701 Pennsylvania Ave. N.W., Suite 700
Washington, D.C. 20004-2694
(202) 737-5980 • (202) 478-5113 (fax)

dmaa@dmaa.org • www.dmaa.org

May 21, 2009

The Honorable Kathleen Sebelius
Secretary
U.S. Department of Health and Human Services
Office for Civil Rights
200 Independence Avenue, SW
Washington, DC 20201

ATTN: HITECH Breach Notification

Submitted via regulations.gov

RE: Guidance specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information.

Dear Secretary Sebelius:

DMAA: The Care Continuum Alliance respectfully submits this response to the Department of Health and Human Services Guidance and Request for Information on Security for Protected Health Information published April 17, 2009.

DMAA represents more than 200 corporate and individual stakeholders promoting wellness and health promotion, managing chronic care and coordinating complex care. DMAA members include wellness, disease and care management organizations, pharmaceutical manufacturers and benefits managers, health information technology innovators, biotechnology innovators, employers, physicians, nurses and other health care professionals, and researchers and academicians.

DMAA supports efforts to protect the integrity of personal health information (PHI) in concert with the protection of the availability of information for treatment, payment, chronic care coordination, and care management and we appreciate the opportunity to assist the Department in the development of these regulations.

DMAA is concerned with the prospect of regulatory requirements from both HHS and the Federal Trade Commission applying to subcontractors of business associates. Under the proposed rule, entities offering PHRs as subcontractors to business associates will be subject to both HIPAA and FTC regulation, unless the issue is better addressed in the Final Rule.

Section 13402 of the HITECH Act provides that HIPAA covered entities and their business associates are responsible for implementing the data breach notification provisions. That

section clearly identifies HHS as the agency with jurisdiction for implementing the statutory requirements and regulating covered entities and business associates. While not specifically addressed in the statute, DMAA believes that future data breach regulations should explain that business associates are required to cause their agents and subcontractors to notify the business associate in the event of a data breach to enable the business associate to satisfy its regulatory obligations. As required by the statute, the business associate will then be responsible for notifying the covered entity. The regulations also should clarify that such business associates' agents and subcontractors would not be subject to FTC jurisdiction in order to avoid any potential overlapping or inconsistent regulatory requirements.

Existing HIPAA regulations require covered entities to have written agreements in place with every business associate. (45 C.F.R. §164.504(e).) Further, business associate are required to ensure that subcontractors to whom it provides protected health information agrees to the same restrictions and conditions applicable to the associate. (45 C.F.R. §164.504(e)(2)(ii)(D).) These contractual requirements (i.e., in the agreement between a covered entity and a business associate and in the agreement between a business associate and any agent or subcontractor) include that the business associate, and any agent or subcontractor, notify the covered entity about any disclosure of protected health information not allowed for by the written agreement.

This existing process and contractual requirements are reasonable and workable for providing notice back to the covered entity if a data breach occurs, particularly given the various relationships that exist between entities. In the event that a data breach occurs, including an obligation for the business associate's agents and subcontractors to notify the business associate in future HHS regulations will allow individual consumers to be promptly and accurately notified by the covered entity, which is likely the primary entity with which individuals have established a direct relationship.

DMAA urges HHS to clarify in future regulations that any agent or subcontractor of a HIPAA business associate will be expected to notify the business associate in the event of a data breach and will not be subject to FTC jurisdiction.

DMAA appreciates this opportunity to provide comment to the Department in the development of workable rules and guidance on these issues.

Sincerely,

Tracey Moorhead
President and CEO