Employee Benefits Division Policy Memorandum

Number: **Policy Memo #137**
Date Issued: **February 15, 2010**
Policy File Ref: **A1810**
Subject: **HIPAA Policies and Administrative Requirements**
Topic: **Breach Notification and Security**

PURPOSE:

To establish policies to ensure compliance by the Department of Civil Service and NYSHIP with requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the HITECH provisions of the American Recovery and Reinvestment Act (ARRA) of 2009.

These policies and procedures apply to all EBD workforce members and other staff designated as part of the EBD health care component. The EBD health care component includes staff of EBD, and other select Department staff, such as IRM, Counsel's Office, Internal Audit, the Public Information Office and the Executive Office, that have access to protected health information in performing functions for EBD.
This policy applies to EBD and NYSHIP in addition to the Department's Information Security Policy.

Breach - Definitions

Because NYSHIP is a group health plan that accesses, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses or discloses "unsecured" PHI, it is required to notify affected individuals when a "breach" occurs involving that information.

Secured PHI is PHI that is protected by using one of the encryption and destruction technologies / methodologies identified by DHHS for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals. Summary or de-identified information does not need to be secured.

Unsecured PHI is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by DHHS. Unsecured PHI can include information in any form or medium, including electronic, paper, or verbal form.

Breach is an acquisition, access, use or disclosure of unsecured PHI in a manner not permitted by HIPAA that compromises the security or privacy of the PHI. *For this purpose, PHI is "compromised" to the extent that the action poses a significant risk of financial, reputational, or other harm to the individual.*

Exceptions: No notice is required in the following circumstances, because the HITECH Act excludes these events from the definition of a breach:

No Ability to Retain – a breach does not occur when DCS/NYSHIP or its business associate has a good faith belief that an unauthorized person to whom the PHI is disclosed would not reasonably be able to retain the information.

Good Faith Disclosure – a breach does not occur when the unintentional acquisition, access, or use of the PHI by an employee or other person acting under the authority of DCS / NYSHIP (or a business associate), provided the acquisition, access or use occurred in good faith, within the scope of the individual's employment or other professional relationship; and did not result in further use or disclosure in a manner not permitted under HIPAA.

Inadvertent disclosures. A breach does not occur when the PHI was disclosed inadvertently by an individual otherwise authorized to access the PHI to a similarly situated person, if the information is not further used or disclosed by the similarly situated person in a manner prohibited under HIPAA by the similarly situated person.

Procedure: If staff suspects or is advised by a vendor, enrollee, business associate, or other person that it appears there has been a breach of PHI, whether secured or unsecured, staff is required to report the incident to the Supervisor of Policy Analysis & Strategic Planning Unit. The Policy Unit will determine the status of the alleged breach and will consult with the Director regarding the Division's response.

Breach Notification

Following discovery of a breach of unsecured PHI, DCS/NYSHIP is required to notify each individual whose unsecured PHI has been or is reasonably believed by DCS/NYSHIP to have been accessed, acquired, used, or disclosed because of having been breached.

A breach is "discovered" as of the first day on which the breach is known by DCS/NYSHIP to have occurred, or would have been known to have occurred given the exercise of reasonable diligence.

Notice is required to be provided without unreasonable delay, and in no case later than 60 calendar days after discovery of the breach. The 60-day period may be extended on an exceptional basis, such as at the request of law enforcement.

Procedure: As the NYSHIP Privacy Official, the Director is responsible for ensuring that notification is made timely and appropriately. The Director shall delegate the handling of a specific incident to an Assistant Director as appropriate under the specific circumstances. The Supervisor of Policy Analysis & Strategic Planning shall advise and provide subject matter expertise as needed in addition to reviewing and approving the content and method of notice as set forth below.

Content of Notice

The notice must be written in plain language and should include the following, to the extent possible:

a brief description of what happened, including the date of the breach and the date of its discovery;

a description of the types of unsecured PHI involved in the breach, such as full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information;

any steps individuals should take to protect themselves from potential harm resulting from the breach;

a brief description of what DCS/NYSHIP is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches;

contact information to enable individuals to ask questions or obtain additional information (toll-free phone number, e-mail address, web site, mailing address).

The notice should not disclose the actual PHI that was breached, as the notice may be read by persons other than the individual whose PHI was the subject of the breach.

Method of Notice

The method of notice depends upon the circumstances.

<u>Individual Notification</u>:

Written notice by First Class Mail – this is the primary form of individual notification, sent to the individual at his/her last known address. Notice may be sent by electronic mail if the individual has consented to electronic notice and has not withdrawn his/her consent.

Substitute Notice – a substitute form of notice reasonably calculated to reach the individual may be provided when there is insufficient or out-of-date contact information that precludes written notification to the individual. If 10 or more such individuals are affected, a conspicuous notice must be posted on the DCS/NYSHIP website home page for a period of time determined by DHHS. Alternatively, notice may be published in major print or broadcast media where the affected individuals likely reside. Any such media or website postings must include a toll-free phone number where the individual can learn whether his/her PHI may be included in the breach.

Urgent Notice – If DCS/NYSHIP determines that the situation requires urgency because of the possible imminent misuse of unsecured PHI, DCS/NYSHIP may provide notification to individuals by telephone or other means, as appropriate, in addition to providing written notice.

Notification to the Media:

In addition to Individual Notification, notice must be provided to prominent media outlets if the breach of unsecured PHI involves more than 500 residents of a State or jurisdiction. Notification shall be made to prominent media outlets serving the State or jurisdiction wherein the affected individuals reside, and must be provided without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. Notification to the media may be provided in the form of a press release.

Notification to DHHS:

Breaches involving 500 or more individuals – DCS/NYSHIP is required to notify DHHS immediately. DHHS provides instructions for providing such notice on its web site. DHHS will post on its website a list of covered entities that have submitted reports of breaches of unsecured PHI involving more than 500 individuals.

Breaches involving fewer than 500 individuals - DCS/NYSHIP shall maintain a log that documents the breaches and submit the log to DHHS within 60 days after the end of the calendar year (March 1).

Breach by Business Associate

DCS/NYSHIP is required to ensure that its HIPAA Business Associates ("BA") are aware of their responsibility to comply with HIPAA Privacy and Security requirements consistent with 45 CFR Parts 160 through 164. The BA Agreement shall address the following concerns:

Discovery of Breach:

A BA is required to notify DCS/NYSHIP immediately of any potential or actual breach of unsecured PHI of which the BA becomes aware. The BA is required to provide any additional information when it becomes available, without unreasonable delay and within 60 days of the date the breach is discovered.

A breach is treated as discovered by the BA as of the first day on which the breach is known to the BA or should have been known by the BA through the exercise of reasonable diligence.

The BA shall be subject to consequences for failure to provide timely notification.

The BA must provide DCS/NYSHIP with the identify of each individual whose unsecured PHI has been, or is reasonably believed to have been breached.

The BA must provide the any information necessary to enable NYSHIP to send out breach notifications, to make web site postings, and to maintain a log of breaches that have been identified, as well as any other information DCS deems necessary to comply with HIPAA requirements.

The BA is required to have adequate policies and procedures, and to provide adequate training for its employees, for identifying breaches of unsecured PHI, and for notifying DCS/NYSHIP on a timely basis.

Notice of Breach:

The BA's discovery of a breach is imputed to DCS/NYSHIP if the BA is acting as DCS/NYSHIP's agent; in such cases, DCS/NYSHIP is required to provide notification of a breach based upon the date that the BA discovers (or should have discovered) the breach.

If the BA is not an agent of DCS/NYSHIP and instead is an independent contractor, DCS/NYSHIP shall provide notification based on the date the BA notifies DCS/NYSHIP of the breach.

However, DCS/NYSHIP retains the option of having the BA notify affected individuals of a breach. DCS/NYSHIP will retain responsibility to notify media outlets and DHHS as required.

Other HITECH Requirements:

The BA must agree to comply with restrictions on marketing and sales of records.

The BA shall not receive any remuneration related to its receipt or use of PHI except as specifically provided in BA agreement.

The BA must limit its access, use and disclosure of PHI to "limited data sets" or "minimum necessary" information.

The BA shall comply with HIPAA requirements generally applicable to NYSHIP.