SUNY DOWNSTATE MEDICAL CENTER

UNIVERSITY HOSPITAL OF BROOKLYN
POLICY AND PROCEDURE

Subject:	**NOTIFICATION OF PROTECTED HEALTH INFORMATION (PHI) BREACHES**		**No. OCA-3**
			Page 1 of 4
Prepared by:	Alexandra Bliss	**Original Issue Date:**	06/10
Reviewed by:	Shoshana Milstein	**Supersedes:**	09/13
Committee Approved:	Compliance and Audit Oversight Committee	**Effective Date:**	12/16
		TJC standards:	IM.04.01.01, IM.02.01.03
Approved by:	William P. Walsh, MBA, MSW	**Standards:**	Health Information Technology for
	Patricia Winston, MS, RN		
	Margaret Jackson, MA, RN		Economic and Clinical Health Act, 45 CFR Parts160 and 164, NYS Technology Law section 208, NYS General Business Law section 899-aa.
	Michael Lucchesi, MD		
			Issued by: Regulatory Affairs

I. POLICY:

Title XIII of The American Recovery and Reinvestment Act of 2009 (ARRA) is the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH significantly impacts the Health Insurance Portability and Accountability (HIPAA) Privacy and Security Rules by creating an interim final rule which requires notification of certain breaches of unsecured Protected Health Information (PHI), specifically, PHI that has not been rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of specified technologies or methodologies.

The HIPAA Omnibus Rule revised the interim final rule under HITECH and created a final Breach Notification Rule. Effective September 23, 2013, DMC will comply with the final breach notification regulations as well as with already existing notification laws, including New York State's Information Security Breach and Notification Act of 2005.

II. DEFINITIONS

Breach: The acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI.

Breach excludes:

1. Good faith, unintentional acquisition, access or use of PHI by employees or workforce members of DMC or its business associates (if such acquisition, access or use was made in good faith, was within the scope of authority and does not result in a further unpermitted use or disclosure).

2. Inadvertent disclosures to another authorized person within DMC or DMC's organized healthcare arrangement (See HIPAA- 5, "Covered Entity Designation") and the information received as a result of such disclosure is not further used or disclosed in an unpermitted manner.

3. A disclosure of PHI where the recipient could not reasonably have retained the data.

4. The data disclosed is limited to a limited data set that does not include dates of birth or zip codes.

Discovery of Breach: A breach of PHI shall be treated as "discovered" as of the first day on which such breach is known to the organization, or by exercising reasonable diligence should have been known to the organization (and not when it is actually determined to constitute a breach).

Unsecured PHI: Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary.

III. PROCEDURE/GUIDELINES:

A. Breach Determination- An acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule which does not meet the exclusions listed in the breach definition under Section II is presumed to be a breach unless DMC or its business associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following four factors:

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

B. Breach Reporting

1. Reporting of possible breaches of PHI shall be done by all members of DMC's workforce, in accordance with DMC's *Compliance Program Manual*, Section D. Reporting System. DMC's workforce may report suspicions of potential breaches via the DMC Compliance Line available at (877) 349-SUNY (7869) or via the "Compliance Line" link at www.downstate.edu.

2. As per the *Business Associate Agreement* Policy (policy number HIPAA-3), business associates of DMC are responsible for reporting any use or disclosure of information not provided for in their contract or any security incident of which they become aware involving the PHI of DMC.

C. Remediation and Mitigation

If the investigation determines that PHI has been breached, the following will occur:

1. *The State University of New York's Breach Notification Risk Assessment Tool* will be utilized to conduct a risk assessment. This assessment will be performed with applicable parties as necessary, including, Counsel, Risk Management, Health Information Management and/or the Information Security Officer.

   If it cannot be determined that there is a low probability that the PHI has been compromised:

   a. Affected individual(s) will be notified, in writing, within sixty (60) days of the discovery of breach.

      i. DMC's *Notification Letter* shall be sent by first class mail to the last known address notifying the individual(s) of the incident, of actions taken to protect the individual(s) from misuse of the information, and actions taken by the organization to prevent or minimize future like occurrences.
      ii. If the incident involves more than five hundred (500) individuals, the Office of Compliance & Audit Services (OCAS) will coordinate with the Office of Institutional Advancement to notify applicable media outlets.
      iii. In the event that contact information is out of date or insufficient for ten (10) or more patients, substitute notification will be placed in geographic areas where the patients affected likely reside.
      iv. If applicable, Institutional Advancement will post information on DMC's website to serve as breach notification outreach as necessary.

   b. Notice shall be provided to the Secretary of Health and Human Services (HHS) as follows:

      i. For breaches involving five hundred (500) or more individuals, DMC shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.
      ii. For breaches involving less than five hundred (500) individuals, no later than sixty (60) days after the end of each calendar year, DMC will submit to the Secretary of HHS as instructed at www.hhs.gov.

   c. Notice shall be provided to the State University of New York's System Administration Director of Policy and Planning of all breaches within sixty (60) days of the end of the calendar year. In the event that no breaches have occurred, notice shall be sent to such effect.

2. Action will be initiated by the responsible parties involved to facilitate remediation of future occurrences of such violation or breach based on a root cause analysis of the contributing factors.

3. Sanctions will be applied as appropriate to workforce members violating privacy policies and procedures, in accordance with DMC policies and procedures and Compliance Program.

4. If a business associate commits the breach or violation and the business associate does not cooperate with remediation efforts, the contract may be terminated or the incident reported to the Secretary of the Department of Health and Human Services.

5. The Office of Compliance & Audit Services will retain documentation of all reports and actions taken for a period of six years. DMC's Compliance Line database will be updated with the details of breach occurrence as well as scanned copies of the completed Risk Assessment Tool and Notification Letter(s).

D. Maintenance of Breach Information/Log: As described above, DMC shall maintain a process to record/log all breaches of unsecured PHI regardless of the number of patients affected. The following information will be collected/logged on the Breach Notification Assessment Tool and entered in DMC's Compliance Line database:

1. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.

2. A description of the types of unsecured protected health information that were involved in the breach (such as full name, social security number, date of birth, home address, account number, etc.).

3. A description of the actions taken with regard to notification of patients regarding the breach.

4. Resolution steps taken to mitigate the breach and prevent future occurrences.

IV. ATTACHMENTS:

DMC's Breach Notification Risk Assessment Tool; DMC Patient Notification Letter Template.

V. REFERENCES

Section 13402 of the Health Information Technology for Economic and Clinical Health Act, 45 CFR Parts 160 and 164, NYS Technology Law section 208, NYS General Business Law section 899-aa.

Date Reviewed	Revision Required (Circle One)		Responsible Staff Name and Title
6/2010	(Yes)	No	Shoshana Milstein
9/2013	(Yes)	No	Shoshana Milstein
12/2016	Yes	(No)	Shoshana Milstein