HIPAA SECURITY AND PRIVACY POLICY & PROCEDURE MANUAL FOR SOFTWARE AS A SERVCE (SAAS) and APPLICATION ENTITIES

Company Name: Will be referred to as UIW throughout each policy.	**University of the Incarnate Word**
Policy Name:	Security Policy Privacy Policy
Policy Version:	Version 1.3
Effective Date:	2023
Review Date:	Yearly
Security Officer: Will be referred to as Security Officer throughout each policy.	**Brian Anderson**
Privacy Officer: Will be referred to as Privacy Officer throughout each policy.	**Vanessa Martinelli**
Compliance Officer: Will be referred to as Compliance Officer throughout each policy.	**Allyson Medina**
Responsible for Review:	

TABLE OF CONTENTS

HIPAA Confidentiality Agreement

As an employee of **UIW**, I understand that **UIW**, a covered entity under the HIPAA regulations, has a legal responsibility to protect the privacy and security of patient Protected Health Information (PHI) and Electronic Protected Health Information (ePHI).

During the course of my employment with **UIW**, I may see, hear, or touch Protected Health Information (PHI), Electronic Protected Health Information (ePHI), and other information that **UIW** 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 the facility, equipment, or computer systems confidential at all times.
- When my employment with UIW is terminated or completed, I will immediately return all property to UIW. This property includes, but is not limited to, keys, access cards, UIW documents however stored or maintained, and ID badges.
- 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.

Attestation

I hereby attest and acknowledge that I have read and understood the contents of this HIPAA Security Policy and Procedure Manual. Through my attestation, I hereby confirm that I am bound by **UIW's** security policies and procedures and will perform my job duties accordingly. I understand that if I violate any UIW security policy or procedure, I am subject to disciplinary action, up to and including termination of my employment.

I hereby acknowledge and agree that this attestation is the equivalent of a physical or e-signature.

University of the Incarnate Word Security Manual Synopsis

This section is for all employees to review and attest. Below is a summary of each policy, including the relevant HIPAA regulations. To view the full policy of a section, please click on the title of that section in the synopsis.

Definitions for the terms used in this Security Manual are included in the Glossary at the end of the manual.

Security 1.0 Assigned Security Responsibility

UIW shall have one individual identified and assigned to HIPAA security responsibility (the "HIPAA Security Officer").

The HIPAA Security Officer is responsible for ensuring UIW**'s** HIPAA Security Rule policies and procedures are implemented and followed in each department.

§164.308(a)(2) *Assigned security responsibility*

Security 2.0 User Access Management

UIW must safeguard the confidentiality, integrity, and availability of electronic protected health information. To do this, UIW must manage who can access ePHI, implementing **user access** measures.

Before users are given access, UIW must train users in basic information security awareness. Once prerequisites have been satisfied, management and supervisors shall grant access to employees, under specific rules set forth in this policy. Access must be limited to what is necessary for a workforce member to perform his or her job.

Managers and supervisors must modify or terminate access when access has been compromised, is no longer needed, or when an employee terminates or is absent from employment. Under certain circumstances, management may grant itself emergency access, or may grant emergency access to individuals who have yet to complete training.

UIW must routinely review user access rights to ensure continuous compliance with this policy. Upon such review, UIW must update or modify user access rights, as necessary.

§164.308(a)(3)(i) *Workforce security*
§164.308(a)(3)(ii)(A) *Authorization and/or supervision*
§164.308(a)(3)(ii)(B) *Workforce clearance procedure*
§164.308(a)(3)(ii)(C) *Termination procedures*
§164.308(a)(4)(i) *Information access management*

§164.308(a)(4)(ii)(B) *Access authorization*
§164.308(a)(4)(ii)(C) *Access establishment and modification*
§164.312(a)(1) *Access control*
§164.312(c)(1) *Integrity*
§164.312(a)(2)(ii) *Emergency access procedure*

Security 3.0 Authentication & Password Management

Passwords are the first line of defense in protecting user accounts and the information contained in those accounts. All workforce members are required to comply with the Authentication & Password Management policy to ensure that their passwords are strong enough to protect the sensitive information in user accounts.

The policy consists of:

- Standards of Authentication – Verification
- The rules for maintaining Unique User ID and Password Management
- The guidelines for appropriate User ID and Passwords

UIW shall implement unique user IDs for each employee. Password guidelines, which incorporate best practices from the latest National Institute of Standards and Technology (NIST) guidelines (set forth in NIST SP 800-63B) are set forth below, and shall be used by **UIW.**

1. Passwords shall be a minimum of eight (8) characters in length and be a maximum length of at least sixty-four characters.
2. **UIW** and its workforce shall have the ability to use all special characters. **UIW** does not require that special characters be used. However, passwords shall be restricted as follows:
    a. Use of sequential and repetitive characters (i.e., 12345 or aaaaa) shall be restricted.
    b. Use of context-specific passwords (i.e., name of UIW site) shall be restricted.
    c. Use of commonly used passwords (i.e., p@ssw0rd, etc.) shall be restricted.
    d. Passwords obtained from previous security breaches shall not be used.
3. Password protection requirements for users:
    a. Never reveal a password over the phone to anyone.
    b. Never reveal a password in an email message.
    c. Never reveal a password to your supervisor.
    d. Never talk about a password in front of others.
    e. Never hint at the format of a password (i.e., "my family name").
    f. Never reveal a password on questionnaires or security forms.
    g. Never share a password with family members.
    h. Never reveal a password to co-workers.
    i. Never write down your password; instead, memorize it.
    j. Never keep a list of user IDs and passwords in your office; and

k. Never misrepresent yourself by using another person's user ID and password.

§164.312(c)(2) *Mechanism to authenticate electronic protected health information*
§164.312(d) *Person or entity authentication*
§164.308(a)(5)(ii)(D) *Password management*
§164.312(a)(2)(i) *Unique user identification*

Security 4.0 Facility Access Controls

UIW must develop and implement facility access controls. These controls are a series of measures to safeguard ePHI stored in a physical location or its equipment.

Safeguard measures under a facility security plan include controlling workforce and visitor access; proper use and securing of metal/hard keys, network closets, server rooms, alarm systems, and doors. These measures are required to prevent unauthorized physical access and theft.

These procedures allow facility access to appropriate persons, so they can access data in an emergency.

When a facility undergoes repairs or modifications, these modifications must be logged and tracked, in accordance with this policy. When **UIW** remodels existing sites or designs a new facility, it must revise its existing facility security plans, or create new ones, accordingly. All new and revised facility security plans must be evaluated on an ongoing basis and approved by **UIW's** compliance officers.

UIW must conduct annual facility audits. These audits must ensure that ePHI safeguards for existing sites are being continuously maintained.

§164.310(a)(2)(ii) *Facility security plan*
§164.310(a)(1) *Facility access controls*
§164.310(a)(2)(iii) *Access control and validation procedures*
§164.310(a)(2)(iv) *Maintenance records*
§164.310(a)(2)(i) *Contingency operations*

Security 5.0 Workstation Access Controls

UIW **must adequately shield** all observable ePHI from unauthorized disclosure or access on computer screens. **UIW's** workforce members must ensure that ePHI and other confidential information on computer screens is not visible to unauthorized persons.

Since ePHI is portable, workforce members must protect ePHI in *all* locations, including, but not limited to, homes or client sites.

The policy covers specific requirements for:

- Workforce members who work in other facilities.
- Workforce members who work from home or other non-office sites.
- Password protection of workforce member personal computers.
- Security for all other forms of portable ePHI, such as locking up CD ROM Disks, floppy disks, USB drives, PDAs, and laptops.
- Automatic, time-based user session-lock when a computer or workstation is left idle.
- Accessing (by, i.e., VPN) ePHI outside **UIW's** Wide Area Network (WAN).

Workforce Member Requirements:

- Session locks the computer when it is left unattended.
- Ensure the computer is set to automatically lock when the computer is not in use.
- Ensure that no confidential information is viewable by unauthorized persons; and
- When working from home or other non-office work sites, protect ePHI from unauthorized access or viewing.

§164.310(a)(2)(iii) *Access control and validation procedures*
§164.310(b) *Workstation use*
§164.310(c) *Workstation security*
§164.312(a)(2)(iii) *Automatic log off*

Security 6.0 Device and Media Controls

ePHI stored or transported on storage devices and removable media, such as thumb drives and external hard drives, must be properly controlled and managed. Media containing PHI must also be properly backed up and disposed of.

Workforce Responsibilities:

1. Individual workforce members shall track laptops, PDAs, CD ROM Disks, and floppy disks, and all other portable media that contain ePHI.
2. To limit the amount of portable ePHI, workforce members shall not save any ePHI onto floppy disks, CD ROMs, and other portable items when it is not necessary.
3. Workforce members shall remove and destroy all ePHI before disposing of the media.

§164.310(d)(1) *Device and media controls*
§164.310(d)(2)(i) *Disposal*
§164.310(d)(2)(ii) *Media reuse*
§164.310(d)(2)(iii) *Accountability*
§164.310(d)(2)(iv) *Data backup and storage*

Security 7.0 Audit Controls

UIW's IT team must conduct a security audit on **UIW's** computing resources.

Audits let the IT Team know whether safeguards are working. Audits may be conducted to:

1. Ensure integrity, confidentiality, and availability of information and resources.
2. Investigate security incidents to ensure conformance to **UIW's** IT and security policies.
3. Monitor user or system activity where appropriate.
4. Verify that software patching is being maintained at the appropriate security level.
5. Verify that virus protection is being maintained at current levels.

§164.308(a)(5)(ii)(C) *Log-in monitoring*
§164.308(a)(1)(ii)(D) *Information system activity review*
§164.312(b) *Audit controls*

Security 8.0 Incident Response & Reporting

UIW must identify, track, respond to, and report security incidents. In addition, **UIW** must mitigate the harmful effects of such incidents.

Workforce Members:
Workforce members are responsible for promptly reporting any security-related incidents to the Security Officer.

§ 164.308(a)(6)(i) *Security incident procedures*
§ 164.308(a)(6)(ii) *Response and reporting*

Security 9.0 Transmission Security

UIW must guard against unauthorized access to, or modification of, ePHI transmitted over an electronic communications network ("data in motion"). UIW shall commit resources to ensure that when ePHI is transmitted from one point to another, the ePHI is sufficiently protected to mitigate associated risk. Encryption measures play vital role in protecting ePHI.

§164.312(e)(1) *Transmission security*
§164.312(e)(2)(i) *Integrity controls*
§164.312(e)(2)(ii) *Encryption*

Security 10.0 Protection from Malicious Software

UIW must install and maintain anti-virus software on computers it owns, leases, and/or operates; and configure all workstations to activate and update anti-virus software automatically, each time the computer is turned on, or, when a user logs onto the network. If a virus, worm, or other malicious code has infected or been identified on a server or

workstation, UIW must minimize the damage such code may cause. Workforce members must maintain cyber-hygiene standards.

Workforce Responsibilities:

1. Workforce members who utilize laptops to log on to the network shall work with their IT support to ensure all updates are received.
2. Workforce members shall not disable automatic virus or automatic malware scanning features.
3. All **non-UIW** computers that directly access the WAN shall have anti-virus software and anti-malware software and remain current with updates.
4. All downloaded files shall be malware-checked and virus-checked prior to use.
5. All storage media (i.e., disks) shall be treated as if they contain viruses or malware. Workforce members are permitted to use removable storage disks provided that all disks are virus-checked and malware-checked prior to use.
6. If a virus or malware is detected, workforce members are instructed to immediately contact their Security Officer.
7. For the purposes of protecting data and preventing the spread of malware, workers shall:
    - Attend HIPAA Security Training; and
    - Maintain back-up copies of data files.

§164.308(a)(5)(ii)(B) *Protection from malicious software*

Security 11.0 Contingency Plan, Disaster Recovery

Disasters and other emergencies may disrupt business continuity. Disasters include active hurricanes, tornadoes, shooter situations, war, and acts of terrorism. Other emergencies include fire, flood, pandemic, or outbreak. UIW must be prepared to respond to emergencies by creating, evaluating, testing, and updating contingency plans. Contingency measures include:

- Applications and data criticality analysis.
- Data backup.
- Disaster Recovery Plan; and
- Emergency Mode Operation Plan.

§164.308(a)(7)(i) *Contingency plan*
§164.308(a)(7)(ii)(A) *Data backup plan*
§164.308(a)(7)(ii)(B) *Disaster recovery plan*
§164.308(a)(7)(ii)(C) *Emergency mode operation plan*
§164.308(a)(7)(ii)(D) *Testing and revision procedures*
§164.308(a)(7)(ii)(E) *Applications and data criticality analysis*
§164.310(a)(2)(i) *Contingency operations*

Security 12.0 Business Associates

Business associates perform services for **UIW** involving access to electronic protected health information. Such relationships must be formalized in a legally binding contract called a business associate agreement. Business associate performance under these agreements must be monitored. **UIW** must act on complaints it receives about business associates.

§164.308(b)(1) *Business associate contracts and other arrangements*
§164.308(b)(3) *Written contract or other arrangement*

Security 13.0 Monitoring and Effectiveness

UIW must periodically evaluate its compliance with HIPAA security standards, by conducting security assessments. Assessments determine whether security controls have been properly implemented. When risk assessments are complete, **UIW** will conduct risk management to remediate flaws revealed by the assessment.

§164.308(a)(8) *Perform a periodic technical and non-technical evaluation*
§164.308(a)(1)(i) *Security management process*
§164.308(a)(1)(ii)(A) *Risk analysis*
§164.308(a)(1)(ii)(B) *Risk management*

Security 14.0 Security Awareness and Training

All members of **UIW's** workforce who can access ePHI must receive training needed to:

- Implement and maintain UIW**'s** HIPAA Security Policies and Procedures; and
- Comply with the HIPAA Security Rule.

Security Awareness Training is key to eliminating UIW**'s** exposure to both malicious threats and accidental errors and omissions.

§ 164.308(a)(5)(i) *Security awareness and training*
§ 164.308(a)(5)(ii)(A) *Security reminders*

Security 15.0 Sanctions Policy

Sanctions, penalties, and disciplinary actions must be applied against workforce members who fail to comply with security policies and procedures. Workforce members must report security incidents. Workforce members are protected from retaliation for reporting such incidents.

§ 164.308(a)(1)(ii)(C) *Sanction policy*

Security 16.0 Policies and Procedures

UIW must develop and implement HIPAA Security Rule policies and procedures. These procedures must be revised when changes in regulations or changes in the work environment take place. These policies and procedures must be regularly reviewed. Reviews must be documented.

§ 164.316(a) *Policies and procedures*
§164.316(b)(1) *Documentation*
§164.316(b)(2)(i) *Time limit*
§164.316(b)(2)(ii) *Availability*
§164.316(b)(2)(iii) *Updates*

Security 17.0 Satellite Office and Home Office Policy

Satellite and Home Offices are offices that directly perform services for covered entities or business associates. PHI may not be stored in these offices. Devices used in these offices must be protected and encrypted.

Security 18.0 Work from Home Policy

Telecommuting is a voluntary work arrangement that allows employees to perform their jobs at home as part of the regular workweek. Employees who telecommute must observe proper security procedures.

Security 19.0 Bring Your Own Device Policy

UIW may allow employees to conduct work using their personally owned devices to access UIW's resources and services. Employees must take proper security precautions so the security and integrity of UIW's data and technology infrastructure remains maintained.

Security 20.0 Clean Desk Policy

To reduce the risk of security breaches, **UIW** has established a clean desk policy. Under this policy, sensitive or confidential materials may not be kept in open spaces that can be accessed by individuals other than authorized employees. When such items are not in use, and whenever an employee leaves his or her workstation, the employee must remove the items from open workspace areas and securely lock them away.

§164.310(c) *Workstation Security*

Privacy Manual Synopsis

This section is for all employees to review and attest. Below is a summary of each policy, including the relevant HIPAA regulations. To view the full policy of a section, please click on the title of that section in the synopsis.

Definitions for the terms used in this Privacy Manual are included in the Glossary at the end of the manual.

Privacy 1.0 HIPAA Privacy Program

UIW's Privacy Officer oversees **UIW's** compliance with the HIPAA Privacy Rule. The Privacy Officer oversees **UIW's** efforts to secure and maintain the confidentiality of protected health information (PHI), maintain sensitive UIW information, and prevent and detect inappropriate and illegal uses and disclosures of PHI. Employees must be familiar with the Privacy Officer's job functions and must contact the Privacy Officer when this Policy requires that they do so.

§164.530 *HIPAA Privacy Program*

Privacy 2.0 Accounting of Disclosures

Individuals have the right to receive an **accounting of disclosures** of their protected health information ("PHI") that have been made by **UIW** to another entity, including disclosures to or by business associates. Individuals can exercise this right by making a written request to **UIW** for an accounting. **UIW** must properly respond to the request, and send the accounting when appropriate.

45 CFR § 164.528(a) *Accounting for Disclosures*

Privacy 3.0 Business Associates

UIW relies on business associates, which are vendors that handle **UIW** functions that require access to PHI. This policy covers how **UIW's** workforce determines who is a business associate. The policy then covers the details and requirements of the business associate contract UIW, and a business associate must enter into.

§ 164.502(e)(1) *Disclosures to Business Associates*
§ 164.504 *Uses and Disclosures: UIWal Requirements*

Privacy 4.0 Judicial and Administrative Proceedings

UIW must disclose a patient's PHI when that PHI is sought in a judicial or administrative proceeding. Such proceedings include court proceedings, and proceedings before government agencies, such as the Department of Health and Human Services ("HHS") and

the Centers for Medicare and Medicaid Services ("CMS"). Employees will be trained in how to respond to requests for PHI sought in these proceedings.

§164.512(e) *Use and Disclosure of PHI for Judicial and Administrative Proceedings*

Privacy 5.0 Uses and Disclosures for Marketing

UIW may use or disclose PHI for certain marketing purposes. **UIW** may not use or disclose PHI for marketing activities that are purely commercial. Employees will be trained as to when PHI can be disclosed for marketing activities.

164.508 (a)(3) *Uses and Disclosures for Which an Authorization is Required: Marketing*

Privacy 6.0 Minimum Necessary

Under the minimum necessary standard, **UIW** may only use, request, or disclose PHI that is necessary to fulfill a request, or perform a job function. Employees will be trained to this standard so that PHI is used, requested, or disclosed only to the extent that is legally required.

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

Privacy 7.0 Uses and Disclosures for Which an Authorization is Required

Under certain circumstances, written patient authorization is necessary prior to UIW's use or disclosure of that patient's individual's PHI. Written patient authorization must be validly obtained. This policy describes when written authorization is required, and what constitutes a valid authorization.

§164.508 *Uses and Disclosures for Which an Authorization is Required*

Privacy 8.0 Uses and Disclosures, No Authorization Required

Under certain circumstances, **UIW** may use and disclose PHI when neither authorization nor an opportunity for a patient to agree or object is required. This policy informs employees of what those circumstances are, and what steps employees must take to fulfill requests for PHI.

§164.501 *Uses and Disclosures for Health Care Operations*
§164.512 *Consent or Authorization Not Required*

Privacy 9.0 Uses and Disclosures Requiring Patient Opportunity to Agree or Object

Under some circumstances, **UIW** must provide a patient the opportunity to agree or object to disclosure of PHI. This policy covers how **UIW** responds to such requests made when these circumstances apply.

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

Privacy 10.0 Complaints About UIW

UIW must have a complaint process, under which individuals may make complaints about UIW's compliance with the HIPAA Privacy Rule, the HIPAA Breach Notification Rule, and UIW's policies and procedures related to these rules.

45 CFR 164.530(d) *Complaints*

Privacy 11.0 Sanctions

Workforce members who violate **UIW's** privacy policy and procedures are subject to sanctions. Sanctions are disciplinary measures intended to deter future violations. UIW, in deciding upon the appropriate sanction, may review the severity of the violation, the impact of the violation, and the workforce member's work history. Sanctions imposed should be consistent, and proportional with the severity of the offense.

45 CFR 164.530(e) *Sanctions*
45 CFR 164.530(f) *Mitigation*

Privacy 12.0 No Retaliation; No Waiver of Rights

UIW shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who exercises his or her rights under the Privacy Rule, including the right to file a complaint about UIWs privacy policies, practices, and procedures. In addition, UIW shall not require any person to waive these rights as a condition of the provision of treatment or payment for healthcare.

45 CFR 164.530(g) *Refraining from Intimidating or Retaliatory Acts*
45 CFR 164.530(h) *Waiver of Rights*

Privacy 13.0 Uses and Disclosures for Treatment, Payment, and Healthcare Operations

UIW is not required to obtain written patient authorization to use or disclose PHI under certain circumstances. When UIW uses or discloses PHI for purposes of treatment, payment, or healthcare operations, UIW need not obtain such authorization, except for certain exceptions, and when required to do so by state law.

45 CFR 164.506 *Treatment, Payment, or Healthcare Operations*

Privacy 14.0 Sale of PHI

UIW will not engage in activities constituting the sale of patient PHI, unless prior written patient authorization is obtained. "Sale of PHI" is the indirect or direct receipt of remuneration, including non-financial benefits such as in-kind benefits, in exchange for patient PHI.

45 CFR 164.508(a)(4) *Sale of PHI*

Privacy 15.0 Policy for Disclosures by Whistleblowers and Workforce Member Crime Victims

Workforce members and business associates have the right to disclose PHI if they believe another workforce member or business associate has engaged in conduct that violates the HIPAA regulations, or UIW's policies and procedures relate to those regulations. In addition, workforce members who are the victims of a crime may disclose PHI about the suspected perpetrator to law enforcement officials.

45 CFR 164.502(j) *Disclosures by Whistleblowers and Workforce Member Crime Victims*

Privacy 16.0 Use or Disclosure of PHI for Specialized Government Functions

UIW may use and disclose PHI without written patient 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; and
- Correctional institutions and other law enforcement custodial situations.

45 CFR 164.512(k) *Uses and Disclosures for Specialized Government Functions*

Privacy 17.0 Limited Data Set and Data Usage Agreements

UIW 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 UIW obtains a signed, written Data Use Agreement (DUA) from the person or entity to whom the limited data set is to be disclosed.

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

FULL POLICY LANGUAGE:

Policy Purpose:

At all times, **UIW** shall have one individual identified and assigned to HIPAA security responsibility (the "HIPAA Security Officer").

Policy Description:

The HIPAA Security Officer is responsible for **UIW's** compliance with the HIPAA Security Rule. The HIPAA Security Officer is responsible for ensuring that **UIW's** HIPAA Security Rule policies are implemented and followed.

Responsibilities include:

1. Ensuring that the necessary and appropriate HIPAA related policies are developed and implemented. These policies must provide for safeguarding the integrity, confidentiality, and availability of electronic protected health information (ePHI) within UIW.
2. Ensuring that the necessary infrastructure of personnel, procedures, and systems are in place:
    a. To develop and implement the necessary HIPAA policies.
    b. To monitor, audit, and review compliance with all HIPAA policies; and
    c. To provide a mechanism for reporting incidents and HIPAA security violations.
3. Acting as a spokesperson and single point of contact for UIW with respect to all HIPAA security issues**.**
4. Fulfilling all other duties documented within Security Officer's written job description and job title (which documentation shall be created by **UIW)**.

Policy Responsibilities:

All HIPAA Security Officer responsibilities shall be assigned to this person.

The HIPAA Security Officer shall carry out the assigned responsibilities in coordination with their Job Description.

RELEVANT HIPAA REGULATIONS:

- § 164.308(a)(2) *Assigned security responsibility*

FULL POLICY LANGUAGE:

Policy Purpose:

The intent of this policy is to establish rules for authorizing access to areas where ePHI is accessible. These areas include, but are not limited to, the computing network, applications, and workstations. Workforce members requiring access to ePHI will need authorization to work with ePHI in locations in which it resides.

This workforce security policy ensures that only workforce members who require access to ePHI for work-related activities shall be granted access. When work activities no longer require access, authorization shall be terminated. In addition, this policy provides guidelines on how workforce access is routinely reviewed and updated.

Policy Description:

Management and Access Control:

Only the workforce member's supervisor or manager can grant access to UIW**'s** ePHI information systems.

Access to the information system or application may be revoked or suspended, consistent with UIW**'s** policies and practices, if there is evidence that an individual is misusing information or resources.

Any individual whose access is revoked or suspended may be subject to disciplinary action or other appropriate corrective measures.

Minimum Necessary Access:

UIW shall ensure that only those workforce members who require access to ePHI are granted access. Each supervisor or manager is responsible for ensuring that the access to ePHI granted to each of his or her subordinates is the minimum necessary amount of access required for each subordinate's job role and responsibilities. If the subordinate no longer requires access, it is the supervisor or manager's responsibility to complete the necessary process to terminate access.

Granting Access to ePHI:

- **Screen Workforce Members Prior to Access:**
  The manager or supervisor shall ensure that information access is granted only after verifying that the access of a workforce member to ePHI is necessary and appropriate.

- **Sign Security Acknowledgement:**

Prior to being issued a User ID or logon account to access any ePHI, each workforce member shall sign UIW**'s** Confidentiality Agreement, and shall thereafter comply with all of **UIW's** security policies and procedures.

- **Security Awareness Prior to Getting Access:**
  Before access is granted to any of the various systems or applications that contain ePHI, workforce members shall be trained to a minimum standard. Topics to be covered in training will include:

  1. Proper uses and disclosures of the ePHI stored in systems or application(s).
  2. How to properly log on and log off the systems or application(s).
  3. Protocols for correcting user errors (i.e., inadvertent alteration or destruction of ePHI).
  4. Instructions on contacting a designated person or help desk when ePHI may have been altered or destroyed in error; and
  5. Reporting a potential or actual security breach.

- **Management Approval:**
  UIW shall implement the following policies:

  1. User IDs or logon accounts may only be assigned with management approval.
  2. Managers are responsible for requesting the appropriate level of computer access for staff to perform their job functions.
  3. All requests regarding User IDs or computer system access for workforce members must be communicated to the appropriate individuals by email. This allows requests to be tracked.
  4. System administrators must process only those requests that have been authorized in writing by managers.
  5. The system administrator must retain requests for a minimum of one (1) year.

Granting Access in an Emergency:

- **Emergency User Access:**
  Management has the authority and discretion to grant emergency access for workforce members who have not completed the steps listed in the "Granting Access to ePHI" section above if:

  1. UIW declares an emergency or is responding to a natural disaster, which makes the management of client information security subordinate to immediate workforce safety concerns and activities.
  2. Management determines that granting immediate access is in the best interest of the client whose ePHI may be exposed. The reason(s) for this determination should be documented.

If management grants emergency access, the granting of access shall be documented and reviewed within 24 hours.

After the emergency event is over, the user access shall be removed. The workforce member shall then complete the normal requirements for being granted access.

- **Granting Emergency Access to an Existing User Access Account:**
  In some circumstances, management may need to grant itself emergency access to a user's account, without the user's knowledge or permission. Management may grant this emergency access in these situations:

  1. The workforce member is terminated or resigns, and management requires access to the person's data.
  2. The workforce member is on approved leave of absence for a prolonged period.
  3. The workforce member has not been in attendance and therefore is assumed to have resigned; or
  4. The workforce member's superior needs immediate access to data on a workforce member's computer to provide client treatment.

Termination of Access:
Department managers or their designated representatives are responsible for terminating a workforce member's access to ePHI in these circumstances:

1. If management has evidence or reason to believe that the user is using information systems or resources in a manner inconsistent with **UIW's** HIPAA Security Rule policies.
2. If the workforce member or management has evidence or reason to believe the user's password has been compromised.
3. If the user resigns, is terminated, is suspended, retires, or is away on unapproved leave.
4. If the user's job description changes and system access is no longer justified by the new job description.

If a workforce member's employment is terminated, the workforce member's access to ePHI shall be terminated in accordance with the terms of the "Policy Responsibilities" section, below.

If the workforce member is on an approved leave of absence for more than three weeks, management shall suspend the user's account until the workforce member returns from his or her leave of absence.

Modifications to Workforce Member's Access:

If a workforce member transfers to another program or changes role(s) within the same program within UIW**:**

1. The workforce member's new supervisor or manager is responsible for promptly evaluating the workforce member's current access.
2. The workforce member's new supervisor or manager is responsible for requesting access to ePHI commensurate with the workforce member's new role and responsibilities.

Ongoing Compliance for Access:
To ensure that workforce members have access to ePHI only when it is required for their job function, the following measures shall be implemented by **UIW:**

1. Every new User ID or log on account that has not been used for thirty (30) consecutive calendar days since creation shall be investigated to determine if the workforce member still requires access to the ePHI.
2. At least every six (6) months, IT teams are required to send to supervisors/managers (or appropriate designees):
    a. A list of all workforce members with access to all applications.
    b. A list of workforce members and their access rights for all shared folders that contain ePHI; and
    c. A list of all Virtual Private Network (VPN) workforce members.
3. The supervisors/managers shall then notify their IT teams of any workforce members that no longer require access or who require modified access.

Policy Responsibilities:
Security Officer or Designee Responsibilities:

1. The Security Officer shall, via email, provide the System Administrator with the names of workforce members who are terminating or transferring out of UIW**,** along with the applicable supervisor's name and the effective date of termination or transfer.
2. The Security Officer shall work with HR or its designee to arrange a process to immediately email and telephone IT and Facilities Management if a workforce member is being released from probation or has been terminated with cause. The HR division shall provide the workforce member's name, supervisor's name, and effective date, so that access can be discontinued when the personnel action is effective.

UIW's IT Team(s) Responsibilities - Account Management:

1. Upon written notification of access modification or termination, a user's access to ePHI shall immediately be modified or removed.
2. A monthly report shall be created that identifies new User IDs or log on accounts not accessed within thirty (30) days of creation. Managers shall be notified to determine whether these accounts should be removed.

3. The IT Team shall provide a report every six (6) months to the manager/supervisor or designee, documenting users with access to ePHI, and requesting verification that access is still required to fulfill the user's job functions.

Managers' and Supervisors' Responsibilities:

1. Each manager/supervisor is responsible for ensuring that the access to ePHI granted to each of their subordinates is the minimum necessary access required for each such subordinate's job role and responsibilities.
2. If the user no longer requires access, it is the manager/supervisor's responsibility to undertake the necessary measures as soon as possible to terminate access.
3. The manager/supervisor shall validate new User IDs or log on accounts that are not accessed within 30 days of creation. If access is no longer required, the User ID shall be deleted.
4. Managers/supervisors shall review and verify semi-annual user and folder access reports and VPN access reports prepared by the IT team, to determine if the workforce members still require access to ePHI.
5. The manager/supervisor shall ensure members of the workforce have signed the IT security agreement and are trained before approving access to ePHI.

User Responsibility:

Each user shall read and agree to comply with UIW**'s** IT Security Policies, sign UIW**'s** HIPAA Confidentiality Agreement, attend HIPAA Security training, and report all security incidents.

Procedures:

UIW shall document written procedures for granting user access, the authorization of access to ePHI, and the termination of user access. These procedures shall include, as a minimum, all of the policy requirements above.

RELEVANT HIPAA REGULATIONS:

- §164.308(a)(3)(i) *Workforce security*
- §164.308(a)(3)(ii)(A) *Authorization and/or supervision*
- §164.308(a)(3)(ii)(B) *Workforce clearance procedure*
- §164.308(a)(3)(ii)(C) *Termination procedures*
- §164.308(a)(4)(i) *Information access management*
- §164.308(a)(4)(ii)(B) *Access authorization*
- §164.308(a)(4)(ii)(C) *Access establishment and modification*
- §164.312(a)(1) *Access control*
- §164.312(c)(1) *Integrity*
- §164.312(a)(2)(ii) *Emergency access procedure*

Continued on Next Page

FULL POLICY LANGUAGE:

Policy Purpose:

Passwords are an important aspect of computer security and are the front line of protection of user accounts and the ePHI contained therein. A compromised password may result in a security breach of **UIW's** network. All **UIW** workforce members are responsible for taking the appropriate steps to select and secure their passwords. The purpose of this policy is to reinforce the use of effective passwords, also known as "strong passwords," and require workforce members to change their passwords on a regular basis.

Policy Description:

Information systems used to access ePHI shall uniquely identify and authenticate workforce members through the use of strong passwords.

Authentication – Verification:

Industry standard protocols will be used on all routers and switches used in the Wide Area Network (WAN) and the Local Area Networks (LANs). Authentication types can include:

1. Unique user ID and passwords.
2. Biometric identification system.
3. Telephone callback.
4. A token system that uses a physical device for user identification.
5. Two forms of authentication for wireless remote access; or
6. Information systems used to access ePHI shall use technology such as digital certificates, to identify and authenticate connections to specific devices involved in system communications.

The password file on the authenticating server shall be adequately protected and encrypted.

Unique User ID and Password Management:

1. All **UIW** workforce members shall be assigned a unique user ID to access the network. All workforce members are responsible for creating and maintaining the confidentiality of the password associated with their unique user ID. Managers/supervisors are required to ensure that their staff understands the user responsibilities for securely managing confidential passwords.
2. Upon receipt of a user ID, the person assigned to this ID is required to change the password provided by the administrator to a password that only he or she (the

user) knows. Effective passwords shall be created in order to secure access to electronic protected health information (ePHI).

3. Workforce members who suspect that their password has become known by another person shall change their password immediately. No user shall give his or her password to another person.
4. Workforce members are required to change all passwords every 120 days. Passwords that must be changed include network user ID passwords, and all application access passwords. Where technology is capable, network and application systems shall be configured to enforce automatic expiration of passwords every six months.
5. All privileged system-level passwords (i.e., root, enable, NT admin, application administration accounts, etc.) shall be changed at least each fiscal quarter. All passwords are to be treated as sensitive, confidential **UIW** information.

User ID & Password Guidelines:

UIW shall implement unique user IDs for each employee. Password guidelines, which incorporate best practices from the latest National Institute of Standards and Technology (NIST) guidelines (set forth in NIST SP 800-63B) are set forth below, and shall be used by **UIW.**

1. Passwords shall be a minimum of eight (8) characters in length and be a maximum length of at least sixty-four characters.
2. **UIW** and its workforce shall have the ability to use all special characters. **UIW** does not require that special characters be used. However, passwords shall be restricted as follows:
    a. Use of sequential and repetitive characters (i.e., 12345 or aaaaa) shall be restricted.
    b. Use of context-specific passwords (i.e., name of UIW site) shall be restricted.
    c. Use of commonly used passwords (i.e., p@ssw0rd, etc.) shall be restricted.
    d. Passwords obtained from previous security breaches shall not be used.

UIW shall implement the following additional password requirements:

1. Password selection software should not allow "obvious" passwords:
    a. Common words, words related to the user, repeated letters, numeric sequences, etc. (i.e., "password123", "johnsmith", or "abcabcabc").
2. Login software should include features to prevent brute force attacks, such as:
    a. Delays between login attempts; and
    b. Lock account after a reasonable number of failed attempts.
3. Password protection requirements for users:
    a. Never reveal a password over the phone to anyone.
    b. Never reveal a password in an email message.
    c. Never reveal a password to your supervisor.
    d. Never talk about a password in front of others.
    e. Never hint at the format of a password (i.e., "my family name").
    f. Never reveal a password on questionnaires or security forms.

g. Never share a password with family members.
h. Never reveal a password to co-workers.
i. Never write down your password; instead, memorize it.
j. Never keep a list of user IDs and passwords in your office; and
k. Never misrepresent yourself by using another person's user ID and password.

Policy Responsibilities:

Managers' and Supervisors' Responsibility:

Managers/supervisors are responsible to reinforce secure password use in their offices with emphasis on 'no password sharing.' If access to another worker's account is required, managers/supervisors shall follow the emergency access section of **UIW's** HIPAA User Access Management policy.

IT Team(s) Responsibilities for Network User ID Creation:

1. System administrators shall provide the password for a new unique user ID to only the user to whom the new ID is assigned.
2. Workforce members may at times request that their password be reset. System administrators shall verify the identity of the user requesting a password reset or verify that the person making the request is authorized to request a password reset for another user. When technically possible, a new or reset password shall be set to expire on its attempted use at log on so that the user is required to change the provided password to one only they know.

All Workforce Members Accessing ePHI:

Any workforce member who suspects that their password has become known by another person shall change their password immediately.

Procedures:

Managers' and Supervisors' Responsibility:

Managers/supervisors are responsible to reinforce secure password use in their offices with emphasis on 'no password sharing.' If access to another worker's account is required, managers/supervisors shall follow the emergency access section of **UIW's** HIPAA User Access Management policy.

IT Team(s) Responsibilities for Network User ID Creation:

1. System administrators shall provide the password for a new unique user ID to only the user whom the new ID is assigned.
2. Users may at times request that their password be reset. System administrators shall verify the identity of the user requesting a password reset or verify that the person making the request is authorized to request a password reset for another user. When technically possible, a new or reset password shall be set to expire on its initial use at log on so that the user is required to change the provided password to one only they know.

All Workforce Members Accessing ePHI:

Any workforce member who suspects that their password has become known by another person shall change their password immediately.

RELEVANT HIPAA REGULATIONS:

- §164.312(c)(2) *Mechanism to authenticate electronic protected health information*
- §164.312(d) *Person or entity authentication*
- §164.308(a)(5)(ii)(D) *Password management*
- §164.312(a)(2)(i) *Unique user identification*

Continued on Next Page

FULL POLICY LANGUAGE:

Policy Purpose:

To describe the physical safeguards **UIW** shall implement to safeguard ePHI from any intentional or unintentional use or disclosure.

Policy Description:

General:

UIW shall safeguard ePHI from any intentional or unintentional use or disclosure. UIW shall implement physical safeguards to protect its facilities where ePHI can be accessed. Such safeguards shall maintain the confidentiality, integrity, and availability of ePHI.

New or Remodeled Facility for UIW:

When designing a new building and remodeling existing sites, facility managers and/or designees shall work with the Security Officer(s) to ensure the facility plan components below are compliant with the HIPAA Regulations.

Facility Security Plan:

UIW shall safeguard its facilities and the equipment therein from unauthorized physical access, tampering, and theft. **UIW's** Security Officer(s) shall annually audit **UIW's** facilities to ensure ePHI safeguards are continuously being maintained.

Facility Security Guidelines for the Workforce:

1. Do not share access cards to enter the facility.
2. Do not allow other persons to enter the facility by "piggybacking" *(entering the facility by walking behind an authorized person, through a door without using a card in the reader).*
3. Do not share hard key access to enter the facility; and
4. Do not share alarm codes or keypad codes to enter the facility.

One or more of the following shall be implemented for all sites that access ePHI:

1. **Visitor Access Control:** In facilities where ePHI is available, all visitors shall be escorted and monitored. Each facility shall implement its own procedures that govern visitor access controls. These procedures may vary depending on the facilities structure, the type of visitors, and where the ePHI is accessible.
2. **Metal/Hard Keys:** Facilities that use metal/hard keys shall change affected or appropriate key locks when keys are lost, or a workforce member leaves without returning the key. In addition, the facility shall have:
    a. Clearances based on programmatic need, special mandated security requirements and workforce member security; and

b. A mechanism to track which workforce members are provided access.

3. **Network Closet(s):** Every network closet shall be locked whenever the room is unoccupied or not in use. **UIW** shall document who has access to the network closets and periodically change the locking mechanisms.
4. **Server Room(s):** Every server room shall be locked whenever the room is unoccupied or not in use. UIW shall document who has access to each server room and periodically change the locking mechanisms.
5. **Alarm Systems:** All buildings that have ePHI shall have some form of alarm system that is activated during non-business hours. Alarm system codes may only be provided to workforce members that require this information to leave and enter a building. These alarm codes shall be changed at least every six (6) months.
6. **Doors**: All external facility doors and doors to areas where ePHI is housed shall remain completely shut. It is each workforce member's responsibility to make sure the door that is being entered or exited is completely shut before leaving the vicinity. Sometimes the doors do not completely close by themselves. If a door's closing or locking mechanism is not working, it is every worker's responsibility to notify the facility manager or designee for that facility.

Contingency Operations - Emergency Access to Facilities:
Each facility shall have emergency access procedures in place that allow facility access to appropriate persons to access data. This includes a primary contact person and back-up person for when facility access is necessary after business hours for persons who do not currently have access to the facility.

Maintenance Records Policy:
Repairs or modifications to the physical building for each facility where ePHI can be accessed shall be logged and tracked. These repairs are tracked centrally by Facility Management (i.e., building manager, landlord, maintenance). The log shall include events that are related to security (for example, repairs or modifications of hardware, walls, doors, and locks).

Policy Responsibilities:
Manager/Supervisor Requirements:

1. Take appropriate corrective action against any person who knowingly violates the facility plan.
2. Authorize clearances that are appropriate to the duties of each workforce member.
3. Notify the security administrator or designee within one (1) business day when a user no longer requires access to the facility; and
4. Verify that each worker surrenders her/his card or key upon ending employment with **UIW.**

Worker Requirements:

1. Display their access/security card to demonstrate their authorization to access restricted areas.
2. Immediately report lost or stolen (key/ID) cards, or metal keys or keypad-cipher lock combinations; and

3. Surrender access card or key upon leaving employment.

Facility Manager/Security Officer or Designee Requirements:

1. Request and track maintenance repairs.
2. Establish and maintain a mechanism for accessing the facility in an emergency.
3. Track who has access to the facility.
4. Change metal locks when a key is lost or unaccounted for.
5. Change combination keypads/cipher locks every three (3) months.
6. Change the alarm code every six (6) months.
7. Disable access cards not used for 90 days or more; and
8. Complete access card audits every six (6) months to verify user access.

Security Officer Responsibilities:

1. Work with Facility Management and **UIW** to ensure facilities comply with the HIPAA Security Rule for facility access controls; and
2. Conduct annual audits of **UIW's** facilities to ensure the facility is secured and the requirements of this policy are being enforced.

Procedures:

UIW shall document written procedures for their facility security plan. Procedures shall be written to address the unique requirements of each facility. An essential part of compliance is to document and implement processes to ensure the safeguards in the facility security plan are being maintained.

UIW shall submit new and revised procedures and plans to the Security Officer(s) for approval and ongoing evaluation. Any procedures developed by **UIW** shall be consistent with **UIW's** HIPAA policies and not deviate from **UIW's** standards.

RELEVANT HIPAA REGULATIONS:

- §164.310(a)(2)(ii) *Facility security plan*
- §164.310(a)(1) *Facility access controls*
- §164.310(a)(2)(iii) *Access control and validation procedures*
- §164.310(a)(2)(iv) *Maintenance records*
- §164.310(a)(2)(i) *Contingency operations*

FULL POLICY LANGUAGE:

Policy Purpose:

This policy outlines processes **UIW** and its workforce must use to shield ePHI from unauthorized, incidental, or accidental workstation viewing.

Policy Description:

Workstation Use:

1. Workforce members shall ensure that observable ePHI is adequately shielded from unauthorized disclosure and unauthorized access on computer screens. **UIW** and its workforce shall make every effort to ensure that ePHI and any other confidential information on computer screens is not visible to unauthorized persons.
2. Workforce members working in facilities that are not part of **UIW** shall maintain awareness of their surroundings to ensure that no one can incidentally view ePHI, and that no ePHI is left unattended.
3. Workforce members who work from home or other non-office sites shall take the necessary steps to protect ePHI from other persons who may have access to their home or other non-office site. These measures include password protection of their personal computers, and security measures for all other forms of portable ePHI such as locking up CD ROM Disks, floppy disks, USB drives, PDAs, and laptops.
4. User session-lock shall be implemented when the computer is left idle. It shall be automatic after a specified time based on location and function. The session shall be locked to disable access to the PC until the user enters their unique password with login information.
5. While accessing ePHI outside UIW**'s** Wide Area Network (for example: extranet, VPN), automatic log off shall occur after a maximum of 15 minutes of inactivity. Automatic log off is a system-enabled enforcement of session termination after a period of inactivity and blocks further access until the workforce member reestablishes the connection using the identification and authentication process.

Policy Responsibilities:

Manager/Supervisor Requirements:

1. Take appropriate corrective action against any person who knowingly violates the security requirements associated with workstation use.
2. Ensure that workers set their computers to automatically lock when the computer is not in use; and
3. Ensure that no confidential information is viewable by unauthorized persons at workstations in offices under their management.

Workforce Member Requirements:

1. Session locks the computer when it is left unattended.
2. Ensure the computer is set to automatically lock when the computer is not in use.
3. Ensure that no confidential information is viewable by unauthorized persons; and
4. When working from home or other non-office work sites, protect ePHI from unauthorized access or viewing.

IT Support:

1. When installing new workstations, set the session lock timer to lock the computer when left unattended; and
2. When installing new systems or applications, set the automatic log-off timer to terminate the session when the computer is left unattended.

Procedures:

Procedures for protecting workstations include:

1. Use of polarized screens or other computer security screen overlay devices that shield confidential information.
2. Placement of computers out of the visual range of persons other than the authorized user.
3. Clearing confidential information from the screen when it is not actively in use.
4. Setting up an automatic session lock option on all computer workstations.
5. Shutting down or locking workstation sessions when left unattended; and
6. When the technology is capable, setting the applications to automatically log off after a specific time of inactivity.

UIW shall develop and implement procedures to ensure confidentiality of ePHI. **UIW** shall submit all new and revised procedures to the Security Officer for approval and ongoing evaluation. Any procedures developed by **UIW** shall be consistent with **UIW's** HIPAA policies and not deviate from **UIW's** standards.

RELEVANT HIPAA REGULATIONS:

- §164.310(a)(2)(iii) *Access control and validation procedures*
- §164.310(b) *Workstation use*
- §164.310(c) *Workstation security*
- §164.312(a)(2)(iii) *Automatic log off*

FULL POLICY LANGUAGE:

Policy Purpose:

The intent of this policy is to ensure that ePHI stored or transported on storage devices and removable media is appropriately controlled and managed.

Policy Description:

Device and Media Controls/Accountability:

1. **UIW** shall protect all hardware and electronic media that contains electronic protected health information (ePHI). This includes personal computers, PDAs, laptops, storage systems, backup tapes, CD ROM disks, and removable disks.
2. Every area of UIW is responsible for developing procedures that govern the receipt and removal of hardware and electronic media that contain(s) ePHI into and out of a facility. Procedures shall include maintaining a record of movements of electronic media with ePHI and any persons responsible for its transportation.

Portable Media Use – Security:

1. In addition to protecting **UIW's** workstations and facilities, workforce members shall protect ePHI when working from all other locations. This includes, but is not limited to, home, other offices, or when working in the field.
2. To limit the amount of portable ePHI, workforce members shall not save any ePHI on floppy disks, CD ROM disks, or other portable items.
3. Methods for protecting portable media with ePHI include:
    a. All workforce members shall receive permission from their supervisor before removing ePHI from their facility. Approvals shall specify the type of permission and the time period for authorization, not to exceed one (1) year.
    b. Workforce members who work in the field shall not leave ePHI unlocked or visible in their vehicles. In addition, these workforce members may not leave any ePHI in client facilities/homes.
    c. If ePHI is lost, workforce members are responsible for promptly contacting their supervisor, the Security Officer, or designated Compliance Officers responsible for HIPAA Compliance within one (1) business day of awareness that ePHI has been lost.

Disposal:

Before electronic media that contains ePHI can be disposed, the following actions shall be taken on all computers containing ePHI:

1. Hard drives shall be either wiped clean or destroyed. Hard drive cleaning, if chosen, shall meet the Department of Defense (DOD) standards, which require, *"The method*

of destruction shall preclude recognition or reconstruction of the classified information or material." Another method for removal of ePHI from hard drives is known as purging. Purging includes degaussing or exposing the media to a strong magnetic field to disrupt the recorded magnetic domains.

a. In addition, the hard drive, once cleaned, shall be tested to ensure the information cannot be retrieved.
b. Backups shall also be destroyed or returned to the owner and their return documented. Destruction must ensure there is no ability to reconstruct the data.
c. Other media, such as memory sticks, USB flash drives or micro drives, CD-ROMs, and floppy disks, shall be physically destroyed (i.e., broken into pieces, pulverized, or shredded by a shredder that can perform this function) before disposing of the item.

Media Reuse:

1. All ePHI shall be removed from hard drives when the equipment is transferred to a worker who does not require access to the ePHI, or when the equipment is transferred to a new worker with different ePHI access needs. Hard drives shall be wiped clean before transfer.
2. Cleaning shall meet the Department of Defense (DOD) standards as outlined above. In addition, the hard drive, once cleaned, shall be tested to ensure the information cannot be retrieved.

Sending a Computer Server Hard Drive to Repair:

As technology permits, before **UIW** sends a device out for repair, an exact copy of ePHI shall be created, and ePHI shall be removed from the server hard drive.

Moving Computer Server Equipment with ePHI:

Before moving server equipment that contains ePHI, a retrievable exact copy shall be created.

Device and Media Acquisition:

UIW, when acquiring information systems, shall ensure those systems meet UIW**'s** security requirements and/or security specifications. Information Systems (applications, servers, copiers, etc.) acquisition requires an assessment of risk.

<u>Policy Responsibilities:</u>

Manager/Supervisor Responsibilities:

Ensure that only workforce members who need to remove ePHI from their facilities are granted permission to do so. Such permission, when given, must be within the parameters of this policy.

IT Responsibilities:

1. Ensure all hard drives are wiped clean before disposal or reuse.
2. Test hard drives to ensure they are clean.

3. Before moving hardware or sending hard drives for repair that contain ePHI, create a retrievable copy of ePHI data and wipe the hardware or hard drive.
4. Maintain an inventory and a record of movements or transfers of hardware and electronic media such as workstations, servers, or backup tapes.

Workforce Responsibilities:

1. Individual workforce members shall track laptops, PDAs, CD ROM Disks, and floppy disks, and all other portable media that contain ePHI.
2. To limit the amount of portable ePHI, workforce members shall not save any ePHI onto floppy disks, CD ROMs, and other portable items when it is not necessary.
3. Workforce members shall remove and destroy all ePHI before disposing of the media.

Procedures:

UIW shall document written procedures to track, dispose, and reuse media devices used for ePHI. UIW shall submit all new and revised procedures to the Security Officer for approval and ongoing evaluation. Any procedures developed by UIW shall be consistent with UIW**'s** HIPAA policies and not deviate from UIW's standard.

RELEVANT HIPAA REGULATIONS:

- § 164.310(d)(1) *Device and media controls*
- § 164.310(d)(2)(i) *Disposal*
- § 164.310(d)(2)(ii) *Media reuse*
- § 164.310(d)(2)(iii) *Accountability*
- § 164.310(d)(2)(iv) *Data backup and storage*

UNIVERSITY OF THE INCARNATE WORD

Security 7.0 Audit Controls

FULL POLICY LANGUAGE:

Policy Purpose:

The purpose of this policy is to outline mechanisms that ensure servers, workstations, and other computer systems are appropriately secured through proper audit controls.

Policy Description:

Log-in Monitoring:

1. UIW has the right to monitor system access and activity of all workforce members.
2. To ensure that access to servers, workstations, and other computer systems containing ePHI is appropriately secured, the following login monitoring measures shall be implemented:
    a. A mechanism to log and document four (4) or more failed log-in attempts in a row shall be implemented on each network system containing ePHI when the technology is capable.
    b. Login activity reports and logs shall be reviewed, at a minimum, on a biweekly basis, to identify any patterns of suspicious activity.
    c. All failed login attempts of a suspicious nature, such as continuous attempts, shall be reported immediately to the Security Officer or the designee for UIW.
    d. To the extent that technology allows, any user ID that has more than five (5) repeated failed login attempts in a row shall be disabled for a minimum of 15 minutes.

Information System Activity Review – Audit Controls:

To ensure that activity for all computer systems accessing ePHI is appropriately monitored and reviewed, these requirements shall be met:

1. Where technology allows, the audit record shall capture sufficient information to establish what events occurred, the sources, and the outcomes of the events.
2. Every application and system administrator or designee shall be reviewed, at a minimum, once each fiscal quarter, audit logs, activity reports, or other mechanisms to document and manage system activity.
3. Indications of improper use shall be reported to management for investigation and follow up.
4. Audit logs of access to networks and applications with ePHI shall be archived.
5. Audit information and audit tools shall be protected from unauthorized access, modification, and deletion.

Policy Responsibilities:

System administrators and Security Officers are responsible for implementing and monitoring audit controls for all systems that contain ePHI.

Procedures:
UIW shall submit all new and revised procedures to the Chief Compliance Officer for approval and ongoing evaluation. The Security Officer shall create audit control checklists and logs to assist with, and standardize, the audit function. Any procedures developed by UIW shall be consistent with its HIPAA policies and not deviate from UIW**'s** standards.

RELEVANT HIPAA REGULATIONS:

- §164.308(a)(5)(ii)(C) *Log-in monitoring*
- §164.308(a)(1)(ii)(D) *Information system activity review*
- §164.312(b) *Audit controls*

Continued on Next Page

FULL POLICY LANGUAGE:

Policy Purpose:

The purpose of this policy is to formalize the response to, and reporting of, security incidents. This includes identification and response to suspected or known security incidents, the mitigation of the harmful effects, and the documentation of security incidents and their outcomes.

Policy Description:

UIW shall employ tools and techniques (including, but not limited to, The Guard and its Process) to monitor events, detect attacks, and provide identification of unauthorized use of the systems that contain ePHI.

Reporting:

1. All security incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of ePHI shall be reported and responded to promptly.
2. Incidents to be reported include, but are not limited to:
    a. Virus, worm, ransomware, or other malicious code attacks.
    b. Network or system intrusions.
    c. Persistent intrusion attempts from a particular entity.
    d. Unauthorized access to ePHI, an ePHI based system, or an ePHI based network.
    e. ePHI data loss due to disaster, failure, error, or theft.
    f. Loss of any electronic media that contains ePHI.
    g. Loss of the integrity of ePHI; and
    h. Unauthorized person(s) found in UIW**'s** facility.
3. UIW**'s** Compliance Officer shall be notified immediately of any suspected or real security incident. If it is unclear as to whether a situation is a security incident, the Compliance Officer shall be contacted to evaluate the situation.

Response and Resolution:

The Chief or Lead Compliance Officer (CCO/LCO), who supervises the Privacy Officer and the Security Officer, is the only person in **UIW's** workforce that can resolve a security incident (In small UIWs, the duties of the Privacy Officer, Security Officer, and CCO/LCO, are commonly performed by the same person).

The CCO/LCO shall track the incident and review reports provided by the Security Officer to determine if an investigation of the incident is necessary. The Compliance Officers shall also determine if a report of the incident should be forwarded to the Department of Health and Human Services (HHS). The CCO/LCO shall decide if UIW**'s** Legal Counsel, Law

Enforcement, Human Resources, or Communication and Media Office should be informed and involved in the resolution of the incident. All HIPAA security-related incidents and their outcomes shall be logged and documented by the CCO/LCO Compliance Officers. UIW and its CCO/LCO will record all the incidents and retain these incident reports for six years.

Policy Responsibilities:
Violations of this policy shall be reported to UIW's Chief Compliance Officer.

UIW:
UIW shall train personnel in their incident response roles and responsibilities and provide refresher training as needed. UIW shall test the incident response capability at least annually using tests and exercises to determine the effectiveness.

Workforce Members:
Workforce members are responsible for promptly reporting any security-related incidents to the Security Officer.

IT Help Desk:
The Security Officer shall document all security incidents and provide reports to the CCO/LCO.

Compliance Officers:
The Chief Compliance Officer(s) that is responsible to determine if the incident requires further investigation**.** UIW**'s** Security Officer and Privacy Officer shall determine if corrective actions should be implemented. The CCO/LCO is responsible for documenting the investigations and any corrective actions. The CCO/LCO is responsible for maintaining all documentation on security breaches for six (6) years.

Procedures:
UIW shall submit all new and revised procedures to the CCO/LCO for approval and ongoing evaluation. Any procedures developed by UIW shall be consistent with UIW**'s** HIPAA policies and not deviate from UIW**'s** standard HIPAA operating procedures.

RELEVANT HIPAA REGULATIONS:

- § 164.308(a)(6)(i) *Security incident procedures*
- § 164.308(a)(6)(ii) *Response and reporting*

FULL POLICY LANGUAGE:

Policy Purpose:

The intent of this policy is to guard against unauthorized access to, or modification of, ePHI that is being transmitted over an electronic communications network. When ePHI is transmitted from one point to another, it shall be protected in an encrypted manner. This policy also requires encryption of data at rest for all devices that connect to or store ePHI.

Policy Description:

Encryption:

Proven, standard algorithms shall be used as the basis for encryption technologies. The use of proprietary encryption algorithms is not allowed for any purpose unless authorized by UIW**'s** HIPAA Security Officer.

Circumstances Where Encryption is Required:

1. All devices that connect to or store ePHI must be encrypted.
2. No ePHI shall be sent outside UIW**'s** domain unless it is encrypted. This includes all email and email attachments sent over a public internet connection.
3. When accessing a secure network, an encryption communication method, such as a VPN, shall be used.

Circumstances Where Encryption if Optional:

1. When using point-to-point communication protocols to transmit ePHI, no encryption is required.
2. Dial-up connections directly into secure networks are considered to be secure connections for ePHI and no encryption is required.

Rules for Modem Use:

1. Modems shall never be left connected to personal computers in auto-answer mode.
2. Dialing directly into or out of a desktop computer that is simultaneously connected to a Local Area Network (LAN), or another internal communication network is prohibited.
3. Dial-up access to WAN-connected personal computers at the office is prohibited.

ePHI Transmissions Using Wireless LANs and Devices within UIW Domain:

1. The transmission of ePHI over a wireless network within UIW**'s** domain is permitted if both of the following conditions are met:
    a. The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized; and

b. The local wireless network is utilizing an encryption mechanism for all transmissions over that wireless network and uses two (2) types of authentication.

2. If transmitting ePHI over a wireless network that does not utilize an authentication and encryption mechanism, the ePHI shall be encrypted before transmission.

Perimeter Security:

1. Any external connection to UIW**'s** Wide Area Network (WAN) shall come through the perimeter security's firewall.
2. If determined to be safe by the Security Officer, outbound services shall be initiated for internal addresses to external addresses.
3. Inbound services shall be negotiated on a case-by-case basis with the Security Officer.
4. All workforce members connecting to the WAN shall sign a Confidentiality Agreement before connectivity is established.

Firewall Controls to Transmit ePHI into and Out of UIW:

1. Networks containing systems and applications with ePHI shall implement perimeter security and access control with a firewall.
2. Firewalls shall be configured to support the following minimum requirements:
    a. Limit network access to only authorized workforce members and entities.
    b. Limit network access to only legitimate or established connections (an established connection is return - traffic in response to an application request submitted from within the secure network); and
    c. Console and other management ports shall be appropriately secured or disabled.
3. The configuration of firewalls used to protect networks containing ePHI based systems and applications shall be submitted to the Security Officer for review and approval.

Policy Responsibilities:

All workforce members that transmit ePHI when using the public internet or a wireless device outside UIW WAN, are responsible for ensuring the information is safeguarded by using encryption.

Procedures:

Each area of UIW shall submit all new and revised procedures to the Chief Compliance Officer/Lead Compliance Officer for approval and ongoing evaluation. Any procedures developed by UIW shall be consistent with UIW**'s** HIPAA policies and not deviate from UIW's privacy and security standards.

RELEVANT HIPAA REGULATIONS:

- §164.312(e)(1) *Transmission security*
- §164.312(e)(2)(i) *Integrity controls*
- §164.312(e)(2)(ii) *Encryption*

Continued on Next Page

UNIVERSITY OF THE INCARNATE WORD

Security 10.0 Protection from Malicious Software

FULL POLICY LANGUAGE:

Policy Purpose:

The intent of this policy is to establish procedures for protections to guard against, detect, and report malicious software. Malicious software includes, but is not limited to viruses, worms, trojans, and ransomware attacks.

Policy Description:

UIW shall ensure all computers it owns, leases, and/or operates, are installed with, and maintains, anti-virus and anti-malware software. All workstations shall be configured to activate and update anti-virus and anti-malware software automatically each time the computer is turned on or the user logs onto the network.

In the event that a virus, worm, or other malicious code has infected or been identified on a server or workstation, that equipment shall be disconnected from the network until it has been appropriately disinfected.

Policy Responsibilities:

Workforce Responsibilities:

1. Workforce members who utilize laptops to log on to the network shall work with their IT support to ensure all updates are received.
2. Workforce members shall not disable automatic virus or automatic malware scanning features.
3. All **non-UIW** computers that directly access the WAN shall have anti-virus software and anti-malware software and remain current with updates.
4. All downloaded files shall be malware-checked and virus-checked prior to use.
5. All storage media (i.e., disks) shall be treated as if they contain viruses or malware. Workforce members are permitted to use removable storage disks provided that all disks are virus-checked and malware-checked prior to use.
6. If a virus or malware is detected, workforce members are instructed to immediately contact their Security Officer.
7. For the purposes of protecting data and preventing the spread of malware, workers shall:
    - Attend HIPAA Security Training; and
    - Maintain back-up copies of data files.

IT Responsibility:

Set up laptop computers so they automatically load malware updates when they are connected to UIW**'s** network.

Procedures:
To ensure that all **UIW** workforce members are made aware of the threats and vulnerabilities due to malicious code and software such as viruses and worms, and are effectively trained to identify and prevent these types of attacks, the following procedures shall be established and implemented:

1. The workforce shall be trained to identify and protect data, when possible, against malicious code and software.
2. Security reminders shall be given to the workforce to inform them of any new virus, worm, or other type of malicious code that may threaten ePHI.

UIW shall submit all new and revised procedures to the Chief Compliance Officer/Lead Compliance Officer for approval and ongoing evaluation. Any procedures developed by UIW shall be consistent with its HIPAA policies and not deviate from UIW**'s** privacy and security standards set forth in those policies.

RELEVANT HIPAA REGULATIONS:

- §164.308(a)(5)(ii)(B) *Protection from malicious software*

Continued on Next Page

UNIVERSITY OF THE INCARNATE WORD

Security 11.0 Contingency Plan, Disaster Recovery

FULL POLICY LANGUAGE:

Policy Purpose:

To outline how emergency response procedures are to be created, implemented, and maintained.

Policy Description:

1. UIW shall establish (and implement as needed) procedures for responding to an emergency or other occurrence (i.e., fire, vandalism, system failure, or natural disaster) that damages systems containing ePHI. These procedures consist of:
    a. Applications and data criticality analysis.
    b. Data Backup.
    c. Disaster Recovery Plan; and
    d. Emergency Mode Operation Plan.
2. Each of these procedures shall be evaluated and updated at least annually as business needs and technology requirements change.

Applications and Data Criticality Analysis:

1. UIW shall assess the relative criticality of its specific applications and data for the purpose of developing its Data Backup Plan, its Disaster Recovery Plan, and its Emergency Mode Operation Plan.
2. UIW shall identify critical business functions, define impact scenarios, and determine resources needed to recover from each impact.
3. The assessment of data and application criticality shall be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

Data Backup Plan:

1. All ePHI shall be stored on network servers in order for it to be automatically backed up by the system.
2. ePHI may not be saved on the local drives of personal computers.
3. ePHI stored on portable media (i.e., thumb drives, external hard drive, CD ROM Disks) shall be saved to the network to ensure backup of ePHI data.
4. UIW shall conduct daily backups of user-level and system-level information and store the backup information in a secure location. A weekly backup shall be stored offsite.
5. UIW shall establish and implement a Data Backup Plan, pursuant to which it will create and maintain retrievable exact copies of all ePHI.
6. The Data Backup Plan shall apply to all files that may contain ePHI.

7. The Data Backup Plan shall require that all media used for backing up ePHI be stored in a physically secure environment, such as a secure, off-site storage facility. Or, if backup media remains on site, the media shall be stored in a physically secure location, different from the location of the computer systems it usually backs up.
8. If a **non-UIW**, off-site storage facility or backup service is used, a written contract shall be entered into, to ensure that the contractor shall safeguard the ePHI in an appropriate manner.
9. Data backup procedures outlined in the Data Backup Plan shall be tested on at least an annual basis, to ensure that exact copies of ePHI can be retrieved and made available.
10. UIW shall submit its new and revised Data Backup Plan to the Chief Compliance Officer for approval.

Disaster Recovery Plan

1. To ensure that UIW can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster affecting systems containing ePHI, UIW shall establish and implement a Disaster Recovery Plan. The Disaster Recovery Plan shall provide procedures for restoration or recovery of any loss of ePHI and shall indicate the systems needed to make that ePHI available in a timely manner. The Disaster Recovery Plan for UIW shall be incorporated into UIW**'s** Disaster Recovery Plan.
2. The Disaster Recovery Plan shall include procedures to restore ePHI from data backups in the case of a disaster causing data loss.
3. The Disaster Recovery Plan shall include procedures to log system outages, failures, and data loss to critical systems. In addition, procedures will be implemented to train the appropriate personnel on the Disaster Recovery Plan.
4. The Disaster Recovery Plan shall be documented and easily available to the necessary personnel at all times. These personnel shall be trained to implement the Disaster Recovery Plan.
5. The disaster recovery procedures outlined in the Disaster Recovery Plan shall be tested on a periodic basis to ensure that ePHI and the systems needed to make ePHI available can be restored or recovered.
    a. UIW shall submit its new and revised Disaster Recovery Plan to the Chief Compliance Officer for approval.

Disaster and Emergency Mode for Small Practices:

Small businesses shall maintain a list of persons/departments to call, along with their phone numbers. The list shall contain at least the following persons/departments, along with their phone numbers:

1. Real Estate/Office Suite Maintenance/Management.
2. Computers.
3. Computer Networking.
4. Restoration of Data to Server or Connection to the Internet.
5. EHR Support; and

6. Any other person or department needed to continue business.

Emergency Mode Operation Plan:

1. UIW shall establish and implement, as needed, procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode. Emergency mode operation involves critical business processes that shall occur to protect the security of ePHI during and immediately after a crisis situation.
2. Emergency mode operation procedures outlined in the Disaster Recovery Plan shall be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.
3. UIW shall submit its new and revised Emergency Mode Operation Plan to the Chief Compliance Officer for approval.

Policy Responsibilities:

The Chief Compliance Officer shall oversee the creation, evaluation, testing, and updating of the various contingency plans described herein.

UIW shall submit its new and/or revised procedures and plans to the Security Officer for approval and ongoing evaluation. Any procedures developed by UIW shall be consistent with its HIPAA policies and not deviate from UIW**'s** standards.

For additional information on the terms used in this policy, please click here.

RELEVANT HIPAA REGULATIONS:

- §164.308(a)(7)(i) *Contingency plan*
- §164.308(a)(7)(ii)(A) *Data backup plan*
- §164.308(a)(7)(ii)(B) *Disaster recovery plan*
- §164.308(a)(7)(ii)(C) *Emergency mode operation plan*
- §164.308(a)(7)(ii)(D) *Testing and revision procedures*
- §164.308(a)(7)(ii)(E) *Applications and data criticality analysis*
- §164.310(a)(2)(i) *Contingency operations*

FULL POLICY LANGUAGE

Policy Purpose:

To provide rules for determination of what contractors of **UIW** are Business Associates, and to provide rules for creation, review, and termination of Business Associate Agreements.

Policy Description:

Business Associates:

1. UIW has multiple contractual and business relationships. However, not all contractors or business partners are "Business Associates," as HIPAA defines that term. This security policy only applies to contractors or business partners that fall within the definition of a "Business Associate." Essentially (and as explained in greater detail under "Definitions," below), a Business Associate is any person or UIW that UIW hires to help UIW to do something. The "something" under the contract involves UIW**'s** either directly or indirectly sharing protected health information (PHI) or electronic protected health information (ePHI) with the Business Associate.
2. The Lead Compliance Officer(s) of UIW shall review all contracts to determine if the contract requires a Business Associate Agreement ("BAA"). If a BAA is required, contract managers must complete the BAA and notify the Compliance Officer(s). The BAA requires the Business Associate to provide satisfactory assurance that the Business Associate shall appropriately safeguard PHI and ePHI and report any security incidents.
3. UIW shall audit the Business Associate via electronic questionnaire. If decided by the Chief Compliance Officer, UIW shall conduct a security audit of the Business Associate's HIPAA Policies and Procedures as a means of due diligence to ensure that the Business Associate is taking the necessary precautions under the HIPAA Security Rule to protect the data that is shared with it.

Business Associate Non-Compliance:

1. If UIW knows of any activity, practice, or pattern of activity or practice of the Business Associate that constitutes a material breach or violation of an obligation under the contract or other arrangement, UIW shall, as a first resort, take reasonable steps to repair the breach or end the violation, as applicable. Such steps include working with, and providing consultation to, the Business Associate.
2. If such steps are unsuccessful, UIW **shall** terminate the contract or arrangement, if feasible. If termination is not feasible, the problem shall be reported to the Office for Civil Rights (OCR) within 30 days of the incident.

Policy Responsibilities:

The Chief Compliance Officer, the Security Officer, and the Privacy Officer of UIW shall work together to ensure that all Business Associates are identified, tracked, and investigated when an allegation is made.

Procedures:

Tracking and Identifying Company Business Associates:

UIW shall identify those business relationships that meet the definition of a Business Associate relationship. Contract managers shall note that designation in the contract record and notify the Chief Compliance Officer when a contractor is determined to be a Business Associate.

Response to Complaints about Business Associates:

A workforce member of UIW may receive a report or complaint, from any source, about the Business Associate's inappropriate or inadequate safeguarding of PHI. If and when a workforce member receives a report or complaint, the workforce member shall promptly provide information regarding that report or complaint to the Chief Compliance Officer(s). The Chief Compliance Officer(s) shall coordinate with the Business Associate's contract administrator to document the alleged violation and determine if remediation is required for the Business Associate to attain/retain contract compliance.

Where contract compliance cannot be attained/retained, **UIW shall terminate the contract, if feasible**. If termination is not feasible, the Chief Compliance Officer shall report the problem to the Office for Civil Rights (OCR) within 30 days of the incident.

RELEVANT HIPAA REGULATIONS:

- § 164.308(b)(1) *Business associate contracts and other arrangements*
- § 164.308(b)(3) *Written contract or other arrangement*

Continued on Next Page

FULL POLICY LANGUAGE:

Policy Purpose:

The intent of this policy is to establish periodic evaluations of UIW's policies and procedures, to ensure these measures detect, contain, and correct security violations. The evaluation shall determine whether the HIPAA policies and procedures are effectively safeguarding the confidentiality, integrity, and availability of ePHI. Security assessments shall be conducted periodically to determine continued compliance with security standards and specifications. Assessments are conducted to:

1. Determine if security controls are correctly implemented, and, as implemented, are effective in their application.
2. Ensure that HIPAA security regulations, policies, and directives are complied with; and
3. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Policy Description:

Risk Assessment & Management:

UIW, along with the Security Officer, shall monitor the effectiveness of its ability to secure ePHI. In order to accomplish this, UIW shall conduct a risk assessment when:

1. New technology is implemented that either contains ePHI or is used to protect ePHI.
2. New facilities that maintain or house ePHI are created or established.
3. Existing facilities that maintain or house ePHI are being remodeled or the design layout is being altered.
4. New programs, functions, or departments that affect the security of UIW are added.
5. Security breaches are identified; and
6. Changes in the mode or manner of service delivery are made.

As part of risk management, security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level shall be documented and implemented.

Risk Management Control:

The primary goal of risk management is to facilitate communications and coordinate all changes that may occur in the IT environment. These changes include, but are not limited to, the installation, update, or removal of network services and components, operating system upgrades, applications, database servers, or software.

Change Notification:

1. For informational purposes, the Chief Compliance Officer and the Security Officer shall be notified, by email, of changes. Notification shall be given within 48 hours of the change.
2. Emergency Changes shall be communicated to the Chief Compliance Officer and the Security Officer as soon as is reasonable.
3. Any change with a negative effect that could adversely affect customers, patients, or clients, shall be communicated to the Chief Compliance Officer and the Security Officer as soon as is reasonable.

Change Implementation:
All non-emergency changes made as part of risk management shall occur within the recognized downtime unless approved in advance by all affected parties. Interdepartmental non-emergency changes shall occur as per the dictates of department procedures.

Change Closure:
When **UIW**, under its risk management policy and procedure, completes a change or closes a change, that change or close shall be documented.

Evaluation:
UIW shall assess security controls at least annually. The assessment shall be conducted to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome.

Technical and non-technical evaluations shall be conducted periodically to identify any new risks or to determine the effectiveness of the HIPAA Security Policies and Procedures. These evaluations include, but are not limited to, the following:

1. Random audit reviews of a facility's physical environment security.
2. Random audit reviews of workstation security.
3. Periodic, unannounced tests of the physical, technical, and administrative controls.
4. Assessment of changes in the environment or business process that may affect the HIPAA Security Policies and Procedures.
5. Assessment when new federal, state, or local laws and regulations, which may affect the HIPAA Security Policies and Procedures; are implemented.
6. Assessment of the effectiveness of the HIPAA Security Policies and Procedures when security violations, breaches or other security incidents occur; and
7. Assessment of redundancy needed in the network or servers for ePHI availability.

Policy Responsibilities:
The Chief Compliance Officer:

1. The Chief Compliance Officer must coordinate with the Security Officer(s) to conduct audits of compliance with the HIPAA Security Rule.
2. Shall coordinate the creation of procedures to implement this policy; and
3. Shall have responsibility for providing tools and processes for assessing technical and nontechnical evaluations as part of UIW**'s** ongoing compliance efforts.

If assessments recommend changes to the HIPAA Policies and Procedures, the Chief Compliance Officer is responsible for reviewing these changes and presenting them to management. If needed, the Chief Compliance Officer will update the workforce training materials.

Procedures:

The Chief Compliance Officer shall create procedures to ensure ongoing evaluations and assessments are completed to mitigate risks to ePHI.

Risk Management: Risk management is an information security process. This process requires an **UIW** to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the general requirements of the HIPAA Security Rule.

RELEVANT HIPAA REGULATIONS:

- §164.308(a)(8) *Perform a periodic technical and non-technical evaluation*
- §164.308(a)(1)(i) *Security management process*
- §164.308(a)(1)(ii)(A) *Risk analysis*
- §164.308(a)(1)(ii)(B) *Risk management*

Continued on Next Page

Security 14.0 Security Awareness and Training

FULL POLICY LANGUAGE:

Policy Purpose:

To provide rules for training of workforce and management on system and application security awareness principles.

Policy Description:

Security Awareness Training:

Security awareness training is key to eliminating UIW**'s** exposure to both malicious threats and accidental errors or omissions.

System & Application Training:

This policy sets forth a minimum standard for system and application security awareness to reduce UIW**'s** risk. The standard contains the following components:

1. Proper uses and disclosures of the ePHI stored in the application.
2. How to properly log on and log off the application.
3. Protocols for correcting user errors.
4. Instructions for contacting a designated person or help desk when ePHI may have been altered or destroyed in error; and
5. Reporting a potential security breach.

HIPAA Security Training:

1. All **UIW** workforce members shall receive security training. The Chief Compliance Officer, or the Security Officer under the Chief Compliance Officer's management, will provide the training and training materials.
    a. Worker-Level Training: This training covers Security Policies and Procedures that directly affect members of the workforce.
    b. Managerial-Supervisory Training: This training encompasses all HIPAA Security Policies and Procedures, as well as Management's role in enforcement and supervision.
2. All new workforce members are required to attend the appropriate training within sixty (60) days of entering the workforce.
3. All workforce members must receive training annually.

Tracking Security Training:

UIW**'s** training coordinator or designee shall enter their workforce members into The Guard, to sign them up for the appropriate level of training.

HIPAA Security Reminders:
The Chief Compliance Officer and Security Officer shall develop and implement periodic security updates and issue at least quarterly reminders to UIW**'s** workforce. These security reminders shall be provided using those media that UIW uses to communicate with its workforce (i.e., email, posters, newsletters, intranet site, etc.).

Policy Responsibilities:

1. Security Officers are responsible for ensuring that all workforce members in their operational areas are trained no later than thirty (30) days after entering their workforce.
2. Chief Compliance Officers shall have oversight responsibility to audit reports from The Guard to ensure required workforce member attendance.
3. If needed, the Chief Compliance Officer or Security Officer may require workforce members to attend more training if security incidents warrant such further training.

Procedures:

1. UIW shall create and maintain written procedures on how new workers are notified of training, when training takes place, and where new workers should report for training.
2. UIW shall submit any new and/or revised procedures and plans to the Security Officer and Chief Compliance Officer for approval and ongoing evaluation. All procedures developed by UIW shall be consistent with its HIPAA policies and will not deviate from UIW**'s** existing privacy and security standards.

RELEVANT HIPAA REGULATIONS:

- § 164.308(a)(5)(i) *Security awareness and training*
- § 164.308(a)(5)(ii)(A) *Security reminders*

Security 15.0 Sanction Policy

FULL POLICY LANGUAGE:

Policy Purpose:

To outline disciplinary measures (sanctions) to be taken against members of the workforce who violate the HIPAA Security Rule and/or **UIW's** Security Rule policies and procedures as set forth in this manual.

Policy Description:

Sanctions:

1. All members of UIW**'s** workforce must be aware of their responsibilities under UIW**'s** HIPAA Security Rule policies and procedures.
2. All members of UIW**'s** workforce must sign a HIPAA Confidentiality form, indicating that they have been informed of UIW**'s** security practices.
3. Managers and supervisors must ensure that workforce members who have access to ePHI are informed of their responsibilities with respect to that ePHI.
4. Management must ensure that training is timely and appropriate; that updates are timely communicated to workforce members; and that only the most current, up-to-date information is used in training, policies, and procedures.
5. Members of UIW**'s** workforce, who violate policies and procedures relating to safeguarding of protected health information or otherwise confidential information, are subject to disciplinary action by UIW**.** Disciplinary action may include measures up to and including immediate dismissal from employment.
6. Corrective action for violations, including, but not limited to, contract cancellation or termination of services, shall be implemented by UIW and shall apply to members of the workforce not subject to UIW**'s** discipline process.
7. Members of the workforce who knowingly and willfully violate state or federal law for failure to safeguard ePHI are subject to criminal investigation and prosecution, and/or civil monetary penalties.
8. If UIW fails to enforce security safeguards, it may be subject to administrative penalties by the Office for Civil Rights (OCR), including federal funding penalties.

Reporting Violations:

All workforce members shall notify the Security Officer and Chief Compliance Officer when there is a reasonable belief that any security policies or procedures are being violated.

Retaliation Prohibited:

1. Neither UIW as an entity nor any member of its workforce shall intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any individual for:
    a. Exercising any right established under UIW**'s** policy.

b. Participating in any process established under UIW**'s** policy including the filing of a complaint with UIW or with the Office for Civil Rights.
c. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to UIW**'s** policy and procedures; and
d. Opposing any unlawful act or practice, provided that the individual or other person (including a member of UIW**'s** workforce) has a good faith belief that the act or practice being opposed is unlawful and the manner of such opposition is reasonable and does not involve a use or disclosure of an individual's protected confidential information in violation of UIW**'s** policy.

2. Those engaging in retaliation shall be subject to sanctions under this policy.

Policy Responsibilities:
All workforce members are responsible for notifying the Security Officer and Chief Compliance Officer when there is a belief that any security policies are being violated.

Workforce: The definition of UIW**'s** workforce is taken from the HIPAA Privacy Rule. Section 160.103 of the Privacy Rule defines the term "workforce" as "Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity, is under the direct control of such entity, whether or not they are paid by the Covered Entity."

RELEVANT HIPAA REGULATIONS:

- § 164.308(a)(1)(ii)(C) *Sanction policy*

FULL POLICY LANGUAGE:

Policy Purpose:

This policy describes what ongoing measures **UIW** shall take to comply with the standards, implementation specifications, and other requirements of the HIPAA Security Rule.

Policy Description:

1. The Compliance Officers (Chief Compliance Officer and/or Security Officer) shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule. The Compliance Officers shall work with workforce members to draft and revise policies and procedures.
2. All policies and procedures implemented to comply with the HIPAA Security Rule shall be documented in writing (which may be in electronic form). All records of actions, activities, or assessments required by the Rule shall be documented. The documentation should be detailed enough to communicate the security measures taken and to facilitate periodic evaluations.
3. Documentation shall be retained for a minimum of six (6) years from the time of its creation or the date when it last was in effect, whichever is later.
4. All documentation shall be available to those persons responsible for implementing the procedures to which the documentation pertains.
5. Documentation shall be reviewed at least annually, and updated as needed, in response to environmental or operational changes affecting the security of the ePHI.

Policy Responsibilities:

Compliance Officers:

The Compliance Officers shall be responsible for leading the development, implementation, and maintenance of the policies, procedures, and related documentation.

Department Management:

UIW shall submit all new and revised procedures to the Compliance Officers for approval and ongoing evaluation.

Procedures:

In general, the following process shall be used to develop and implement policies and procedures:

1. The Compliance Officers shall draft new or updated HIPAA information security policies.

2. The new information security policy shall be presented to UIW**'s** management for awareness, input, and endorsement.
3. The Compliance Officers shall give final approval for the new or updated policy; and
4. The Compliance Officers shall communicate the new or updated policy to the workforce including updating training and related materials as needed.

Any procedures developed by UIW shall be consistent with its HIPAA policies and shall not deviate from **UIW's** existing privacy and security standards.

RELEVANT HIPAA REGULATIONS:

- §164.316(a) Policies *and procedures*
- §164.316(b)(1) *Documentation*
- §164.316(b)(2)(i)*Time limit*
- §164.316(b)(2)(ii) *Availability*
- §164.316(b)(2)(iii) *Updates*

Continued on Next Page

Security 17.0 Satellite Office and Home Office Policy

FULL POLICY LANGUAGE:

Policy Purpose:

The intent of this policy is to specify the circumstances under which devices can be used at Satellite Office and Home Office sites. These sites, by definition, contain no signage to designate that they are part of, or perform services for, the main healthcare entity. These locations are used solely for treatment purposes. When treatment is finished, the provider leaves the facility. Satellite Offices and Home Offices may not be used for storing PHI documented in physical or digital form.

Policy Description:

1. Devices used at Satellite and Home sites must be protected and encrypted and listed in the Device Audit as encrypted.
2. Site(s) must have a Physical Site Audit filled out and stored in The Guard.
3. All **UIW** staff that work in the Satellite and Home offices must go through HIPAA training.
4. No footprint (evidence of PHI) shall be allowed at either Satellite or Home Offices.
5. If the above are not followed, UIW must be able to defend its decisions to the Department of Health and Human Services (HHS), should a breach occur because these protocols were not followed.

Policy Responsibilities:

The Chief Compliance Officer shall oversee the creation, approval, and updating of the Satellite Office and Home Office Policy. New and/or revised procedures and plans shall be submitted to the Security Officer for approval and ongoing evaluation.

Procedures:

UIW shall submit its new and/or revised procedures and plans to the Security Officer for approval and ongoing evaluation. Any procedures developed by UIW shall be consistent with its HIPAA policies and not deviate from UIW**'s** existing privacy and security standards.

If any of the above does not apply to an office, then this site is considered a location and is subject to all the HIPAA requirements that the main office is subject to.

Example of a Satellite Office:

A doctor's office in city A has multiple patients in city B, so, once a week, the doctor uses a site in city B (i.e., an examination room in another doctor's office, etc.) to see patients who live there so they do not have to travel as far. This site is not used for storing charts, for storing computers, or for leaving any documentation behind. It is strictly used for seeing

the doctor's patients, and then the site is vacated. When leaving, the doctor leaves behind no footprint, no computers, no charts, no trash, and nothing about or pertaining to any of the patients that were there that day.

Home Office: A home office is a location with no signage to designate that it is part of, or performs services for, the main **UIW**. This location is not used for storing charts, for storing computers, and does not retain any documentation. It is strictly used for providing treatment and healthcare viewing of electronic records. There is no footprint, no data stored on computers, no charts, no trash, nothing that can be traced back to any of the PHI that was interacted with. If UIW uses a home office, UIW should not allow storage of PHI at the Home Office. Printed matter should be shredded immediately after use, and it should not be stored. Computers should be set up so PHI cannot be downloaded from the main site. **No footprint can be left at the home office.**

If any of the above does not apply, then this site is not considered to be a Home Office. Instead, it is considered to be a location and is subject to all the HIPAA requirements that the main office is subject to.

Continued on Next Page

UNIVERSITY OF THE INCARNATE WORD

Security 18.0 Work from Home Policy

FULL POLICY LANGUAGE:

Policy Purpose:
This policy outlines the security procedures to be followed by employees who telecommute.

Policy Description:
Telecommuting is a voluntary work arrangement that allows employees to perform their jobs at home as part of the regular workweek. Employees who telecommute must observe proper security procedures. Please refer to UIW Telework and Alternative Work Schedule policy.

Procedures:
Employees who telecommute must take proper security measures to ensure that ePHI remains appropriately safeguarded. With respect to the devices employees who telecommute use to perform their work, employees must do the following:

1. Employees must have a device that the employee will dedicate for business purposes only.
2. Employees must ensure device drives are encrypted. This can be accomplished by using an encryption application such as Microsoft BitLocker (requires Windows 10 Pro) or Apple File Vault.
3. Employees must install antivirus and antimalware protections before employees can use a device for business purposes.
4. Employees must enable the "Automatic Updates" function of any device, software program, or operating system used to perform work.
5. Employees must have a strong password-protected account on their device. Password guidelines, which incorporate best practices from the latest National Institute of Standards and Technology (NIST) guidelines (set forth in NIST SP 800-63B) are set forth below, and shall be used by employees:
    a. Passwords shall be a minimum of eight (8) characters in length. A maximum length of sixty-four characters is permitted.
    b. Passwords may consist of all special characters; however, use of all special characters is not a requirement.
    c. Password use shall be restricted as follows:
        i. Use of sequential and repetitive characters (i.e., 12345 or aaaaa) is restricted.
        ii. Context-specific passwords (i.e., the name of UIW's website) are restricted.

iii. Commonly used passwords (i.e., p@ssw0rd, etc.) shall be restricted.
iv. Passwords obtained from previous security breaches shall not be used.

6. Employees must have a password-protected screen lock timeout set to a maximum of 15 minutes.
7. Employees must ensure that all wireless router traffic is encrypted, using (at a minimum) WPA2-AES encryption.
8. Employees must make sure that the password to a wireless network is a strong password, in accordance with (5) above.
9. Employees may not download or print PHI at home offices or any other location from which employees telecommute.
10. Employees must conduct a physical site audit and provide the details of that audit to the current Security Officer, no less than once every twelve months. The audit consists of the following questions:
    a. Does the employee store paper documents that contain PHI in the employee's home office?
    b. Does the employee print paper documents that contain protected health information at the employee's home office?
    c. Does the employee receive paper faxes at a physical fax machine in the employee's home office?
    d. Does the employee take paper or electronic files containing PHI or ePHI to the employee's home office?
    e. Does the employee's home office have a lockable door?
    f. Does the employee's home or home office have an alarm system?
11. **UIW's** Security Officer and/or IT department must confirm employees have all security measures required by this policy in place before access to UIW's resources is granted.

FULL POLICY LANGUAGE:

Policy Purpose:

To outline the security precautions that must be taken by employees who conduct work using their personally owned devices.

Policy Description:

UIW may allow employees to conduct work using their personally owned devices (such as smartphones, laptops, and PDAs). When employees use their personally owned devices to access UIW's resources and services, employees must take proper security precautions, so the security of both the devices and **UIW's** data and technology infrastructure is maintained.

Procedures:

Expectation of Privacy:

UIW shall respect the privacy of employees' personal devices, and will only request access to these devices:

1. When required for IT personnel to implement security controls and measures; and
2. To respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings.

Acceptable Use:

1. Personal devices may be used for an "acceptable business use." "Acceptable business use" means use for activities that directly or indirectly support UIW's business functions.
2. Personal devices may be used for an "acceptable personal use" while on company time. "Acceptable personal use" means reasonable and limited personal communication or recreational activities, such as reading.
3. UIW has a zero-tolerance policy for texting or emailing while driving, only hands-free talking while driving is permitted.
4. Personally owned devices may never be used to:
    a. Store or transmit illicit materials.
    b. Store or transmit proprietary information.
    c. Harass others.
    d. Engage in outside business activities.
5. Employees may use their personally owned devices to access, as necessary, the following company-owned resources: Email, Calendars, Contacts, and Documents.

Devices and Support:

- The following devices are supported:
    - iPhone, iPad, Android, Blackberry, Windows, Mac
- Connectivity issues are supported by IT; employees should contact the device manufacturer or their carrier for an operating system or hardware-related issue.
- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software, and security tools, before they can access the network.

Security:

- Devices must be password-protected using a strong password.
- All devices must be encrypted according to NIST guidelines.
- The device must lock itself with a password or PIN if the device is idle for five minutes.
- Rooted (Android) or jailbroken (iOS) devices are forbidden from accessing the network.
- Laptops, Smartphones, and tablets that are not on the company's list of supported devices are not allowed to connect to the network.
- Laptops, Smartphones, and tablets belonging to employees that are for personal use only are not allowed to connect to the network.
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.
- The employee's device may be remotely wiped if:
    - The device is lost or stolen.
    - The employee terminates his or her employment.
    - IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

Employee Responsibilities:

- While **UIW** will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- UIW reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to UIW within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- UIW reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

UNIVERSITY OF THE INCARNATE WORD

Security 20.0 Clean Desk Policy

FULL POLICY LANGUAGE:

Policy Purpose:

To outline the measures employees must take to maintain a clean desk, so that PHI or ePHI are not left exposed to unauthorized viewing, use, or disclosure.

Policy Description:

UIW must have in place physical safeguards to protect the security of PHI and ePHI. These safeguards include security measures to enhance workstation security. To protect workstation security, **UIW** has adopted a clean desk policy. Under the clean desk policy, employees may not keep sensitive or confidential materials in open spaces that can be accessed by unauthorized individuals. When such items are not in use, and whenever an employee leaves his or her workstation, the employee must remove the items from open workspace areas and securely lock them away.

Procedures:

Clean Desk Policy Requirements:

UIW's workforce must observe the following clean desk policy requirements:

- Employees are required to ensure that all information containing PHI, or that is otherwise sensitive or confidential, be secured:
  - At the end of the day.
  - Before employees leave the workstation for a period of greater than 10 minutes.
- An employee must lock computer workstations when his or her workspace is unoccupied.
- Employees must completely shut down computer workstations at the end of the workday.
- Any material containing PHI or ePHI, or material that is otherwise confidential or sensitive, must be removed from an employee's desk and locked in a drawer, when the desk is unoccupied and at the end of the workday.
- File cabinets containing PHI, or material that is otherwise confidential or sensitive, must be kept closed and locked when not in use or when not attended.
- Keys used for access to PHI, or otherwise confidential or sensitive information, may not be left at an unattended desk.
- Passwords may not be left on sticky notes posted on or under a computer, nor may passwords be left in writing in an accessible location.
- Printouts or faxes containing PHI, or otherwise confidential or sensitive information should be immediately removed from the printer or fax.

- Upon disposal, PHI or otherwise confidential or sensitive information must be shredded in official shredder bins or placed in locked, confidential disposal bins.
- Portable *computing devices* such as laptops/tablets must be kept in a locked drawer, cabinet, or closet.
- Portable *storage devices* such as USB drives must be kept in a locked drawer, cabinet, or closet.

Policy Compliance:
Supervisors and managers must notify employees when they are not following the policy. If non-compliance continues, supervisors must notify the Security Officer.

UIW's Security Officer will ensure compliance with the clean desk policy through various methods, including, but not limited to periodic walk-throughs, and soliciting feedback from supervisors and managers.

An employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, in accordance with **UIW's** sanctions policy.

RELEVANT HIPAA REGULATIONS:

- §164.310(c) *Workstation Security*

Continued on Next Page

UNIVERSITY OF THE INCARNATE WORD

Privacy 1.0 HIPAA Privacy Program

FULL POLICY LANGUAGE:

Policy Purpose:

At all times, **UIW** shall have one individual identified and assigned to HIPAA Privacy responsibility. This individual is known as the HIPAA Privacy Officer.

Policy Description:

The Privacy Officer is responsible for **UIW's** overall compliance with the HIPAA Privacy Rule, and for ensuring that **UIW's** HIPAA Privacy Rule policies and procedures are developed, implemented, and followed. The Privacy Officer is the point person for **UIW's** Privacy Program, through which the Privacy Officer's and other **UIW** duties are carried out.

UIW must follow the below procedures under the Privacy Program.

Procedures:

Designation of Individuals:

- Designation of the Privacy Officer, who is responsible for development and implementation of UIW's policies and procedures.
- Designation of a contact person (who may be either the Privacy Officer or another designated individual) who is responsible for receiving privacy-related complaints, and who can provide further information about **UIW's** Notice of Privacy Practices.

Training:

- **UIW** must train all workforce members on its Privacy Policies and Procedures, as necessary and appropriate for workforce members to carry out their functions within UIW. Training shall be provided as follows:
    - To each new member of the workforce within a reasonable period of time after the person joins the workforce.
    - To each member of **UIW's** workforce whose functions are affected by a significant change in **UIW's** privacy policies and procedures, within a reasonable period of time after that change becomes effective.
    - **UIW** must document that the training has been provided.
- Questions concerning training or any aspect of training may be directed to the Privacy Officer.

Administrative Safeguards:

UIW must safeguard protected health information (PHI) from any intentional or unintentional use or disclosure that violates the HIPAA Privacy Rule. **UIW** must also reasonably safeguard protected health information to limit incidental PHI uses or disclosures that are made pursuant to an otherwise permitted or required use or

disclosure. The Privacy Officer has responsibility for these tasks.

Complaints:
UIW must provide a process for individuals to make complaints concerning its privacy policies and procedures, and its compliance with those procedures. **UIW** must keep records of complaints and their resolution.

Sanctions:
UIW must develop and apply appropriate sanctions against workforce members who fail to comply with its privacy policies and procedures and/or the HIPAA Privacy Rule. **UIW** must document all sanctions it applies. The Privacy Officer shall be responsible for the determination of appropriate sanctions. The Privacy Officer, in his or her discretion, may review the sanction decision at the request of an employee.

Mitigation:
UIW must mitigate, 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 **UIW** or its business associates.

No Retaliation:
UIW may not threaten, coerce, discriminate against, or take other retaliatory action against anyone who files a complaint, or who exercises a right to which they are entitled under the Privacy Rule.

Waiver of Rights:
UIW may not require any individual to waive his or her right to file a complaint with UIW or HHS, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Policies and Procedures:
The policies and procedures to be developed by the Privacy Officer must comply with all Privacy Rule standards, implementation specifications, and requirements. These policies and procedures must be designed, considering **UIW's** size and the type of activities that relate to PHI undertaken by **UIW**.

Changes to Policies and Procedures:
UIW must change its policies and procedures as necessary and appropriate to comply with changes in the law. Whenever a change in law necessitates a change to **UIW's** policies or procedures, **UIW** must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the Notice of Privacy Practices, **UIW** must change the contents of the notice accordingly. **UIW** may not implement a change to a policy or procedure prior to the effective date of the revised notice.

Notice of Privacy Practices:
UIW must implement, distribute, and maintain a Notice of Privacy Practices. **UIW** must maintain a copy of this notice (including revisions to the Notice) for six years from the date

it was last in effect. **UIW** must also update the notice to reflect changes in the law or in UIW's policies and procedures. **UIW** must distribute the notice, and direct questions regarding the Notice to the Privacy Officer.

Business Associates:
UIW will implement, monitor, and maintain business associate agreements (BAAs) with affiliate business associates (BAs) when required by law.

Documentation:
UIW must maintain its policies and procedures in written or electronic form, and must maintain all required documentation (which includes the policies and procedures, and any communications or actions the HIPAA Privacy Rule requires to be in writing) for six years from the date of its creation or the date when it was last in effect, whenever is later. Required documentation includes, but is not limited to, documentation related to compliance enforcement; complaint investigation; training; policies, and procedures and modifications to them; and designated record sets.

RELEVANT HIPAA REGULATIONS:

- §164.530 *HIPAA Privacy Program*

Continued on Next Page

FULL POLICY LANGUAGE:

Policy Purpose:

The purpose of this policy is to ensure patients can receive an accounting of disclosures of their protected health information.

Policy Description:

Under HIPAA, **UIW** must give patients an accounting of disclosures of PHI it made, upon patient request.

Required Disclosures:

Types of disclosures that **UIW** must include in responding to a request for an accounting include:

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

Required Tracking:

Information that must be maintained (tracked) and included in an accounting shall consist of:

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.
4. A brief statement of the purpose of the disclosure (or a copy of the individual's written authorization) or a copy of the individual's written request for disclosure.
5. Multiple disclosures to the same party for a single purpose (or pursuant to a single authorization) 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.

Disclosures Not to Be Included in an Accounting:
An accounting of disclosures shall not include the following disclosures:

1. Disclosures made to law enforcement or correctional institutions as provided by state law.
2. Disclosures for facility directories.
3. Disclosures to the individual patient.
4. Disclosures for national security or intelligence purposes.
5. Disclosures involved in the patient's care.
6. Disclosures made for notification purposes, including identifying and locating a family member; and
7. Disclosures made for treatment, payment, and healthcare operations.

Patients may request an accounting of disclosures that were made up to six years prior to the date of request.

Procedures:
Processing the Request:
1. All requests for an accounting of disclosures must be submitted, in writing, to UIW.
2. UIW must retain this request, retain a copy of the written account to be provided to the patient, and maintain a record of the name/departments responsible for the completion of the accounting.
3. A patient 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. UIW 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.

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

1. Querying all systems and patient records that contain patient disclosures.
2. Obtaining a Patient Disclosure Report from all departments that maintain such reports.
3. Contacting business associates, as necessary, to request the information provided.

Preparing the Accounting of Disclosures:
Accountings of disclosures shall be prepared by **UIW** as follows:

1. Each item on the accounting of disclosures to be sent to the patient must include:
    - The date the disclosure was made.

- 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).
- A brief description of the PHI that was disclosed; and
- A brief description of the purpose of the disclosure.

2. Each disclosure made to an external researcher for a particular research purpose involving fifty or more individuals to an Institutional Review Board waiver of authorization must include:
    - The name of the protocol or other research activity.
    - A brief description in plain language of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records.
    - A brief description of the types of PHI that were disclosed;
    - The date or period of time during which disclosures occurred.
    - The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
    - A statement that the PHI of the patient may or may not have been disclosed for a particular protocol or research activity.

Sending the Accounting:

1. In accordance with the HIPAA regulations, **UIW** must provide the individual with an accounting no later than **60** days after receipt of the request.
2. If the accounting cannot be completed within 30 days after receipt of the request, **UIW** must 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. UIW must provide 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.
4. **UIW** must provide the accounting to the individual at no charge for a request made once during any twelve-month period.
    - 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:

- **UIW** must maintain written requests for an accounting provided to an individual for at least six years from the date it was created.
- **UIW** 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 UIW's state).

RELEVANT HIPAA REGULATIONS:

- 45 C.F.R. § 164.528(a) *Accounting for Disclosures*

FULL POLICY LANGUAGE:

Policy Purpose:

The purpose of this policy is to provide rules for **UIW's** determining whether a vendor is a business associate as defined by the HIPAA regulations. The purpose is also to provide rules for creation, maintenance, and termination of business associate agreements.

Policy Description:

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, use, or disclosure of protected health information. Business associates do not include members of UIW**'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 receives, uses, or discloses in carrying out specified functions or activities for a covered entity. **UIW** may only disclose protected health information (PHI) to a business associate after a valid business associate agreement is in place.

Procedures:

Business Associate Determination:

UIW 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 UIW's workforce.
- The vendor/business is performing a function on behalf of UIW.
- That "something" involves the access to, use, and/or disclosure of PHI.

To make the business associate determination, **UIW** will inventory all outside business and service vendors to determine if they are business associates.

Business associate agreements shall be implemented for all qualified entities. These agreements shall require that business associates comply with the minimum necessary standard set forth in 45 C.F.R. 164.502(b). Under this standard, business associates must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the PHI use, disclosure, or request.

Business Associate Contracts/Agreements:

If an entity is determined to be a business associate, that business associate must provide in writing to **UIW** 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 shall be in the form of a written business associate contract (BAC) that contains the provisions specified in the Privacy Rule. These provisions must:

1. Establish the permitted and required uses and disclosures of protected health information by the business associate.
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 with regard to electronic protected health information.
4. Require the business associate to report to **UIW** any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information.
5. Require the business associate to disclose protected health information as specified in its contract to satisfy **UIW's** obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings.
6. To the extent the business associate is to carry out **UIW's** obligation(s) covered under the Privacy Rule, the agreement must require the business associate to comply with the requirements applicable to the obligation.
7. 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 **UIW** for purposes of HHS determining **UIW's** compliance with the HIPAA Privacy Rule.
8. 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 **UIW**.
9. Require the business associate to ensure that any subcontractors it may engage on its behalf, which will have access to protected health information, agree to the same restrictions and conditions that apply to the business associate with respect to such information; and
10. Authorize termination of the contract by UIW if the business associate violates a material term of the contract.

In the Event of Material Breach or Violation:
If **UIW** knows of a material breach or violation by the business associate of the contract or agreement, UIW is required to take reasonable steps to cure the breach or end the violation.

If such steps are unsuccessful, UIW must terminate the contract or agreement. If termination of the contract or agreement is not feasible, UIW must report the problem to the Secretary of the Department of Health and Human Services (HHS).

Workforce members shall immediately notify UIW**'s** Privacy Officer if and when they learn that a business associate may have breached or violated its business associate agreement.

RELEVANT HIPAA REGULATIONS:

- § 164.502(e)(1) *Disclosures to Business Associates*
- § 164.504 *Uses and Disclosures: UIW Requirements*

Continued on Next Page

Privacy 4.0 Judicial and Administrative Proceedings

FULL POLICY LANGUAGE:

Policy Purpose:

To establish rules for how **UIW** shall respond to requests for disclosure of PHI in the course of judicial or administrative proceedings.

Policy Description:

UIW 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. **UIW** must cooperate with courts and with counsel to provide lawfully sought PHI, while simultaneously ensuring protection of patient privacy.

Procedures:

Disclosing PHI in Response to a Court/Administrative Order:

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

The Privacy Officer, working with legal counsel, shall review any such order to determine whether **UIW** will object to the order on account of over breadth, irrelevance, or any other lawful basis for objecting to disclosure. If the Privacy Officer and legal counsel conclude that an objection to the order is required, such objection shall be filed in accordance with applicable state 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. UIW may release PHI in response to a subpoena, discovery request, or other lawful process, which is not accompanied by a court order, as follows:
   UIW may release PHI if it receives ***written*** "satisfactory assurance" from the party requesting the information that the requesting party has made reasonable efforts to ensure that the patient who is the subject of the PHI has been given notice of the request.
   a. "Satisfactory assurance" that the requesting party has tried to notify the patient of the PHI includes the following:
      i. The requesting party has given UIW a *written statement and supporting documentation* demonstrating that:
         1. The requesting party has made a good faith attempt to provide written notice to the patient (if the patient's location is unknown, documentation showing that a notice was mailed to

the patient's last known address shall be provided by the requesting party).
    2. The notice provided by the requesting party to the patient contained enough information to allow the patient to make an informed objection to the court or administrative tribunal regarding the release of the patient's PHI; and
    3. The time for the patient to raise objections to the court or administrative tribunal has passed, and, either no objections were filed, **or** all objections filed by the patient have been resolved and the disclosures being sought are consistent with the court's resolution.
2. UIW may release PHI to a requesting party if it receives ***written*** satisfactory assurance from the requesting party that such party has made reasonable efforts 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, which 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 **UIW** at the end of the proceeding.
    a. "Satisfactory assurance" in this instance means that UIW has received from the requesting party a written statement, along with supporting documentation, demonstrating that:
        i. 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
        ii. The requesting party has asked for a qualified protective order from such a court or administrative tribunal.
3. UIW may release PHI to a requesting party even without satisfactory assurance from that party if UIW either:
    a. Makes reasonable efforts to provide notice to the patient about releasing his or her PHI, so long as the notice meets all of the following requirements:
        i. The notice is written and given to the patient (if the patient's location is unknown, **UIW** should establish documentation showing that a notice was mailed to the patient's last known address).
        ii. The notice contained enough information to allow the patient to make an informed objection to the court or administrative tribunal regarding the release of the patient's PHI; and
        iii. The time for the patient to raise objections to the court or administrative tribunal has lapsed and either no objections were filed, or all objections filed by the patient 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 convince the parties to stipulate such order.

RELEVANT HIPAA REGULATIONS:

- §164.512(e) *Use and Disclosure of PHI for Judicial and Administrative Proceedings*

UNIVERSITY OF THE INCARNATE WORD

Privacy 5.0 Uses and Disclosures for Marketing

FULL POLICY LANGUAGE:

Policy Purpose:

To establish rules for how **UIW** shall utilize PHI for marketing purposes.

Policy Description:

UIW engages in marketing activities. These activities are defined as communications about products and services that encourage recipients of the communication to buy or use those products and services. Marketing that seeks to utilize protected health information requires prior written patient authorization.

Procedures:

Determine Whether the Communication is Marketing:

1. Per §164.501, marketing is defined as:
   a. Making a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service; or
   b. An arrangement involving **UIW** and another entity or affiliate, whereby PHI is disclosed by **UIW**, in exchange for direct or indirect remuneration, so that the other entity or affiliate can make a communication that encourages the purchase or use of its own product or service.
2. The following are examples of situations that **do not** meet the definition of marketing:
   a. Communications that are merely promoting good health, which are not related to a specific product or service, are not considered "marketing." Examples include information about how to lower cholesterol; mailings about general new developments in healthcare; new diagnostic tools; and mailings about upcoming health or "wellness" classes, support groups, and health fairs.
   b. Communications about government-sponsored programs. Under the Privacy Rule, there is no "commercial" component to communications about benefits available through public programs. Therefore, **UIW** is permitted to use/disclose PHI to communicate about, for example, eligibility for Medicare supplement benefits; such communication does not require prior written patient authorization.
   c. UIW may make communications in newsletter format without authorization so long as the content of such does not fit the definition of "marketing," above.
   d. Oral or written communications that describe UIW**'s** network or covered services:
      i. UIW can convey information to beneficiaries and members about health insurance products offered by UIW that could enhance or

substitute for existing health plan coverage. For example, if a child is about to "age-out" of coverage under a family's policy, the plan may send the family information about continuation coverage for the child; this information is not considered "marketing." However, if the communication contains information about excepted benefits, such as accident-only policies or other lines of insurance, the communication is considered to be marketing.

e. Communications about treatment for the patient; Doctors can write a prescription or refer an individual to a specialist for follow-up tests because these are communications about treatment.
f. Communications about case management or care coordination, or recommendations of treatment alternatives and care options, including health care providers or settings of care.

Authorization to Use or Disclose PHI for Marketing Purposes:

1. UIW shall obtain written patient 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 patient; or
   b. A promotional gift of nominal value provided by UIW.
2. If the marketing involves UIW**'s** receiving direct or indirect remuneration by a third party, written patient authorization is required. Such authorization shall state that such remuneration is involved.

RELEVANT HIPAA REGULATIONS:

- 164.508 (a)(3) *Uses and Disclosures for Which an Authorization is Required: Marketing*

Continued on Next Page

FULL POLICY LANGUAGE:

Policy Purpose:

To establish rules for ensuring PHI is only used and disclosed as needed.

Policy Description:

The HIPAA Privacy Rule requires covered entities, including **UIW**, to adhere to a "minimum necessary" standard with respect to the use and disclosure of PHI. When using or disclosing PHI, **UIW** shall make reasonable efforts to limit PHI uses, disclosures, and requests disclosed to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Procedures:

Applicability of Standard:

The minimum necessary standard applies:

To uses and disclosures of PHI that are permitted under the HIPAA Privacy Rule. The standard also applies:

- To the accessing of PHI or electronic protected health information (ePHI), **by**
- Covered entities, **to**
- Business associates and other covered entities.

In addition, the HIPAA minimum necessary standard applies to *requests* for PHI from other covered entities.

The minimum necessary requirement **does not apply** to:

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 patient information (with the possible exception of psychotherapy notes).
3. Uses or disclosures made pursuant to a valid and HIPAA compliant authorization.
4. Disclosures requested by the individual or the individual's legal representative.
5. 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
6. Uses and disclosures that are required by 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. **UIW** will identify the classes of persons or job titles within **UIW's** workforce who need access to PHI to carry out their job duties and responsibilities described in **UIW's** job descriptions.
2. **UIW** will authorize access to computerized health information. Use of this information will be limited based on reasonable determination regarding an individual's position and/or department.
3. An individual's access will be controlled via ID and password. The sharing of logon IDs and passwords is prohibited.

Routine or Recurring Requests and Disclosures for Patient Information:

1. Requests for patient information made on a routine or recurring basis shall be limited to the minimum amount of patient information necessary to meet the needs of the request/disclosure.
2. Minimum necessary definitions and standard protocols shall be established for routine and recurring requests/disclosures (i.e., patient information that is routinely disclosed to a medical transcription service).
3. Individual review of the request will not be required for requests/disclosures made on a routine or recurring basis where standard protocols have been developed; however, periodic review shall be made for routine or recurring requests to ensure the requests are still valid and necessary.

Non-Routine Requests for Disclosure of Patient Information:

1. Non-routine requests for patient information will be reviewed on an individual basis to limit the patient information requested/disclosed to the minimum amount necessary to accomplish the purpose of the request/disclosure.
2. Such requests will be reviewed on an individual basis unless the request/disclosure is to a health care provider for treatment purposes.
3. Disclosures/requests authorized by the patient or the patient's legal representative will not be subject to the minimum necessary standard but are subject to the terms of the authorization.
4. **UIW** 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 necessary to accomplish the purpose of the use/disclosure.

Reasonable Reliance:

1. **UIW** may rely on the judgment of the party requesting the disclosure as to the minimum amount of patient information necessary for the stated purpose, when:
    a. Making permitted disclosures to public officials, if the public official presents that the patient information is the minimum necessary for the stated purpose(s).
    b. The patient information is requested by another covered entity (i.e., health care provider, health plan or health care clearinghouse).
    c. The patient information requested is the minimum necessary for the stated purpose and requested by a professional who is requesting patient

information for the purpose of providing professional services to **UIW** (i.e., member of **UIW's** workforce or business associate of workforce); or

d. The documentation or representations comply with the applicable provisions for using/disclosing patient information for research purposes and have been provided by a person requesting the patient information for such purposes (i.e., appropriate documentation from the Institutional Review Board).

2. **UIW** workforce members should exercise judgment/discretion when making determinations about disclosures and limit the disclosure to the amount of patient information necessary to satisfy the purpose of the request.

Restrictions:

1. Use/disclosure of patient information will be subject to any agreed upon patient restriction(s) entered into by **UIW** with the patient or the patient's legal representative.
2. Requests for restrictions that have been agreed to by **UIW** should be placed in a designated area of the medical record. This area should be checked for restrictions prior to using/disclosing patient information.
3. Patient information may not be used/disclosed without proper consent or authorization.

Requesting Patient Information:

When requesting patient information from covered entities, **UIW** will limit any request for patient information to that which is necessary to accomplish the purpose for which the request is made.

Corrective Action:

Upon determination of inappropriate or unauthorized access to PHI by a staff member, UIW must determine the appropriate corrective action for the misconduct. Please refer to Privacy Policy 1 regarding failure to comply with privacy practices.

RELEVANT HIPAA REGULATIONS:

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

UNIVERSITY OF THE INCARNATE WORD

Privacy 7.0 Uses and Disclosures for Which an Authorization is Required

FULL POLICY LANGUAGE:

Policy Purpose:

To inform **UIW's** workforce of those situations when written patient authorization is required before **UIW** may use or disclose PHI.

Policy Description:

Under this policy, **UIW** may not use or disclose PHI without a valid written authorization from the patient. When a patient provides a valid authorization, the use and disclosure must be consistent with the authorization.

Procedures:

Psychotherapy Notes:

Written authorization for the following uses or disclosures of psychotherapy notes, is not necessary when use or disclosure is necessary to:

a. To carry out the following treatment, payment, or health care operations:
    i. Use by the originator of the psychotherapy notes for treatment.
    ii. Use by UIW for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or
    iii. Use by UIW to defend itself in a legal action or other proceeding brought by the patient.
b. To respond to the federal Department of Health and Human Services (HHS) to determine UIW**'s** compliance with HIPAA privacy rules.
c. To comply with the law.
d. To assist in health oversight activities regarding the originator of the psychotherapy notes; and
e. To help coroners/medical examiners in the examination of deceased persons; and
f. To prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

In addition, psychotherapy notes may also be revealed, when necessary, to persons who are able to prevent or lessen a threat to the health or safety of a person, including the target of a threat in (f) above.

Marketing:

UIW must obtain an authorization for use or disclosure of PHI for marketing, except if the communication is in the form of a face-to-face communication made by **UIW** to an

individual, or a promotional gift of nominal value provided by UIW. If the marketing involves financial remuneration to UIW from a third party, the authorization must state that such remuneration is involved.

Sale of Protected Health Information:
UIW must obtain an authorization for the disclosure of PHI which is a sale of PHI. A sale of PHI occurs when one party remunerates another, directly or indirectly, in exchange for the second party's giving PHI to the first party. When an authorization is given for the sale of PHI, the authorization must state that the disclosure will result in remuneration being given.

Special Authorization Requirements for Marketing and Sale of PHI:

General Requirements:

1. An authorization is not valid, if the document submitted has any of the following defects:
    a. The expiration date has passed, or the expiration event is known by UIW to have occurred.
    b. The authorization has not been filled out completely, with respect to an element described by this policy, if applicable.
    c. The authorization is known by UIW to have been revoked.
    d. The authorization violates this paragraph, or paragraphs below, if applicable; and
    e. Any material information in the authorization is known by UIW to be false.
2. An authorization for use or disclosure of PHI may not be combined with any other document to create a compound authorization, except as follows:
    a. An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of PHI for such research or a consent to participate in such research.
    b. An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes; and
    c. An authorization under this policy, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when UIW has conditioned the provision of treatment, payment, enrollment in the health plan or eligibility for benefits on the provision of one of the authorizations.
3. UIW may not condition treatment, payment, or enrollment in a health plan, or eligibility for benefits on the provision of an authorization, except:
    a. UIW may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of PHI for such research under this policy.
    b. UIW 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:

i. 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
ii. The authorization is not for the use or disclosure of psychotherapy notes.

c. UIW may require an authorization for release to a third party before providing health care that is solely for the purpose of creating PHI for disclosure to a third party.

4. An individual may revoke an authorization provided under this policy at any time, provided that the revocation is in writing, except to the extent that:
   a. UIW has acted in reliance thereon; and
   b. 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.
5. UIW must document and retain any signed authorization.

Core Elements and Requirements:

1. **Core Elements:** A valid authorization under this section must contain at least the following elements (but may contain additional information):
   a. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
   b. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
   c. The name or other specific identification of the person(s), or class of persons, to whom UIW may make the requested use or disclosure.
   d. 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.
   e. 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
   f. 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.
2. In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:
   a. The individual's right to revoke the authorization in writing, and either:
      i. The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or
      ii. To the extent that the information in paragraph (1) above is included in the notice of privacy practices.
   b. The ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization, by stating either:

i. UIW may not condition treatment, payment, enrollment, or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in this policy applies; or
ii. The **consequences** to the individual of a refusal to sign the authorization when, in accordance with this policy (i.e., for research, health plan eligibility, underwriting purposes, and risk rating determinations), UIW can condition treatment, enrollment in a health plan, or eligibility for benefits on failure to obtain such authorization; and
iii. 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.

3. The authorization must be written in plain language.
4. If UIW seeks an authorization from an individual for the use or disclosure of PHI, UIW must provide the individual with a copy of the signed authorization.

RELEVANT HIPAA REGULATIONS:

- §164.508 *Uses and Disclosures for Which an Authorization is Required*

Continued on Next Page

Privacy 8.0 Uses and Disclosures, No Authorization Required

FULL POLICY LANGUAGE:

Policy Purpose:

To set forth rules regarding when **UIW** may use or disclose individual protected health information (PHI) without first having to obtain written patient authorization.

Policy Description:

Under several circumstances, the HIPAA Privacy Rule permits **UIW** to use or disclose PHI without written patient authorization. These circumstances are circumstances under which the law requires such use or disclosure.

Procedures:

Uses and Disclosures Required by Law:

1. UIW may use or disclose PHI to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.
2. UIW must disclose PHI as required by law 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:

1. UIW may disclose PHI related to public health activities if:
   a. A public health authority that is authorized by law to collect or receive such information, request the PHI 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
   b. It is necessary to report child abuse or neglect.
2. 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 individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or
d. To conduct post-marketing surveillance.

3. 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 **UIW** or public health authority is authorized by law to notify such person. An employer, about an individual who is a member of the workforce of the employer, if:
    a. The Covered Entity is the employee's health care provider and requests the information:
        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, or under State law having a similar purpose to record such illness or injury, or to carry out responsibilities for workplace medical surveillance; or
4. 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:
    a. By giving a copy of the notice to the individual at the time the health care is provided; or
    b. 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.
5. 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. **UIW** 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 as an unemancipated minor.

If the covered entity described in (1) through (5) immediately above, is also a public health authority, the covered entity may use protected health information in all cases in which it is permitted to disclose such information for the public health activities specified in (1) through (5) above.

PHI may also be used or disclosed without authorization or affording an individual the opportunity to agree or object under the following circumstances.

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

1. UIW may disclose PHI about an individual whom UIW 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.
    c. To the extent the disclosure is expressly authorized by statute or regulation, and:
        i. UIW, 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, is made, UIW must promptly inform the individual that such a report has been or will be made, except if:
    a. UIW, in the exercise of professional judgment, believes that informing the individual would place the individual at risk of serious harm; or
    b. UIW would be informing a personal representative and UIW 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 UIW, in the exercise of professional judgment.

Uses and Disclosures for Health Oversight Activities:

1. UIW 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 health care 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 "Uses and Disclosures for Health Oversight Activities," above, does 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 related to:
    a. The receipt of health care.
    b. A claim for public benefits related to health; or
    c. Qualification for or receipt of public benefits or services when a patient'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 UIW also is a health oversight agency, the covered entity may use PHI for health oversight activities as permitted by this policy.

Uses and Disclosures About Decedents:

1. **Coroners and Medical Examiners: UIW** 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. UIW 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, UIW may disclose the PHI prior to, and in reasonable anticipation of, the individual's death.
3. UIW may use or disclose PHI to organ procurement UIWs 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 for Research Purposes:

1. UIW may use or disclose PHI for research, regardless of the source of funding of the research, provided that:
    a. Board approval of a waiver of authorization is made available.
    b. UIW 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:
            1. 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.
            2. Includes at least one member who is not affiliated with UIW, 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

3. Does not have any member participating in a review of any project in which the member has a conflict of interest.

c. (Reviews preparatory to research). UIW obtains from the researcher representations that:
    i. Use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research.
    ii. No PHI is to be removed from UIW by the researcher in the course of the review; and
    iii. The PHI for which use, or access is sought is necessary for research purposes.
d. (Research on decedent's information). UIW obtains from the researcher:
    i. Representation that the use or disclosure sought is solely for research on the PHI of decedents.
    ii. Documentation, at the request of UIW, of the death of such individuals; and
    iii. Representation that the PHI for which use, or disclosure is sought is necessary for research purposes.
e. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, the documentation must include all of the following:
    i. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved.
    ii. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:
        1. The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals based on, at least, the presence of the following elements:
            a. An adequate plan to protect the identifiers that lead to individual patients from improper use and disclosure.
            b. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
            c. Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI is needed.
    iii. The research could not be conducted without the waiver or alteration; and

iv. The research could not be conducted without access to and use of the PHI.

f. A brief description of the PHI for which use, or access has been determined to be necessary by the IRB or privacy board, as determined pursuant to the above paragraph.
g. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:
    i. The Internal Review Board must follow the requirements of the HIPAA Rules, including the normal review procedures or the expedited review procedures.
    ii. The Privacy Board must review the proposed research at a convened meeting at which a majority of the privacy board members are present, including at least one member who satisfies the Privacy Officer or Compliance Officer title, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with the below paragraph; and
    iii. A Privacy Board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the PHI for which use, or disclosure is being sought. If the Privacy Board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the Privacy Board, or by one or more members of the Privacy Board as designated by the chair; and
h. The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair of the IRB or the privacy board, as applicable.

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

1. UIW may, consistent with applicable law and standards of ethical conduct, use or disclose PHI if UIW, 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 able to prevent or lessen the threat, including the target of the threat.
    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 UIW 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 UIW**:**
    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. UIW, when using or disclosing PHI, is presumed to have acted in good faith if the belief is based upon UIW's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

RELEVANT HIPAA REGULATIONS:

- §164.501 *Uses and Disclosures for Health Care Operations*
  §164.512 *Consent or Authorization Not Required*

Continued on Next Page

Privacy 9.0 Uses and Disclosures Requiring Patient Opportunity to Agree or Object

FULL POLICY LANGUAGE:

Policy Purpose:

To inform employees of the situations under which a patient must be given an opportunity to agree or object to use or disclosure of their PHI.

Policy Description:

Under several circumstances, before **UIW** may use or disclose an individual's PHI, that person must be given an opportunity to agree or object to the use or disclosure.

Procedures:

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

UIW may use or disclose PHI, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to, or prohibit/restrict the use or disclosure, in accordance with the applicable requirements of this section. UIW may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section. The requirement of opportunity to agree or prohibit applies in the following circumstances:

Use and Disclosure for Facility Directories:

1. Permitted uses and disclosure. Except when an objection is expressed, UIW may:
    a. Use the following PHI to maintain a directory of individuals in its facility:
        i. The individual's name.
        ii. The individual's location in UIW**'s** facility.
        iii. The individual's condition described in general terms that does not communicate specific medical information about the individual; and
        iv. The individual's religious affiliation; and
    b. Use or disclose for directory purposes such information:
        i. To members of the clergy; or
        ii. Except for religious affiliation, to other persons who ask for the individual by name.
2. **Opportunity to Object:** UIW must inform an individual of the PHI that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by this section.
3. **Emergency Circumstances:**

a. If the opportunity to object to uses or disclosures cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, UIW may use or disclose some or all of the PHI permitted by this section for the facility's directory, if such disclosure is:
    i. Consistent with a prior expressed preference of the individual, if any, that is known to UIW; and
    ii. In the individual's best interest as determined by UIW, in the exercise of professional judgment.
b. UIW must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes when it becomes practicable to do so.

Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes:

1. **Permitted Uses and Disclosures**:
    a. UIW 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.
    b. UIW 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.
2. **Uses and Disclosures with the Individual Present:** If the individual is present for, or otherwise available prior to, a use or disclosure permitted by 45 CFR 164.510 and has the capacity to make health care decisions, UIW may use or disclose the PHI if it:
    a. Obtains the individual's agreement.
    b. Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
    c. Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.
3. 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, UIW may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. UIW may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.
4. Uses and disclosures for disaster relief purposes. UIW 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 permitted by this section.

5. Uses and disclosures when the individual is deceased. If the individual is deceased, UIW 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 UIW.

RELEVANT HIPAA REGULATIONS:

- §164.510 *Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object*

Continued on Next Page

UNIVERSITY OF THE INCARNATE WORD

Privacy 10.0 Complaints

FULL POLICY LANGUAGE:

Policy Purpose:

To maintain an effective method for reporting concerns or complaints about **UIW's** privacy policies and procedures; **UIW's** compliance with those policies and procedures, and **UIW's** compliance with the HIPAA Privacy Rule and the HIPAA Breach Notification Rule.

Policy Description:

UIW 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. **UIW** strives to ensure that data breaches are responded to in an appropriate fashion, in accordance with the HIPAA breach notification rule and other applicable law. Individuals have the right to make complaints concerning **UIW's** compliance with the HIPAA Privacy Rule and its HIPAA privacy policies and procedures ("Privacy Complaints"). Individuals also have the right to make complaints concerning UIW**'s** breach notification process and compliance with the Breach Notification Rule.

Procedures:

Processing a Complaint:

1. **UIW's** Notice of Privacy Practices must notify all patients (or their personal representatives) of their right to complain to **UIW** or the Department of Health and Human Services ("HHS").
2. Complaints may be made in person, or by telephone or mail.
3. Workforce members should forward complaints to the Privacy Officer.
4. Upon receipt of any complaint, the Privacy Officer 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 Officer shall coordinate with appropriate individuals to determine whether an investigation is warranted. If an investigation is warranted, the Privacy Officer shall conduct the investigation and determine if a violation of the HIPAA Privacy Rule, the HIPAA Breach Notification Rule, or UIW's HIPAA privacy or breach notification policies and procedures has occurred. The Privacy Officer should make all reasonable efforts to complete the investigation in a timely manner.
6. Upon completion of the investigation, the Privacy Officer 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 individual who made the complaint within 30 days from the Privacy Officer's receipt of the complaint.

7. If the Privacy Officer determines that a violation of policy, procedure, the HIPAA Privacy Rule, or the HIPAA Breach Notification Rule has occurred, the Privacy Officer shall initiate and coordinate actions as appropriate according to **UIW's** Sanctions Policy (see Privacy Policy 24.0).
8. The Privacy Officer 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(d) *Complaints*

Continued on Next Page

UNIVERSITY OF THE INCARNATE WORD

Privacy 11.0 Sanctions

FULL POLICY LANGUAGE:

Policy Purpose:

To ensure that appropriate sanctions will be applied to employees who violate the requirements of the HIPAA Privacy Rule and/or UIW's HIPAA privacy policies and procedures. To ensure that appropriate sanctions will be applied to employees who violate the requirements of the HIPAA Breach Notification Rule and/or UIW's HIPAA Breach Notification Rule policies and procedures.

Policy Description:

It is **UIW's** policy to impose sanctions, as applicable, for violations of **UIW's** policies and procedures regarding workforce HIPAA compliance. It is also **UIW's** policy to monitor compliance with HIPAA policies and to mitigate, to the extent practicable, any harm resulting from inappropriate use or disclosure of protected health information.

Procedures:

Sanctions:

1. When a concern arises regarding a potential violation of the HIPAA Privacy Rule or Breach Notification Rule, the Privacy Officer shall promptly investigate.
2. The Privacy Officer shall uniquely and consistently apply corrective disciplinary action when warranted.
3. The Privacy Officer may consider several criteria when determining the appropriate disciplinary measure.
    a. What was the intent behind the inappropriate use or disclosure of PHI?
        i. Was the use or disclosure unintentional?
        ii. Was the use or disclosure unintentional, and did the use or disclosure result in a reportable breach?
        iii. Was the use or disclosure intentional?
    b. What is the risk to UIW resulting from inappropriate use or disclosure?
        i. Is there a potential risk for patient harm?
        ii. Is there a risk of harm to UIW?
        iii. Is there a risk the public may be affected by inappropriate use or disclosure?
    c. What is the history of the employee or workforce member's work performance?
        i. Has the employee or workforce member previously been disciplined for previous inappropriate use or disclosure of PHI?
        ii. Has the employee or workforce member been subject to a series of progressive discipline actions, related or unrelated to privacy of PHI?

iii. What is the history of **UIW's** disciplinary actions for similar infractions (whether privacy-related or otherwise) committed by *other* employees or workforce members?

d. Are there mitigating circumstances that would support reducing disciplinary/corrective action in the interest of fairness and consistency?

4. In UIW's discretion, inappropriate use and/or disclosures of PHI may be divided into the following three levels with recommended corresponding disciplinary action for each:

a. Level 1 Infraction:

i. Nature of infraction: unintentional, resulting in no breach.

ii. Description of infraction: Infraction occurs when a workforce member unintentionally or carelessly accesses, reviews, or reveals PHI to themselves or to others, either without a legitimate need to know, or beyond what the minimum necessary standard permits.

iii. **Examples of Infraction Include:**

1. Discussing PHI in public areas, such as elevators and lobbies.
2. Inadvertently typing in the wrong patient's name and viewing the wrong patient's PHI as a result.
3. Leaving PHI accessible in a work area, such as leaving patient medical records unattended in a meeting room.

iv. **Recommended Discipline:** Recommended discipline can consist of a verbal warning, and/or additional HIPAA training.

b. Level 2 Infraction:

i. **Nature of Infraction:** An unintentional infraction that results in a reportable breach.

ii. **Description of Infraction:** Infraction occurs when a workforce member unintentionally or carelessly accesses, reviews, or reveals PHI to themselves or others without a legitimate need to know or beyond what the minimum necessary standard requires, AND a reportable breach results.

iii. **Examples of Infraction Include:**

1. Faxing or mailing the wrong patient's information to another entity, resulting in a breach.
2. Inappropriately accessing or disclosing a patient's medical information, either in disregard of the minimum necessary standard, or when the workforce member's role does not authorize access to PHI.
3. Compromising a password by sharing it, resulting in access to PHI.

iv. **Recommended Discipline:** Recommended discipline varies depending on the circumstances. Recommended discipline can range from a written reprimand, final warning, suspension, or unpaid leave, up to, in the case of multiple severe infractions that lead to breaches, termination of employment.

c. Level 3 Infraction:

i. **Nature of Infraction:** Intentional (deliberate and on purpose).

ii. **Description of Infraction:** An intentional infraction occurs when a workforce member accesses, reviews, or discusses PHI either for personal financial or other gain, or with malicious intent (intent to harm UIW, a patient, or the public); a workforce member willfully, and with gross negligence, uses and/or discloses PHI, or destroys PHI; or a workforce member knowingly violates federal and/or and state laws and regulations protecting PHI privacy and security.

iii. **Examples of Infraction Include:**
   1. Deliberately inappropriate access to medical records of the workforce member's family, friends, acquaintances, or prominent individuals.
   2. Intentional unauthorized disclosure of patient information to a third party, including to a friend, relative, or the media.

iv. **Recommended Discipline:** The recommended discipline varies depending on the circumstances. Recommended discipline ranges from a written reprimand, a final warning, a suspension, or unpaid leave, to termination.

Appeals:

1. In the event that a sanction triggers any process of appeal under an applicable UIW disciplinary policy and procedure, the workforce member is entitled to file an appeal. The Privacy Officer 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 UIW 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. UIW 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 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 discipline.
2. Such documentation shall be retained in accordance with **UIW's** document retention policies, and, in any event, for no less than six years.

Mitigation:

1. In response to a report of or information about a workforce member's or business associate's unauthorized use or disclosure of PHI, **UIW** shall act promptly to mitigate (reduce) any known or anticipated harmful effects from the disclosure.
2. **UIW** should promptly identify who made the unauthorized use or disclosure and apply appropriate sanctions.
3. **UIW** shall contact the recipient of the information that was subject to the unauthorized disclosure and request that such recipient either destroy or return the information.
4. **UIW** shall take any and all other appropriate action to prevent further use or disclosure.
5. **UIW**, in accordance with the HIPAA Breach Notification Rule, shall notify the patient or patients whose PHI was or were the subject of unauthorized use or disclosure.
6. **UIW**, in accordance with the HIPAA Breach Notification Rule, shall notify HHS, the media, and/or any other individuals or entities who must receive notification.
7. **UIW** shall document all mitigation efforts and retain such documentation for at least six (6) years.

RELEVANT HIPAA REGULATIONS:

- 45 CFR 164.530(e) *Sanctions*
- 45 CFR 164.530(f) *Mitigation*

Continued on Next Page

Privacy 12.0 No Retaliation; No Waiver of Rights

FULL POLICY LANGUAGE:

Policy Purpose:

To ensure individuals who file complaints are not intimidated or retaliated against by **UIW** or any workforce member. To ensure that individuals are not subjected to waiving their rights to complain under the HIPAA Privacy Rule and the HIPAA Breach Notification Rule in order to receive treatment.

Policy Description:

UIW may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right under the Privacy Rule, Breach Notification Rule, or **UIW's** policies and procedures pertaining to same. In addition, UIW may not require individuals to waive their rights to complain under HIPAA, as a condition of the provision of treatment.

Procedures:

Refraining from Intimidating or Retaliatory Acts:

1. **UIW** shall prohibit the taking of any intimidating or retaliatory acts against any individual or other person (including a workforce member) for:
    a. Exercising their rights or participating in any process established by the HIPAA Rules, such as filing a complaint with HHS about **UIW's** privacy policies or practices, or breach notification process, policies, or practices.
    b. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing authorized by the HIPAA Rules; or
    c. Opposing any act or practice that violates the HIPAA Rules, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of HIPAA.
    d. Disclosing PHI, if:
        i. The person believes in good faith either that UIW has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care or services provided by **UIW** potentially endanger one or more individuals, workers, or the public; **and**
        ii. 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 **UIW.**
    e. Disclosing PHI to a law enforcement official in compliance with this Manual and with the HIPAA regulations.

2. Prohibited actions include any acts by UIW, its workforce members, or business associates, that threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against an individual, because that individual has engaged in an activity mentioned in 1(a) through 1(e) above.
3. Any workforce member who is aware of, or believes he or she is the victim of, intimidating or retaliatory acts committed by a workforce member or business associate should report his or her concerns to the Privacy Officer. Such reports, so long as they are made in good faith, are also protected from retaliation.
4. Upon receipt or report of an allegation that an individual has been subjected to intimidation or retaliation, the Privacy Officer shall investigate, and upon conclusion of the investigation, shall impose appropriate sanctions.

No Waiver of Rights:

1. UIW may not require an individual to waive any complaint rights they have under the HIPAA regulations, and UIW's policies and procedures, as a condition of treatment.
2. An individual who believes that UIW has insisted on or required such a waiver, shall notify the Privacy Officer.
3. The Privacy Officer shall review the allegations of the complaining individual.
4. Upon conclusion of investigation, the Privacy Officer shall impose appropriate sanctions.

RELEVANT HIPAA REGULATIONS:

- 45 CFR 164.530(g) *Refraining from intimidating or retaliatory acts.*
- 45 CFR 164.530(h) *Waiver of Rights*

Continued on Next Page

Privacy 13.0 Uses and Disclosures for Treatment, Payment, and Health Care

FULL POLICY LANGUAGE:

Policy Purpose:

To set forth the conditions under which UIW is not required to obtain written patient authorization before making a use or disclosure of PHI.

Policy Description:

To comply with the HIPAA Privacy Rule, **UIW** must obtain a signed patient authorization before making a use or disclosure of protected health information. However, the HIPAA Privacy Rule does not require UIW to obtain such authorization for treatment, payment, or healthcare operations purposes. **UIW** will not seek to obtain written authorization for these purposes unless an exception requiring written authorization applies, or when state law requires such authorization.

Procedures:

Treatment:

1. "Treatment" is the provision, coordination, or management of health care and related services among health care providers **or by** a health care provider with a third party; consultation between health care providers regarding a patient; or the referral of a patient from one health care provider to another.
2. UIW will not obtain written patient authorization prior to use or disclosure of PHI for treatment purposes.

Payment:

1. "Payment" encompasses the various activities of health care providers to obtain payment or be reimbursed for their services. Common payment activities of providers and health plans include, but are not limited to:
    a. Determining eligibility or coverage under a plan and adjudicating claims.
    b. Risk adjustments.
    c. Billing and collection activities.
    d. Reviewing health care services for medical necessity, coverage, justification of charges, and the like.
    e. Utilization review activities; and
    f. Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about UIW).
2. UIW will not obtain written patient authorization prior to use or disclosure of PHI for payment purposes.

Healthcare Operations:

1. "Health care operations" are certain administrative, financial, legal, and quality improvement activities of UIW that are necessary to run its business and to support the core functions of treatment and payment. These activities include:
    a. Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination.
    b. Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities.
    c. Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims.
    d. Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs.
    e. Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
    f. Business management and general administrative activities, including those related to customer service, or the sale or transfer of assets.
2. UIW will not obtain written patient authorization prior to using or disclosing PHI for healthcare operations.

Exceptions Requiring Prior Written Authorization

Generally, **UIW** will not seek prior written authorization for treatment, payment, or healthcare operations purposes. However, UIW will obtain such authorization if required by federal or state law. Federal law or state law may require obtaining written patient authorization before certain uses or disclosures of PHI can be made. These uses or disclosures for which authorization may be required include:

1. Disclosures that are required by state law, provided that UIW discloses only the precise protected health information required, and only to the recipient required.
2. Disclosures to state, local or federal governmental public health authorities to prevent or control disease, injury, or disability.
3. Disclosures to local, state, or federal governmental agencies to report suspected child abuse or neglect.
4. Disclosures to individuals or UIWs under the jurisdiction of the federal Food and Drug Administration ("FDA"), such as drug or medical device manufacturers, regarding the quality or safety of drugs or medical devices.
5. Disclosures for health oversight audits, investigations, or disciplinary activities, provided that UIW only disclose to a federal, state, or local governmental agency (or a private person or UIW acting under contract with or grant of authority from the governmental agency) that is authorized by law to conduct oversight activities.

6. Disclosures to police or other law enforcement officers regarding a crime that UIW believed happened at its facility, provided that **UIW** believes that the protected health information is evidence of a crime.
7. Disclosures to UIWs involved in the procurement, banking, or transplantation of organs in order to facilitate organ donation and transplantation.

Minimum Necessary Standard:
UIW shall limit its disclosures of, and requests for, protected health information for payment and health care operations to the minimum necessary. **UIW** is not required to apply the minimum necessary standard to disclosures to or requests by a health care provider for treatment purposes.

RELEVANT HIPAA REGULATIONS:

- 45 CFR 164.506 *Treatment, Payment, or Healthcare Operations*

Continued on Next Page

UNIVERSITY OF THE INCARNATE WORD

Privacy 14.0 Sale of PHI

FULL POLICY LANGUAGE:

Policy Purpose:

To ensure sale of PHI is not conducted without prior written patient authorization.

Policy Description:

In accordance with the HIPAA Privacy Rule, **UIW** shall not directly or indirectly receive remuneration, including non-financial benefits such as in-kind benefits, in exchange for any protected health information, unless prior written patient authorization is obtained.

Procedures:

1. If **UIW** receives direct or indirect remuneration from or on behalf of a person or entity in exchange for PHI, that exchange is a sale of PHI. For such an exchange, a valid, written authorization must be obtained from the patient who is the subject of the information.
2. Prior to disclosing any PHI in exchange for direct or indirect remuneration, the Privacy Officer shall confirm whether the contemplated disclosure is a sale of PHI.
3. The disclosure of PHI for any of the following purposes is not considered a sale of PHI under the HIPAA Privacy Rule:
    a. Public health purposes.
    b. Research purposes, where the remuneration is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI.
    c. Treatment and payment purposes.
    d. The sale, transfer, merger, or consolidation of all or part of UIW with another UIW, or an entity that will become another company following the transaction and due diligence related to this activity.
    e. To patients, where the patient requests access to PHI or an accounting of disclosures.
    f. Disclosures required by law; and
    g. Any other disclosures permitted by the HIPAA Privacy Rule, where the only remuneration received by UIW, or the business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI or a fee otherwise expressly permitted by law.
4. Any disclosure of PHI in exchange for remuneration that meets an exception under HIPAA shall be further evaluated under applicable state law to ensure the exchange is permissible without written patient authorization under applicable state law.
5. If a disclosure of PHI meets the definition of a sale of PHI and an applicable exception does not apply, **UIW** shall obtain prior written patient authorization.
    a. Patient authorization shall be obtained, and the authorization obtained shall meet the requirements of HIPAA and applicable state law. The authorization

shall specifically disclose that UIW will receive direct or indirect remuneration in exchange for the PHI.

b. **UIW** shall place a copy of the signed authorization form in the patient's medical record.
c. Questions related to whether a transaction is a "Sale of PHI" disclosure that do not fall under an exception in (3) above, shall be reported to the Privacy Officer, who shall evaluate whether the disclosure constitutes a Sale of PHI.

6. **Workforce Members Must:**
    a. Ensure that any direct or indirect remuneration in exchange for PHI that constitutes a sale of PHI meets an exception and is permissible under HIPAA and applicable state law without individual authorization.
    b. For such activities that do not meet an exception, obtain patient authorization in the form and manner required by HIPAA and applicable state law before a disclosure of PHI in exchange for remuneration.

RELEVANT HIPAA REGULATIONS:

- 45 CFR 164.508(a)(4) *Sale of PHI*

Continued on Next Page

Privacy 15.0 Policy for Disclosures by Whistleblowers and Workforce Member Crime Victims

FULL POLICY LANGUAGE:

Policy Purpose:

To outline the policies and procedures for disclosure of PHI by whistleblowers and workforce member crime victims.

Policy Description:

Under the Privacy Rule "whistleblower exception," workforce members and their business associates, have the right to disclose PHI if they believe in good faith that another workforce member or business associate has engaged in conduct that is unlawful or otherwise violates professional standards. Workforce members 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.

In addition, under the "workforce member crime victims" exception to the Privacy Rule, workforce members who are victims of a crime may disclose protected health information about the suspected perpetrator of the criminal act; to law enforcement, provided the information disclosed is limited as described in this policy.

Procedures:

Disclosures by Whistleblower

1. **UIW's** workforce members and business associates may make whistleblower disclosures of an individual's PHI without the individual's written authorization.
2. **UIW** will not impose any sanctions upon and will not take any intimidating or retaliatory actions against members of **UIW's** workforce and **UIW's** business associates who make Whistleblower Disclosures related to **UIW's** handling of PHI and compliance with HIPAA.
3. **UIW** 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, **UIW** 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:
    a. The workforce member believes, in good faith, that:
        i. UIW has engaged in unlawful conduct; or
        ii. UIW has engaged in conduct that otherwise violates professional or clinical standards; or

iii. The care, services, or conditions provided by UIW potentially endanger patients, workers, or the public.

5. To qualify as protected whistleblowing activity, the PHI disclosures listed above must be made to:
    a. An appropriate healthcare accreditation UIW for the purpose of reporting the allegation of failure to meet professional standards or misconduct by UIW; **or**
    b. A health oversight agency or public health authority that has the authority to investigate or oversee the relevant conduct or conditions of UIW; **or**
    c. An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct alleged to be improper.
6. **Limitation on Disclosures:** Disclosures can only be made if the 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. 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.

Disclosures by Workforce Member Crime Victims:

1. A workforce member 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 UIW 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 workforce member considers himself or herself a workforce crime victim, he/she should immediately notify the HIPAA Privacy Officer, who shall advise the workforce member as to what PHI (see paragraph (1)) may be disclosed to law enforcement.

RELEVANT HIPAA REGULATIONS:

- 45 CFR 164.502(j) *Disclosures by Whistleblowers and Workforce Member Crime Victims*

Privacy 16.0 Use or Disclosure for Specialized Government Functions

FULL POLICY LANGUAGE:

Policy Purpose:

To describe the circumstances under which PHI may be disclosed to government personnel and agencies for purposes of specialized government functions.

Policy Description:

UIW 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

This policy describes how **UIW** will use and disclose PHI for these specialized government functions.

Procedures:

1. **Military and Veterans Activities:**
   a. **Armed Forces Personnel: UIW** 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.
   b. 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.
   c. **Foreign Military Personnel: UIW** may use or disclose to the appropriate military authority the PHI of individuals who are foreign military personnel for the same purposes for which **UIW** may use or disclose PHI regarding Armed Forces Personnel as described above.
2. **National Security and Intelligence Activities: UIW** may disclose PHI to authorized federal officials as necessary to conduct lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. § 401, et. seq.) and implementing authority (e.g., Executive Order 12333).
3. **Protective Services for the President and Others: UIW** 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).

4. **Correctional Institutions and Other Law Enforcement Custodial Situations: UIW** 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 an individual or another inmate.
   c. The health and safety of the officers or employees, of 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.
   e. The administration and maintenance of safety, security, and good order of the correctional institution.
   f. 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.
5. **Minimum Necessary and Accounting for Disclosures:**
   a. **Minimum Necessary Rule:** If **UIW** is permitted to make a disclosure of PHI as described above, **UIW** may disclose only the information specified for the particular situation. If no specific information is specified for a particular situation, then **UIW** may disclose only the minimum necessary PHI to accomplish the purpose of the disclosure.
   b. **Accounting for Disclosures: UIW** must keep a record of any disclosures made to law enforcement pursuant to this policy. This information shall be available to any individual who is the subject of such a disclosure and who requests an accounting of such a disclosure. Records regarding disclosures to law enforcement must be kept for at least 6 years after the date of the disclosure.

RELEVANT HIPAA REGULATION:

- 45 CFR 164.512(k) *Uses and Disclosures for Specialized Government Functions*

UNIVERSITY OF THE INCARNATE WORD

Privacy 17.0 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. To describe the process for creating the Data Use Agreement that must be signed before sharing a Limited Data Set.

Policy Description:

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

Since a limited data set is still identifiable protected health information, a limited data set may only by shared by **UIW** with entities that have signed a Data Use Agreement with **UIW.** A Data Use Agreement allows **UIW** 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. **UIW** 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, UIW 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
    c. Age (in years, months, days, or hours)
4. Only authorized **UIW** workforce members, or authorized business associates, may create a limited data set.
5. If a business associate creates the limited data set, **UIW** must enter into a business associate agreement before the business associate can create the limited data set.

Data Use Agreement:

1. **UIW** may use or disclose a limited data set, only if **UIW** first obtains a signed, written obtains a Data Use Agreement (DUA) from the person/entity to whom the Limited Data Set is to be disclosed.
2. A DUA must be entered before there is any use or disclosure of a limited data set to an outside party. A Data Use Agreement must:
    a. Establish the permitted uses and disclosures of such information by the limited data set recipient. The Data Use Agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate HIPAA privacy requirements, if done by UIW.
    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 data use agreement 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 data use agreement.
        iii. Report to UIW any use or disclosure of the information not provided for by its data use agreement of which it becomes aware.
        iv. Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
        v. Not identify the information or contact the individuals.
3. **Noncompliance by Limited Data Set Recipient**: If at any time **UIW** 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 **UIW** shall take reasonable steps to cure the breach or end the violation. If the breach cannot be cured or the violation ended, then **UIW** must cease all disclosures of the Limited Data 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*

Continued on Next Page

UNIVERSITY OF THE INCARNATE WORD

Glossary

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

Access Control: Control of the ability or the means necessary to read, write, modify, or communicate ePHI.

Accounting of Disclosures of PHI: Information that describes a covered entity's disclosures of PHI other than for treatment, payment, and health care operations; disclosures made with written patient authorization; and certain other limited disclosures.

Administrative Tribunal: A judge or group of judges who conduct hearings and exercise judgment over specific issues.

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

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

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

Audit Logs: Records of events based on applications, users, and systems.

Authorization: A patient's written statement of agreement to the use or disclosure of protected health information.

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: Any entity that uses or discloses protected health information (PHI) on behalf of a Covered Entity (i.e., group health plan, hospital, etc.). Furthermore, a Business Associate is any person or UIW that, on behalf of a Covered Entity, performs (or assists in the performance of) a function or activity involving the use or disclosure of PHI.

Business Associate Agreement/Business Associate Contract: A business associate agreement/business associate contract is a contract or other written arrangement, enforceable by law, between the covered entity and the business associate. The contract must be entered into before the business associate can create, receive, or transmit any PHI. In addition, the contract must (among other things):

- Describe the permitted and required uses of protected health information by the business associate.
- Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and
- Require the business associate to use appropriate safeguards to prevent the use or disclosure of the protected health information other than as provided for by the contract.

Optimally, such contracts should be drafted as to apportion liability to where it properly is placed. Optimally, contracts should contain provisions to the effect that a covered entity is liable under the law for its breach (if any) of unsecured protected health information, and that the business associate is liable under the law for its breach (if any) of unsecured protected health information.

Business Associate Functions and Activities Include: claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate services are legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

Chief or Lead Compliance Officer: The individual designated by **UIW** as being in charge of overall privacy and security compliance for UIW. The Chief Compliance Officer is the only individual within UIW who can resolve a security incident.

Confidentiality Agreement: An agreement between a healthcare UIW and a vendor, or an agreement between a healthcare UIW and a member of its staff. The agreement requires that any UIW hired to perform a task, or any UIW employee, who accidentally encounters ePHI, keep such ePHI confidential.

Covered Entity: A health plan or a health care provider that stores or transmits any health information in electronic form in connection with a HIPAA covered transaction.

Critical Business Functions: Critical business processes that are needed for protection of the security of electronic protected health information.

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."

Decryption Key: Computer code required to transform (decrypt) an encrypted message, document, or other data into a form that can be freely read.

Degaussing: The process of demagnetizing data. Once a hard drive is degaussed, it cannot be read again.

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 may include patient medical and billing records; the enrollment, payment, claims, adjudication, and cases or medical management record systems maintained by or for a health plan; or information used in whole or in part to make care-related decisions.

Disclosure: To release, transfer, prove access to, or divulge PHI to a third party.

Encryption: Under the HIPAA Security Rule, encryption is defined as "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.

Encryption Key: A random string of bits (tiny pieces of information, represented as numbers) generated specifically to scramble and unscramble data. Encryption keys are created with algorithms designed to ensure that each key is unique and unpredictable.

ePHI: Electronic/Protected health information means individually identifiable health information that is:

- Transmitted by electronic media.
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

Extranet: A controlled private network that allows access to specific entities (i.e., partners, vendors, or suppliers). Extranet access is limited to a subset of the information accessible from UIW's intranet.

Facility Directory: A directory of UIW's staff. Patient information may be included in this directory. This information may include patient name, location (room/bed number), condition described in general terms (i.e., "Not feeling well," "Having a good day"), and religious affiliation. Religious affiliation is available to clergy members only.

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

Health Care Operations: Quality assessment and improvement activities; reviewing the competence, qualifications, performance of health care professionals, conducting training programs, accreditation, certification, licensing, credentialing, underwriting, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits; conducting or arranging for medical review, legal services, and audition functions; business planning and development; business management (§164.501).

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, 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 individuals the right to access their protected information; the right to request that this information be amended; 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 individuals. The Privacy Rule also outlines when patient 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.

HIPAA Security Rule: The HIPAA Security Rule requires healthcare UIWs to protect patients electronically stored, protected health information (known as "ePHI") by using appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of this information.

Individual: The patient and his/her Personal Representative.

Individually Identifiable Health Information: Any information, including demographic information, collected from an individual 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; and
    a. Identifies the individual; or
    b. With respect to which there is a reasonable basis to believe that the information can 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.

Intranet: An **intranet** is a private network that can only be accessed by authorized users. An **intranet** is designed for internal communications within **UIW**.

LAN: Stands for Local Area Network. A Local Area Network is a computer network that links devices within a building or group of adjacent buildings.

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 patients, if certain conditions are met.

Malware: Malware is short for "malicious software." Malware consists of programs designed to damage computer systems. Malware consists of (among other things) viruses, worms, trojan horses, and spyware.

Marketing: The provision of information about a product or service that encourages recipients of the communication to purchase or use the product or service.

Medical Record: A collection of documents, notes, forms, and test results that collectively document healthcare services provided to a patient in any aspect of health care delivery by a provider.

Minimum Necessary: The least amount of protected health information (PHI) needed to achieve the intended purpose of the use or disclosure of that PHI.

Network Closet: A **closet** or a small room where electrical **wiring** and computer **networking** hardware are installed.

Notice of Privacy Practices: A document required by the HIPAA Privacy Rule. The Notice of Privacy Practices must provide patients with information on how UIW uses their PHI, and what patients' rights are with respect to that PHI.

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

Opt-Out: To make a choice to be excluded from services, procedures, or practices.

Paper PHI: Protected health information that is not in an electronic format.

Payment: Activities undertaken by UIW to obtain or provide reimbursement for the provision of health care. Activities for payment include eligibility of coverage determination, billing, claims management, collection activities, utilization review including precertification, preauthorization, concurrent and retrospective review of services, and specified disclosures to consumer reporting agencies.

Personal Representative: is one who, under law, has the authority to act on behalf of a patient in making decisions related to health care Personal Representatives may have access to and/or request amendment of PHI relevant to their representative capacity, unless there is a reasonable belief that the patient has been or may be subjected to domestic violence, abuse, or neglect by such person, the release could endanger the patient, or in the exercise of professional judgment it is decided that it is not in the best interest of the patient to treat the person as the patient's personal representative.

Protected Health Information (PHI):
PHI is individually identifiable health information that is created by or received by UIW, including demographic information, which identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- The past, present, or future physical or mental health or condition of an individual.
- The provision of health care to an individual; or
- The past, present, or future payment for the provision of health care to an individual.

PHI is any health information that can be tied to an individual. Under HIPAA, PHI includes one or more of the following eighteen identifiers:

- Names
- Dates, except year
- Telephone numbers
- Geographic data
- FAX numbers
- Social Security numbers
- Email addresses
- Medical record numbers
- Account numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers including license plates
- Web URLs
- Device identifiers and serial numbers
- Internet protocol addresses
- Full face photos and comparable images
- Biometric identifiers (i.e., retinal scan, fingerprints)

- Any unique identifying number or code

Privacy Breach: A violation of the responsibility to follow privacy policy and procedure that results in the accessing of PHI by unauthorized personnel.

Privacy Officer: UIW'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): Individually identifiable health information that is created by or received by UIW, including demographic information, which identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present, or future physical or mental health or condition of an individual.
- The provision of health care to an individual; or
- The past, present, or future payment for the provision of health care to an individual.

Provider: A provider of medical or health services, and any other person or UIW who furnishes, bills, or is paid for health care in the normal course of business. Providers at UIW are those contracted, subcontracted, or employed and provide services on behalf of UIW.

Psychotherapy Notes: Notes recorded in any medium by a mental health professional documenting or analyzing the contents of a conversation during a counseling session.

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

Risk Analysis: Risk analysis is the assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the electronic protected health information (ePHI) held by a covered entity, and the likelihood of occurrence. A risk analysis may include taking inventory of all systems and applications that are used to access and house data and classifying them by level of risk. A thorough and accurate risk analysis considers all relevant losses that would be expected if the security measures were not in place, including loss or damage of data, corrupted data systems, and anticipated ramifications of such losses or damage.

Risk Management: Risk management is an information security process. This process requires an **UIW** to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the general requirements of the HIPAA Security Rule.

Satellite Office: A Satellite Office is a non-descript location, with no signage to state that it is part of, or performs services for, the main **UIW**. This location is used only for providing treatment. When treatment is finished, the individual leaves. Satellite Office is not used for storing PHI documented in physical or digital form. When leaving the Satellite Office, no footprints, computers, charts, or trash can be left behind. Nothing can be traced back to any of the PHI that was interacted with.

Security 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.

Security Incident: An attempt (whether successful or not) to do something unauthorized with respect to ePHI. The "something" that is unauthorized, is an unauthorized access, use, disclosure, modification, destruction, or interference.

Security Officer: A HIPAA security officer is responsible for the continuous management of information security policies, procedures, and technical systems in order to maintain the confidentiality, integrity, and availability of ePHI.

Security Rule Administrative Safeguards: These are safeguards that have to do with internal policies and procedures and proper employee training. Documented security policies and procedures create a uniform process that staff members can follow to maintain the security of ePHI. By implementing administrative safeguards, you can mitigate the potential for a security breach relating to human error.

Security Rule Confidentiality, Integrity, and Availability (CIA) of ePHI: The Security Rule defines "confidentiality" to mean that ePHI is not available or disclosed to unauthorized persons. Under the Security Rule, "integrity" means that ePHI is not altered or destroyed in an unauthorized manner. "Availability" means that ePHI is accessible and usable on demand by an authorized person.

Security Rule Physical Safeguards: These are safeguards that protect **UIW's** physical premises and infrastructure, to ensure there is no unauthorized ePHI access.

Security Rule Technical Safeguards: These are safeguards that include network security and data security. Technical safeguards include measures **UIW** can take to reduce the risk of a cybersecurity incident, especially relating to improper transmission of ePHI over email or malware.

System Administrator: An individual responsible for managing the operation of a computer system.

Training: The HIPAA Security Rule requires **UIW** to provide **workforce training and management.** To comply with this requirement, UIW shall at all times provide for appropriate authorization and supervision of workforce members who work with ePHI. **UIW** shall train all workforce members regarding its security policies and procedures. **UIW**

shall implement and apply appropriate sanctions against workforce members who violate its policies and procedures.

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 a patient; or the referral of a patient for health care from one health care provider to another.

Use: To share, examine, or analyze protected health information.

Virus: A virus is a piece of computer code that inserts itself within the code of another standalone program, then forces that program to take malicious action and spread itself.

VPN: Virtual Private Network. A VPN is an encrypted internet connection that allows users to safely transmit sensitive data, preventing unauthorized user access.

WAN: Stands for Wide Area Network. A Wide Area Network is a computer network to which the computers connected may be far apart (i.e., half a mile or more).

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

WLAN: Stands for Wireless Local Area Network. A wireless LAN is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area, such as a home, campus, or office building.

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UIW, is under the direct control of UIW, regardless of whether these individuals are paid by UIW.

Worm: A worm is a standalone piece of malicious software that reproduces itself and spreads from computer to computer.