OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
WASHINGTON, DC 20301-1200

HEALTH AFFAIRS

APR 28 2010

MEMORANDUM FOR ASSISTANT SECRETARY OF THE ARMY (M&RA)
ASSISTANT SECRETARY OF THE NAVY (M&RA)
ASSISTANT SECRETARY OF THE AIR FORCE (M&RA)

SUBJECT: Reporting a Breach as Defined by the Health Information Technology for Economic and Clinical Health Act Provisions of the American Recovery and Reinvestment Act of 2009

The Military Health System (MHS) is entrusted with securing and safeguarding the Personally Identifiable Information and Protected Health Information (PHI) of our beneficiaries. In addition to the requirements outlined in Department of Defense (DoD) 5400.11-R, "Department of Defense Privacy Program," responsibility for breach notification and reporting has been expanded with the recent passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

The HITECH Act requires that amendments be made to Health Insurance Portability Accountability Act Privacy and Security rules and establishes new individual notification and government reporting requirements when a "breach" of "unsecured Protected Health Information (PHI)" occurs. A "breach" as defined by the Department of Health and Human Services (HHS) differs from the broader definition established by DoD policy. HHS issued guidance in August 2009 for these new requirements in an Interim Final Rule on Breach Notification for Unsecured Protected Health Information ("HHS Breach Rule"). This new interim rule includes requirements to provide notification to individuals affected by breaches and to report breaches of unsecured PHI to HHS. It should be noted that amendments to various requirements may be implemented when the final rule is published. These provisions apply equally to MHS Components including business associates of MHS covered entities.

In order to ensure compliance with these new requirements, breaches that occur within MHS must continue to be reported to the TRICARE Management Activity (TMA) Privacy Office within 24 hours of discovery in accordance with the September 24, 2007, Assistant Secretary of Defense (Health Affairs) Memorandum, "Breach Notification Reporting for the Military Health System." The TMA Privacy Office will determine if the incident qualifies as a breach under the provisions of the HHS Breach Rule and will subsequently report the incident directly to the Secretary, HHS, as appropriate. In such instances where reporting to HHS is required, the TMA Privacy Office will provide courtesy notification to the MHS Component.

Additionally, to the extent required by the terms of the contract, business associates of a MHS-covered entity that discover a breach shall continue to notify the MHS Component immediately in accordance with DoD 5400.11-R, C1.5.1.3. The MHS Component will then report the breach to the TMA Privacy Office, which will make the determination of whether further reporting to HHS is necessary, as outlined above.

More detailed information on breach reporting requirements can be found on the TMA Privacy Web site (www.tricare.mil/tmaprivacy/breach.cfm) and the HHS Web site (www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html). All actual or potential breaches and associated questions regarding the breach notification and response requirements set forth by the HHS Breach Rule should be sent to the TMA Privacy Office via e-mail at PrivacyOfficerMail@tma.osd.mil.

[Signed]

Charles L. Rice, M.D.
President, Uniformed Services University of the Health Sciences
Performing the Duties of the Assistant Secretary of Defense (Health Affairs)

cc:
Surgeon General of the Air Force
Surgeon General of the Army
Surgeon General of the Navy
Deputy Director, TMA