Issuing Department: Internal Audit, Compliance, and Enterprise Risk Management

Effective/Reissue Date: 10/5/2016
Current Version: 4/1/2024

Breach Notification

Policy

NYU Langone Health will investigate all HIPAA and privacy related Incidents and provide timely notification as necessary and appropriate under federal and state laws to:

- affected individuals,
- the U.S. Department of Health and Human Services (Office for Civil Rights),
- media outlets,
- credit reporting agencies, and
- other federal or state agencies, including the New York State Office of Attorney General ("NYS AG") as required.

Procedure

1. NYU Langone Health Workforce Members must immediately report known or suspected Incidents to Internal Audit, Compliance, and Enterprise Risk Management ("IACERM").

2. IACERM will take immediate steps to investigate and contain the Incident and mitigate the risk of harm to affected individuals. IACERM may seek assistance from Medical Center Information Technology ("MCIT"), the Office of General Counsel, Security, Human Resources, the Office of Communications, impacted departments or units, and outside consultants as appropriate.

3. In the event the Incident involves possible criminal activity, such as identity theft or theft of valuable NYU Langone Health equipment or proprietary information, IACERM, MCIT, and/or the relevant NYU Langone Health Workforce Member will file a police report or other notification with the appropriate law enforcement division.

4. IACERM will determine whether the Incident qualifies as a Breach under applicable federal and/or state notification laws.
    - For purposes of HIPAA, an Incident is presumed to be a Breach and notification is necessary unless a low probability exists that Protected Health Information ("PHI") has been compromised as demonstrated through a risk assessment.
    - For purposes of New York State Breach notification laws, a security Incident qualifies as a Breach if there is unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information. A

risk assessment will be completed for all incidents in compliance with New York State law.

- Other states may have different definitions and requirements and any notification requirement will be evaluated by the Privacy Officer in conjunction with the Office of General Counsel.

5. Upon determination of a Breach, IACERM will take all reasonable measures to notify affected individuals. IACERM will notify federal and state agencies, credit reporting agencies, and other individuals as necessary and appropriate. Media outlets will be notified in coordination with the Office of Communications if required or deemed appropriate. All notifications will be made in accordance with regulatory requirements and without unreasonable delay.
    a. IACERM will engage third parties or vendors in accordance with all NYU Langone Health policies to assist, as needed, in the notification process, including providing credit monitoring services to affected individuals as required.
    b. Notification to the Office for Civil Rights for Breaches involving 500 or more affected individuals will be made without unreasonable delay but in no event more than 60 days after the date of discovery of the Breach.
    c. Notification to the Office for Civil Rights for Breaches involving fewer than 500 individuals will be made within 60 days after the end of the calendar year during which the Breach occurred.
    d. Notification to the NYS AG will be made within five business days of notification to the Office for Civil Rights for all cases reported to the Office of Civil Rights, regardless of whether the breach would have otherwise been reported under the New York State Breach notification laws.

6. IACERM will notify the Office of General Counsel and/or New York University Insurance Department so that any required notifications to insurance carriers can be promptly made.

7. All documentation concerning privacy incidents shall be retained for at least six (6) years by IACERM.

8. IACERM may take additional actions as necessary and appropriate to safeguard PHI and PII and to mitigate harm. This includes, but is not limited to:
    - providing identity theft protection services to affected individuals,
    - re-training and educating staff members,
    - implementing or recommending the implementation of controls to prevent further breaches, including technological solutions, and
    - recommending disciplinary action up to and including termination of employment or association with NYU Langone Health under guidance from Human Resources, the applicable department, and/or other applicable institutional policies.

9. As part of the required annual compliance training, all Workforce Members will be trained on how to recognize and report Incidents to IACERM. NYU Langone Health will not

retaliate against any person who, in good faith, reports a possible Incident, in accordance with NYU Langone Health policy.

Related Documents

Compliance Concerns: Reporting, Investigating, and Protection from Retaliation
Compliance Concerns: What You Need to Know About Reporting & the Investigation Process
HIPAA Privacy Policies, Procedures, and Documentation
HIPAA Privacy Policies and Procedures Definitions
IACERM Breach Notification Standard Operating Procedure
IACERM Risk Assessment Standard Operating Procedure

Legal Reference

45 C.F.R. Subpart D
N.Y. GEN. BUS. § 899-aa, bb, "SHIELD Act"
N.J. Stat. Ann§ 56:8-163-66
Conn. Gen. Stat. §36a-701b
73 Pa. Stat. Ann. §§ 2301-2308, 2329
Other state laws as applicable

This version supersedes all NYU Langone Health (as defined in this Policy) previous policies, including but not limited to NYU Hospitals Center, New York University School of Medicine, Lutheran Medical Center, and Winthrop University Hospital.