Niagara University HIPAA Privacy, Security & Breach Notification Policy

Protected Health Information (PHI) Privacy and Confidentiality Policy
Effective Date: Updated 4/2026
Responsible Offices: Niagara University Health Services / Office of Compliance / Human Resources/General Counsel

1. Purpose

Niagara University is committed to protecting the privacy, security, and integrity of health information in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), applicable federal regulations, and guidance from the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), Centers for Medicare & Medicaid Services (CMS), and the Centers for Disease Control and Prevention (CDC).

This policy establishes standards for the protection of Protected Health Information (PHI), Electronic Protected Health Information (ePHI), and breach response obligations for University departments or workforce members who perform HIPAA-covered functions.

2. Scope

This policy applies to:

- University Health Services
- Counseling or wellness units that may qualify as covered components
- Human Resources when administering health plans
- Employees, faculty, students, volunteers, trainees, contractors, and business associates who access PHI
- Any University department designated as part of a HIPAA-covered or hybrid entity function

3. Definitions

Protected Health Information (PHI)

PHI means individually identifiable health information in any form—electronic, paper, or verbal—that relates to:

- Past, present, or future physical or mental health condition
- Provision of health care
- Past, present, or future payment for health care

- Personal identifiers such as name, address, date of birth, Social Security number, or similar identifying data

Electronic Protected Health Information (ePHI)

PHI that is created, stored, received, transmitted, or maintained electronically.

Covered Entity

A health plan, health care clearinghouse, or health care provider conducting certain health care transactions electronically.

Business Associate

A person or organization performing services involving PHI on behalf of Niagara University.

4. Privacy Principles

Niagara University shall:

1. Protect the confidentiality, integrity, and availability of PHI and ePHI.
2. Use or disclose PHI only as permitted or required by law.
3. Limit use and disclosure to the **minimum necessary** information needed.
4. Provide individuals with rights regarding their PHI.
5. Maintain safeguards to prevent unauthorized access, use, or disclosure.
6. Report breaches and security incidents as required.
7. Support lawful public health reporting consistent with CDC and HHS guidance.

5. Permitted Uses and Disclosures

PHI may be used or disclosed without written authorization when permitted by HIPAA, including:

A. Treatment, Payment, and Health Care Operations

- Coordination of care with physicians, hospitals, laboratories, pharmacies, or emergency responders
- Billing, claims, payment, and reimbursement activities
- Quality improvement, credentialing, auditing, compliance, and administrative functions

B. Communication with Other Providers

PHI may be shared by secure email, telephone, fax, or other communication methods when reasonable safeguards are used.

C. Incapacitated Individuals

If an individual is unable to agree or object, PHI may be disclosed when professional judgment determines it is in the individual's best interest.

D. Family Members and Others Involved in Care

Unless the individual objects, Niagara University may disclose relevant information to family members, friends, or others identified by the individual as involved in care or payment.

E. Public Health Activities

PHI may be disclosed to authorized agencies for:

- Disease reporting
- Immunization reporting
- Exposure notification when authorized by law
- Child abuse or neglect reporting
- Outbreak investigation and control

F. Research

PHI may be used or disclosed for research when all HIPAA and institutional approval requirements are met.

G. Required by Law

When disclosure is required by statute, court order, subpoena, or lawful authority.

6. Employment Records and Workplace Health Information

HIPAA generally governs how covered health care providers and health plans use or disclose PHI. HIPAA does **not** generally apply to Niagara University employment records, even if those records contain health-related information.

Examples of employment records may include:

- Sick leave documentation
- Fitness-for-duty records
- Workers' compensation files maintained by the employer
- Leave of absence records
- Workplace accommodation documentation

Employer Requests for Health Information

Niagara University, as an employer, may request health-related documentation from employees when necessary for legitimate employment purposes, including:

- Sick leave verification
- Family or medical leave administration
- Workers' compensation claims
- Workplace safety requirements
- Wellness program participation
- Health insurance enrollment or benefit administration

Requests to Health Care Providers

If Niagara University requests medical information directly from an employee's health care provider, the provider generally may not release PHI without the employee's valid written authorization unless disclosure is otherwise permitted or required by law.

Separation of Records

Employment records shall be maintained separately from medical treatment records whenever feasible and access shall be limited to authorized personnel with a legitimate business need.

7. Uses Requiring Authorization

Written authorization is required for uses or disclosures not otherwise permitted by HIPAA, including certain marketing, third-party disclosures, or non-routine uses.

Authorization may be revoked in writing unless already relied upon.

8. Minimum Necessary Standard

University workforce members shall use, request, or disclose only the minimum PHI necessary to accomplish the intended purpose, except where HIPAA exempts the standard (such as treatment disclosures).

9. Individual Rights

Individuals have the right to:

- Receive a Notice of Privacy Practices
- Examine and obtain a copy of their records, including an electronic copy when available
- Request corrections or amendments

- Request restrictions on disclosures, including restrictions on health plan disclosures for services paid in full out-of-pocket when applicable
- Request confidential communications by alternate means or locations
- Receive an accounting of certain disclosures
- File complaints without retaliation

10. Privacy Rule Administrative Requirements

Niagara University shall:

- Notify individuals of privacy rights and uses of information
- Maintain written privacy procedures
- Designate a Privacy Officer
- Train workforce members
- Apply sanctions for violations
- Secure records so they are not readily available to unauthorized persons

11. Security Rule Requirements (ePHI)

Niagara University shall implement reasonable and appropriate safeguards to protect ePHI.

Administrative Safeguards

- Risk analysis and risk management
- Workforce training and compliance monitoring
- Incident response procedures
- Periodic review of security measures

Physical Safeguards

- Controlled facility access
- Secure workstations and devices
- Locked storage for records and equipment

Technical Safeguards

- Unique user access controls
- Password protection
- Encryption where appropriate
- Secure transmission methods
- Audit logs and monitoring

12. Incidental Disclosures

Limited incidental disclosures may occur despite reasonable safeguards. Such disclosures are not violations when appropriate protections and minimum necessary standards are followed.

13. Breach Notification Rule

Any impermissible use or disclosure of unsecured PHI is presumed to be a breach unless a documented risk assessment demonstrates a low probability that the PHI was compromised.

Required Notifications

Niagara University shall provide notice without unreasonable delay and no later than **60 days** after discovery to:

- Affected individuals
- HHS, as required
- Media, when required by law

Business associates must notify Niagara University of breaches involving University PHI.

14. FERPA and Student Records

Certain student education records are governed by FERPA rather than HIPAA. The University shall determine applicable law based on the nature and purpose of the record.

15. Business Associates

All vendors or contractors with PHI access must execute a Business Associate Agreement requiring HIPAA-compliant safeguards, breach reporting, and permitted uses of information.

16. Workforce Responsibilities

All workforce members must:

- Complete required privacy and security training
- Protect passwords and devices
- Use only authorized access
- Immediately report suspected breaches or incidents
- Refrain from unauthorized access or “snooping”
- Follow secure communication practices

17. Retaliation Prohibited

Niagara University prohibits retaliation against any person who exercises HIPAA rights, files complaints, or reports concerns in good faith.

18. Sanctions

Violations may result in disciplinary action up to and including termination, dismissal, contract termination, civil penalties, or criminal referral.

19. Privacy Officer Contact

HIPAA Privacy Officer
Niagara University

Jeremy Colby
General Counsel's Office PO Box 2025

716-286-8391
jcolby@niagara.edu

20. Policy Review

This policy shall be reviewed periodically and revised as laws, regulations, technology, or University operations change.

Niagara University reserves the right to change the terms of its privacy practices notice and to make new notice provision effective for all protected health information that it maintains. Any revised notice will be available on the Health Services website.