@drb.com	Payroll Analyst	Christi McReynolds
Bury	Melissa	mbury@veeder.com	Director, NA People Operations	Tina Hubert
Cole	Jennifer	jennifer.cole@gilbarco.com	Director, People and Culture, Fueling Soluti	Tina Hubert
Cooper	Caroline	ccooper@drb.com	Sr. Manager, HR	Jennifer Segreti
Cooper	Evette	evette.cooper@gilbarco.com	Sr. People & Culture Business Partner	Tessa Hunsicker
Corlat	Adriana	adriana.corlat@vontier.com	Service Delivery Manager, Apps & Reportin	William McMurray
Creque	Abby	acreque@drb.com	Talent Development Specialist	Brittany Mackey
Cudney	Heidi	heidi.cudney@vontier.com	Total Rewards Project Manager	Danielle Riddell
DeLaRosa	Pablo	pablo.delarosa@vontier.com	Senior Director, Security Response, Resilien	Raj Samprathi
Deveci	Ozgur	ozgur.deveci@vontier.com	Director, Digital Workplace Services	Peter McIntosh
Doherty	Jessica	jess.doherty@vontier.com	VP, HR Transformations & Corporate	Jennifer Paylor
Doss	Kelley	kelley.doss@vontier.com	Director, HRIS and Payroll	Mike Lee
Eastham	Robin	robin.eastham@vontier.com	Senior Benefits Manager	Angela Powell
Engle	Courtney	courtney.engle@matcotools.com	Associate HR Generalist	Ontoinette Threatt
Espinal	Lissette	lissette.espinal@vontier.com	Lead HR Systems Analyst	Mike Lee
Graye	Susan	susan.graye@vontier.com	Director, Talent Acquisition	Jennifer Paylor
Hare	Kenneth	kenneth.hare@vontier.com	HR Support Assistant	Mandy Henderson
Hazeley	Tracy	thazeley@insite360suite.com	People Operations Specialist	Melissa Bury
Henderson	Mandy	mandy.henderson@vontier.com	HR Generalist	Jessica Doherty
Heuser	Emily	emily.heuser@gilbarco.com	Director, HR Global Functions	Joy Snow
Hidalgo	Carol	carol.goodman.hidalgo@matcotools.com	Human Resource Supervisor	Jonathan Miller
Hubert	Christina	tina.hubert@gilbarco.com	Vice President, People and Culture, Fueling	David Coombe
Hunsicker	Tessa	thunsicker@gilbarco.com	Director, People & Culture- FS Global Opera	Tina Hubert
Hunt	Cathi	cathi.hunt@vontier.com	VP & Associate General Counsel Labor & Er	Katie Rowen
Ifland	Kelly	kelly.ifland@ammcoats.com	Human Resources Business Partner	Marissa Wibel
Jackson	Shontiana	shontiana.jackson@ammcoats.com	HR Coordinator	Marissa Wibel
Jackson	Vania	vania.jackson@gilbarco.com	People & Culture Generalist	Joy Snow
Jones	Tamie	tamie.jones@gilbarco.com	Sr. People & Culture Business Partner	Tessa Hunsicker
Kim	Hongseok	hongseok.kim@vontier.com	Manager, Information Security Governance	Michael Sheedy
Krueger	Kimberly	kimberly.krueger@vontier.com	HR Systems Analyst	Lissette Espinal
Lee	Michael	mike.lee@vontier.com	Vice President, Human Resources Technolo	Jennifer Paylor
Lewis	Hannah	hannah.lewis@gilbarco.com	Director, People and Culture, Global Eng, P	Tina Hubert
Lindskold	Eric	eric.lindskold@veeder.com	People and Culture Manager, Altoona	Tessa Hunsicker
Lopez	Ricardo	ricardo.lopez@vontier.com	Digital Workplace Engineer	Ozgur Deveci
Maas	Taylor	taylor.maas@angienergy.com	Sr. People and Culture Business Partner	Nicole Baird
Mackey	Brittany	bmackey@drb.com	Sr. Manager, Talent Management	Jennifer Segreti
Mathews	Amy	amathews@drb.com	Talent Acquisition Partner	Brittany Mackey
Matyoka	Frank	frank.matyoka@gilbarco.com	Director, EH&S (Americas)	Mark Williams
Maxwell	Jaret	jmaxwell@drb.com	HR Specialist	Caroline Cooper
McCall	Matthew	matthew.mccall@gilbarco.com	Director, People & Culture Labor Relations	
McRae	Benita	benita.mcrae@gilbarco.com	Director, People and Culture, North Americ	Mark Williams
McReynolds	Christi	cmcreynolds@drb.com	Associate Manager, HR	Caroline Cooper
Mikkilineni	Srikant	srikant.mikkilineni@vontier.com	Sr. Counsel Privacy and Data	Kelly Clement
Miller	Jonathan	jonathan.miller@matcotools.com	VP, Human Resources	Timothy Gilmore
Montes	Jennifer	jennifer.montes@matcotools.com	HR Generalist	Ontoinette Threatt
Murphy	Lynn	lynn.murphy@vontier.com	Commercial Contracts and Data Protection	Courtney Kamlet
Newsholme	Caitlin	caitlin.newsholme@gilbarco.com	Sr. People and Culture Manager, GSO Oper	Tessa Hunsicker
Paylor	Jennifer	jennifer.paylor@vontier.com	HR Team - VP, Talent and ID&E	Katie Rowen
Powell	Angela	angela.powell@vontier.com	Director, Benefits	Danielle Riddell
Prudente	Emily	emily.prudente@vontier.com	Corporate Compliance Analyst	Kelly Clement
Ra	Harry	harry.ra@vontier.com	HR System Administrator	Kelley Doss
Riddell	Danielle	danielle.riddell@vontier.com	Vice President, Total Rewards	Jennifer Paylor
Ridgley	Rebecca	rridgley@vontier.com	Talent Solutions Program Manager	Jennifer Paylor
Roberts	Moriah	m.roberts@drb.com	Senior HR Business Partner	Caroline Cooper