AMERICAN RECOVERY AND REINVESTMENT ACT (ARRA) OF 2009

SUMMARY OF HEALTH PRIVACY/SECURITY PROVISIONS

HIPAA Privacy & Security ♦ April 2010

TMA Privacy Office Information Paper

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Privacy Act/System of Records ♦ PIAs

PURPOSE

This paper outlines provisions of the recent economic stimulus legislation—the American Recovery and Reinvestment Act of 2009 (ARRA), enacted on February 17, 2009—that are relevant to the Military Health System (MHS). Because ARRA expands the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and provides for stricter penalties and enforcement, the need to understand the Privacy and Security Rules has increased importance.

BACKGROUND

ARRA contains numerous provisions relating to health information technology (HIT). The HIT provisions of ARRA are referred to collectively as the "Health Information Technology for Economic and Clinical Health Act" or "HITECH." Some HITECH Act provisions specifically relate to privacy and security issues. These provisions amend HIPAA and corresponding regulations. In particular, the HITECH Act clarifies that criminal penalties for HIPAA violations apply to individuals as well as covered entities, and it extends enforcement authority to state attorneys general. Other HITECH Act provisions establish financial incentives for health care providers to adopt electronic health records (EHRs). The Department of Health and Human Services (HHS) is required to develop standards (including privacy and security) for certification and "meaningful use" of EHRs. Although EHR financial incentives are not directly relevant to the MHS, EHR standards are relevant to the development of the MHS EHR systems in compliance with HIPAA.

The general effective date of the privacy/security provisions was one year after ARRA's enactment, i.e., February 17, 2010. Some provisions, however, are effective at earlier or later dates. A timeline of effective dates and regulatory guidance is located at the end of this document. Regulations and other guidance has been issued, and more will be issued, by the HHS Office of Civil Rights (OCR), the Office of the National Coordinator (ONC) for HIT, and newly established federal advisory committees (the HIT Policy and Standards Committees).

PRIVACY AND SECURITY AREAS AFFECTED

Breach Notification. The HITECH Act contains a new requirement that HIPAA-covered entities notify individuals after a "breach" of their "unsecured" protected health information (PHI), but only if privacy or security is compromised. If more than 500 individuals of the same state

AMERICAN RECOVERY AND REINVESTMENT ACT (ARRA) OF 2009

SUMMARY OF HEALTH PRIVACY/SECURITY PROVISIONS

or jurisdiction are affected, notice in the media is required, and HHS must be informed "immediately." These new requirements took effect September 23, 2009, after issuance of an HHS interim final rule. Several points are important to note:

- HIPAA "Breach" is defined as the acquisition, access, use, or disclosure of PHI in a manner that is not permitted by the HIPAA Privacy Rule, and which compromises PHI privacy or security. "Compromised" means that the breach poses significant risk of financial, reputational or other harm to the affected individual(s). The definition of breach excludes certain unintentional uses or disclosures involving authorized personnel and situations where an unauthorized person would not have been able to retain the PHI.

- The notification requirements apply only with respect to "unsecured" PHI, that is, PHI not encrypted or destroyed in accordance with HHS guidance. That guidance is included with the interim final rule and is updated annually.

- Notification must be provided to affected individuals "without unreasonable delay" and in no case later than 60 days after initial discovery of the incident. Reporting to HHS is also required. The TMA Privacy Office will advise the MHS covered entity as to notifying affected individuals, and will report the breach to HHS on behalf of the covered entity.

HIPAA Standards and Individual Rights. The HIPAA "minimum necessary" standard will be clarified by HHS guidance due in August 2010. In addition, the HITECH Act details several changes to the individual rights provisions outlined in the HIPAA Privacy Rule:

- **Restrictions** - Upon request by an individual, a covered entity must restrict certain disclosures of PHI pertaining to care for which the individual pays in full without coverage by a third party such as TRICARE.

- **Accounting for Disclosures** - HITECH eliminates an exception to the HIPAA accounting requirement for disclosures made for treatment, payment or health care operations purposes through electronic health records (EHRs). The effect of this change is that MHS beneficiaries will be entitled, upon request, to receive an accounting of most PHI disclosures

AMERICAN RECOVERY AND REINVESTMENT ACT (ARRA) OF 2009

SUMMARY OF HEALTH PRIVACY/SECURITY PROVISIONS

by their medical providers and TRICARE (including managed care support contractors) where those disclosures are made through EHRs. This change does not take effect until 2011 or later, depending on when the EHR system is first put into place.

- **Access** - HITECH requires that individual access to PHI must be provided in electronic form when the information is maintained in an EHR.

Business Associates.

- HITECH makes certain requirements of the HIPAA Privacy and Security Rules and associated penalties applicable to business associates in the same manner as they apply to a covered entity. HHS is expected to issue guidance on amending business associate contracts.
- HITECH makes business associates subject to the EHR accounting requirement noted above.
- HITECH specifies that business associate status applies to certain entities that provide PHI data transmission services, including e-prescribing gateways and health information exchange organizations, and personal health record (PHR) vendors that contract with covered entities.

Separately from the HITECH provisions, ARRA requires Federal agency contracts with health care providers, health plans and health insurance issuers to require those entities to use HIT that satisfies standards and implementation specifications issued under HITECH.

Timeline of Effective Dates and Regulatory Guidance

2/17/09	ARRA enacted; increased civil penalty amounts took effect.
9/23/09-9/24/09	HHS/OCR breach notification regulations took effect (parallel regulations for PHR vendors issued by the Federal Trade Commission also took effect).
11/30/09	HHS/OCR interim final regulations on HIPAA enforcement took effect.
1/13/10	HHS/ONC published interim final rule on EHR standards,

AMERICAN RECOVERY AND REINVESTMENT ACT (ARRA) OF 2009

SUMMARY OF HEALTH PRIVACY/SECURITY PROVISIONS

	implementation specifications and certification, including provisions on disclosure accounting and restrictions; HHS/ Centers for Medicare and Medicaid Services published proposed rule on Medicare and Medicaid EHR Incentive Program.
2/17/10	Effective date of ARRA/HITECH privacy and security provisions for which no other effective date is specified.
2/22/10	Enforcement of sanctions under breach notification regulations begins.
3/10/10	HHS issued proposed rule on certification programs for HIT.
6/30/10	HHS to issue regulations on disclosure accounting.
8/17/10	HHS to issue regulations on (1) minimum necessary requirement. (2) restricting remuneration for PHI, and (3) enforcement.
1/01/11	Effective date of accounting requirement for disclosures of EHR information for treatment, payment and health care operations purposes for entities that acquire EHRs after 1/01/09 (HHS may extend this date to no later than 2013).
2/17/11	Effective date of penalties for willful neglect. Effective date of restrictions on remuneration for PHI.
2/17/12	HHS to issue regulations as to when individuals may receive portion of civil penalty.
1/01/14	EHR accounting requirement takes effect for entities with EHR as of 1/01/09 (HHS may extend this date to no later than 2016).
2/17/14	GAO report on effect of HITECH Act on health costs, EHR adoption, quality improvement.