



TMA Privacy Office Guidance

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



AMERICAN RECOVERY AND REINVESTMENT ACT (ARRA) OF 2009

PRELIMINARY OUTLINE OF HEALTH PRIVACY/SECURITY PROVISIONS

HIPAA Privacy & Security ♦ September 2009

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 provides for increased penalties and enforcement under the privacy requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 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 the “HITECH Act.” Some provisions of the HITECH Act specifically relate to privacy issues. These provisions amend HIPAA and corresponding regulations, the HIPAA Privacy and Security Rules. In particular, ARRA increases penalties for HIPAA violations and extends enforcement authority to state attorneys general.

The general effective date of the privacy-related provisions is one year after ARRA’s enactment, i.e., February 17, 2010. Some provisions, however, are effective at earlier or later dates. Regulatory and other guidance will be forthcoming at various times from the Department of Health and Human Services (HHS) Office of Civil Rights (OCR), the Office of the National Coordinator for Health Information Technology (ONCHIT or National Coordinator), newly established federal advisory committees (the HIT Policy and Standards Committees) and other federal entities. Until that guidance is issued, the effect of ARRA on the MHS will be unclear in many respects.

PRIVACY AREAS AFFECTED

Breach Notification. ARRA contains a new requirement that HIPAA-covered entities notify individuals no later than 60 days after a “breach” of their “unsecured” protected health information (PHI), but only if the covered entity reasonably believes that the PHI was accessed, acquired or disclosed as a result of the breach. If more than 500 individuals are affected, notice in the media is required, and HHS must be informed “immediately.” Several points are important to note:

- On August 24, 2009 HHS published in the Federal Register interim final regulations on the breach notification requirement. The notification requirement takes effect for breaches occurring at least 30 days after this

PrivacyMail@tma.osd.mil ♦ www.tricare.mil/tmaprivacy



TMA Privacy Office Guidance

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



AMERICAN RECOVERY AND REINVESTMENT ACT (ARRA) OF 2009

PRELIMINARY OUTLINE OF HEALTH PRIVACY/SECURITY PROVISIONS

HIPAA Privacy & Security ♦ September 2009

publication, but HHS will exercise its enforcement discretion to not impose sanctions for failure to provide the required notifications with respect to breaches discovered during the 180 day period after publication.

- “Breach” means the acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule if security or privacy is compromised. If this occurrence is unintentional, then it is excluded from the definition of breach in certain circumstances. The HHS regulations provide that the security and privacy of PHI is not compromised, and thus that no breach occurs, if there is no significant risk of financial, reputational or other harm to the affected individual.
- The notification requirements apply only with respect to “unsecured” PHI, that is, PHI not encrypted or destroyed in accordance with HHS guidance. HHS issued guidance for this purpose in April and included updated guidance with the publication of the interim final regulations.
- Similar breach notification requirements apply to personal health record (PHR) vendors and to entities offering products or services through those vendors’ Web sites. These parties were not previously subject to HIPAA. The Federal Trade Commission (FTC), which has enforcement authority for PHRs, published interim final regulations in conjunction with the HHS regulations. The FTC regulations do not apply to HIPAA covered entities (such as TRICARE) that provide PHRs to their beneficiaries.

HIPAA Standards and Individual Rights. By August 2010, HHS must issue guidance on the “minimum necessary” requirement of HIPAA, taking into account new guidance to be issued on de-identification (due by February 17, 2010) and the information needed to improve patient outcomes and the care of chronic disease. ARRA makes several changes to the individual rights provisions in the HIPAA Privacy Rule:

- Upon request by an individual, a covered entity must restrict disclosure of PHI pertaining to care for which the individual pays out-of-pocket in full.
- HIPAA currently does not require an accounting of information disclosed for treatment, payment or health care operations purposes. ARRA, however, adds a requirement for accounting when a covered entity maintains this information as part of an electronic health record (EHR). HHS must issue technology standards for EHR accounting by December 31, 2009, and six months thereafter must issue guidance on the information

PrivacyMail@tma.osd.mil ♦ www.tricare.mil/tmaprivacy



TMA Privacy Office Guidance

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



AMERICAN RECOVERY AND REINVESTMENT ACT (ARRA) OF 2009

PRELIMINARY OUTLINE OF HEALTH PRIVACY/SECURITY PROVISIONS

HIPAA Privacy & Security ♦ September 2009

required for accounting purposes.

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

Contract Language. Various ARRA requirements may need to be reflected in MHS language. For example:

- ARRA makes certain requirements of the HIPAA Security Rule and associated penalties applicable to business associates in the same manner as they apply to a covered entity. (The applicable requirements are administrative/physical/technical safeguards and a business associate contract or memorandum of understanding (MOU) with business associates.) HHS is to issue annual guidance on technical safeguards. It is not yet clear when MHS contracts or MOUs may need to be revised to reflect these changes.
- ARRA makes business associates subject to the EHR accounting requirement noted above. In addition, business associates may not receive remuneration for PHI, subject to various exceptions (regulations in this regard are due by August 17, 2010). ARRA also adds restrictions on permitted marketing communications.
- Business associate contracts are specifically required for certain entities that provide data transmission services, including e-prescribing gateways.

Separately from the privacy provisions, ARRA requires federal agencies to provide in contracts with health care providers, health plans and health insurance issuers that those entities use HIT that satisfies standards and implementation specifications issued under ARRA.

Communications and Training. Various MHS Web sites and training materials may need updating to reflect some of the above changes. In particular, materials relating to breach notification requirements may need revision. The new breach notification requirements, once in force, will be triggered as soon as any employee or agent of the covered entity or its business associate knew or should have known of the breach. Thus MHS personnel need to be aware of the importance of informing their superiors about the occurrence of possible breaches.

In addition, by February 17, 2010, OCR is required to maintain a “multi-faceted

PrivacyMail@tma.osd.mil ♦ www.tricare.mil/tmaprivacy



TMA Privacy Office Guidance

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



AMERICAN RECOVERY AND REINVESTMENT ACT (ARRA) OF 2009

PRELIMINARY OUTLINE OF HEALTH PRIVACY/SECURITY PROVISIONS

HIPAA Privacy & Security ♦ September 2009

national education initiative” on the potential uses of PHI and individual rights, which may establish additional training requirements for the MHS.

Timeline of Effective Dates and Regulatory Guidance.

- 2/17/09 ARRA enacted; increased civil penalty amounts take effect.
- 4/17/09 HHS issued guidance relating to "unsecured" PHI.
- 5/18/09 HIT Standards Committee issued schedule for assessing recommendations developed by HIT Policy Committee.
- 8/24/09-8/25/09 HHS and FTC published interim final regulations on breach notification.
- 9/23/09 HHS breach notification requirements take effect.
- 12/31/09 HIT Policy Committee is to make recommendations, and HHS is to issue interim final regulations, on (1) technologies that protect privacy and security in electronic health records (EHRs), including segmentation of sensitive health information; (2) technologies that allow for accounting of EHR information disclosures; (3) encryption technologies for individually identifiable health information.
- 2/17/10 Most HIPAA changes take effect.
HHS to issue guidance on de-identification.
HHS first annual report to Congress on privacy complaints, enforcement.
GAO report to HHS on penalty payments to individuals.
HHS/FTC report on privacy/security for non-HIPAA covered entities.
- 2/22/10 Enforcement of sanctions under breach notification regulations begins.
- 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 by three years).

PrivacyMail@tma.osd.mil ♦ www.tricare.mil/tmaprivacy



TMA Privacy Office Guidance

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



AMERICAN RECOVERY AND REINVESTMENT ACT (ARRA) OF 2009

PRELIMINARY OUTLINE OF HEALTH PRIVACY/SECURITY PROVISIONS

HIPAA Privacy & Security ♦ September 2009

- | | |
|---------|---|
| 2/17/11 | Enforcement regulations take effect.
Restrictions on remuneration for PHI take effect. |
| 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 as of 1/01/09 (HHS may extend this date by two years). |
| 2/17/14 | GAO report on effect of HITECH Act on health costs, EHR adoption, quality improvement. |

PrivacyMail@tma.osd.mil ♦ www.tricare.mil/tmaprivacy

TMA Privacy Office 5111 Leesburg Pike, Suite 810 Falls Church, VA 22041