DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

CMS CENTERS for MEDICARE & MEDICAID SERVICES

**CENTER FOR MEDICARE**

Date: September 28, 2010

To: Medicare Advantage Organizations
Medicare Prescription Drug Plan (PDP) Sponsors
Cost-Based Contractors
Employer/Union Sponsored Group Health Plans

From: Timothy Hill
Deputy Center Director

Re: Update on Security and Privacy Breach Reporting Procedures

This memorandum replaces in its entirety our December 16, 2008 Health Plan Management System (HPMS) memorandum ("Security and Privacy Reminders and Clarification of Reporting Procedures") and updates requirements and procedures for reporting security and privacy breaches to the Department of Health and Human Services (HHS) and the Centers for Medicare and Medicaid Services (CMS).

## Reporting Incidents to HHS/CMS

Interim final breach notification regulations (45 C.F.R. Part 64, subpart D), issued in August 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act by requiring Health Insurance Portability and Accountability Act (HIPAA) covered entities and their business associates to provide notification following a breach of unsecured protected health information (PHI). Following the discovery of a breach of unsecured PHI, HIPAA covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, the media.

In previous guidance, CMS indicated that organizations were required to report privacy and security breaches to CMS' IT Service Desk. This will no longer be required. Instead, organizations should follow the directions provided by HHS' Office for Civil Rights (OCR) related to these new HITECH breach notification regulations. Additional information, including a description of breach notification requirements, instructions for covered entities to submit breach notifications to the Secretary, and links to the online breach notification forms, can be found at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule.

As of the issue date of this memorandum, CMS will require that organizations provide concurrent notification of any breach notifications submitted to the Secretary to your Regional Office Account Manager. The notification to your Account Manager must include the same information that was submitted in the electronic submission to the Secretary. Additionally, organizations must *immediately* report (i.e., not wait until the mandatory reporting date to the

Secretary) any breaches to their CMS Account Manager if there is the potential for significant beneficiary harm (i.e., a high likelihood that the information was used inappropriately) or situations that may have heightened public or media scrutiny (i.e. a higher number of beneficiaries affected or particularly egregious breaches). CMS expects organizations to report to their Account Manager within 2 business days of learning of breaches that fall into these categories. In cases where your organization has notified OCR of the breach within this timeframe, your organization can send a copy of the breach report to your CMS Account Manager. Otherwise, your organization should send as much detail as possible to your Account Manager via email, including a description of the breach and the number of beneficiaries impacted.

CMS strongly encourages each organization to take immediate remedial steps to protect Medicare beneficiaries when breaches occur and to report those actions to your CMS Account Manager. CMS may direct you to take additional actions, if you do not do so voluntarily, and those actions are in the best interest of protecting Medicare beneficiaries. For example, Regional Office Account Managers may request that your organization send a letter to affected beneficiaries notifying them of the breach and their available rights, and/or provide impacted beneficiaries credit protection services. If the breach involved Social Security numbers, Health Insurance Claim numbers, or credit card numbers, your Account Manager may require that your organization offer free credit protection services to affected beneficiaries for one year.

While OCR is responsible for enforcing the HIPAA Privacy, Security and Breach Notification rules, CMS has the authority and responsibility to ensure that organizations remain compliant with all contractual requirements including ensuring compliance with all federal regulations and sub-regulatory guidance. Under this authority, CMS will continue to take compliance and/or enforcement actions in instances where CMS believes that organizations have not taken appropriate measures to safeguard the security and privacy of their Medicare members' health information.

## Protection of Beneficiary Information

CMS continues to receive reports of organizations with serious and/or repeat instances of non-compliance with Medicare program requirements relating to protecting the confidentiality of member information pursuant to 42 CFR 422.118, and section 10.8 of chapter 4 of the Medicare Managed Care Manual.

Therefore, CMS wishes to reinforce some of the necessary measures that organizations should take to protect the security and privacy of personally identifiable information (PII), including:

- Ensure that data files are not saved on public or private computers while accessing corporate e-mail through the Internet;
- Ensure that electronic systems for beneficiary mailings are properly programmed in order to prevent documents containing PII from being sent to the wrong beneficiaries.
- Ensure that PII data on all portable devices are encrypted.
- Implement security measures to restrict access to PII based on an individual's need to access the data.
- Perform an internal risk assessment or engage an industry-recognized security expert to conduct an external risk assessment of the organization to identify and address security vulnerabilities.

- Quickly remedy weaknesses or gaps in your security program.
- Train staff on the responsibilities and consequences of failing to secure sensitive beneficiary information.
- Document compliance with HIPAA Security and Privacy rules and keep current in response to environmental or operational changes affecting the security of the electronic PHI.
- Ensure the permanent removal of protected health information from electronic media or hard disks, whether they are on fax, copier, or computer, prior to disposal or before the media are made available for re-use.

As a measure to prevent security breaches, plans should also ensure that all first tier, downstream and related entities are aware of their responsibility to protect beneficiary data and report suspected breaches. You should also remind agents and brokers of their responsibility to protect beneficiary information. CMS has the authority to take compliance actions against contracted organizations regardless of whether the breach was caused by the organization itself or first tier, downstream, and other related entities.

Organizations that work with offshore subcontractors (first tier, downstream and related entities) to perform Medicare-related work that uses beneficiary PHI are requested to provide CMS with specific offshore subcontractor information. Additionally, organizations are required to complete an attestation regarding beneficiary PHI protection, per the requirements described in CMS' August 26, 2008 HPMS Memorandum.

If you have any questions about this memorandum, please contact your Regional Office Account Manager.