Policy: Health Insurance Portability and Accountability Act (HIPAA)	**Policy No:** I-3.2
Policy Owner(s): Human Resources	**Original Date:** 4/20/2020
Last Review Date:	**Approval Date: 4/20/2020**

I. **POLICY**: In compliance with the Health Insurance Portability and Accountability Act (HIPAA), John Carroll University protects the privacy and security of protected health information (PHI) whenever it is accessed or stored by the University. Maintaining the privacy and security of PHI is the responsibility of all individuals with job duties requiring access to PHI in the course of their job duties.

II. **PURPOSE**: The Health Insurance Portability and Accountability Act (HIPAA) went into effect on April 14, 2003 to, among other things, protect the privacy and security of PHI. HIPAA applies to "Covered Entities," as defined by HIPAA's Privacy Rule. Because John Carroll University has at least one function that is a Covered Entity under HIPAA that is the University group health plan and electronically transmits health information, it is considered a hybrid Covered Entity.

III. **SCOPE**: All employees of John Carroll University

IV. **DEFINITIONS**:

Business Associate: A person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of the Covered Entity. Examples of business associate activities include: claims processing and administration; utilization review; quality assurance; billing; benefit management; accounting; actuarial; consulting; and legal services.

Covered Entity: As defined by HIPAA's Privacy Rule, and for purposes of this policy, a "Covered Entity" refers to (i) a healthcare provider that conducts certain transactions in electronic form; (ii) a healthcare clearinghouse; (iii) a health plan; or (iv) a business associate (person or organization) performing a function on behalf of the Covered Entity for which access to PHI is needed. The University's health plan is a covered entity under HIPAA, and the University is a hybrid entity under HIPAA.

Protected Health Information: For purposes of this policy, "Protected Health Information" or "PHI" refers to individually identifiable health information received by the University's group health plan or received by the health plan that relates to the past or present health of an individual or to payment of health care claims. PHI information includes medical conditions, health status, claims experience,

medical histories, physical examinations, genetic information, and evidence of disability.

V. **PROCEDURES**:

A. John Carroll as a Hybrid Entity. Since the primary function of John Carroll University is not to provide healthcare functions under HIPAA, the University is permitted to designate itself as a "hybrid entity," which allows it to apply the Privacy Rule only to those parts of the University that, if standing alone, would be a Covered Entity. As a hybrid entity, the University must designate its components that are covered by HIPAA.

Covered components at the University are:

1. The John Carroll University employee group health plans.

B. The HIPAA Privacy and Security Officers. The University has designated the Assistant Vice President of Human Resources as the HIPAA Privacy Officer. Any questions or issues regarding HIPAA compliance or PHI should be presented to the Privacy Officer for resolution. The Privacy Officer also is charged with the responsibility for:

1. Overseeing the development, implementation and adherence to privacy and security policies and procedures regarding the use and handling of PHI.
2. Ensuring employee privacy and security training.
3. Developing guidelines for describing how and when PHI will be maintained, used, transferred or transmitted and safeguarded.
4. Investigating incidents of breach of PHI and accept complaints of HIPAA violations.
5. Maintaining necessary documentation of handling of PHI, as required by HIPAA.
6. Accounting for disclosures of PHI as required by HIPAA.

The Chief Information Officer shall serve as the HIPAA Security Officer to ensure appropriate technical and administrative safeguards are in place as to the security of PHI. Responsibilities include ensuring the security of the University's information technology systems related to PHI and compliance with the University's Sensitive Data and Security Policy.

C. Use of PHI.

1. The health plan performs enrollment; changes in enrollment and payroll deductions; provides assistance in claims problem resolution and explanation of benefits issues; and assists in coordination of benefits with other providers. Some or all of these activities may require the use or transmission of PHI. Thus, all information related to these processes will be maintained in a manner to protect the privacy and security of PHI. Employees will not disclose PHI from these processes for employment-

related or other purposes, except as provided by administrative procedures approved by the Privacy Officer.

2. Disclosures that are permissible under HIPAA:
    a. disclosure of PHI to the individual to whom the PHI belongs;
    b. requests by providers for treatment or payment;
    c. requests related to health care plan operations;
    d. disclosures requested to be made to authorized parties by the individual PHI holder in writing;
    e. disclosures to government agencies for reporting or enforcement purposes; and/or
    f. disclosures to workers' compensation providers and those authorized by the workers' compensation providers.
3. Information regarding whether an individual is covered by a plan for claims processing purposes may be disclosed as necessary.
4. Information external to the health plan is not considered PHI if the information
    a. is being furnished for claims processing purposes involving workers' compensation or short- or long-term disability; and
    b. medical information received to verify Americans with Disabilities Act (ADA) or Family and Medical Leave Act (FMLA) status.
    c. health and medical information received by the Risk Management Office.

D. <u>Business Associates</u>. The University group health plan may disclose PHI to Business Associates of the plan with satisfactory assurances in writing that the business associate will use the PHI only for purposes of the services performed for the health plan and will safeguard the PHI from disclosure.

E. <u>Research</u>. A researcher who obtains PHI from a Covered Entity must comply with the Privacy Rule. The University hybrid entity and individual researchers may use and disclose PHI for research with individual authorization, or without authorization under limited circumstances provided by the Privacy Rule, such as with approval of an Institutional Review Board (IRB).

F. <u>Notice of Privacy Practices</u>. The University will provide health plan participants with a Notice of Privacy Practices at least every three (3) calendar years; post the notice in a conspicuous location; and make the Notice available to participants upon request.

G. <u>Enforcement</u>. The University will apply appropriate sanctions for staff, faculty or students who fail to comply with the University's HIPAA Policy and procedures.

H. <u>Records Retention</u>. HIPAA records and disclosures of PHI will be maintained for a period of six years as required by federal law. Records that have been

maintained for the maximum interval will be destroyed in a manner to ensure that such data are not compromised in the future.

VI. **CROSS REFERENCE**:

Sensitive Data and Security Policy

VII. **ATTACHMENTS**:

HIPAA Authorization Form