American Recovery and Reinvestment Act (ARRA) of 2009 and HITECH Amendments Summary of Privacy Provisions

May 2022

I. Supporting Policies

a. This Information Paper outlines provisions of the 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). ARRA expands the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which provides stricter penalties and enforcement including guidance to understand the Privacy and Security Rules with increased importance.

II. Background

a. 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." Several HITECH Act provisions specifically relate to privacy and security issues. These provisions that relate to privacy and security issues 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.

b. 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.

III. Privacy and Security Areas Affected

a. **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 or jurisdiction are affected, notice in the media is required, and HHS must be informed immediately. If a breach affects fewer than 500 individuals,

the covered entity may notify the Secretary of breaches of unsecured protected health information on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered. The new breach reporting requirements took effect September 23, 2009. The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces the Breach Notification Interim Final Rule. Several points are important to note:

1. HHS "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 Protected Health Information (PHI).
2. 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.
3. 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 Defense Health Agency Privacy and Civil Liberties Office (DHA PCLO) will advise the MHS covered entity as to notifying affected individuals. Further, the DHA PCLO will report breaches of less than 500 to HHS on behalf of the covered entity.

b. **HIPAA Standards and Individual Rights.** The HIPAA "minimum necessary" standard is a key protection of the HIPAA Privacy Rule here protected health information (PHI) should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity. In addition, the HITECH Act details several changes to the individual rights provisions outlined in the HIPAA Privacy Rule:

1. **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.
2. **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 by their medical providers and TRICARE (including managed care support contractors) where those disclosures are made through EHRs.

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

c. **Business Associates.**

1. 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. The HIPAA rules generally require that covered entities and business associates enter contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.
2. HITECH makes business associates subject to the EHR accounting requirement noted above.
3. 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.
4. HITECH specifies a reversal of the burden of proof, so now when a violation of HIPAA occurs the covered entity or business associate now must prove the violation did not result in the unauthorized disclosure of PHI.
5. 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.
6. HR 7898 became law amending the Health Information Technology for Economic and Clinical Health Act (HITECH Act), 42 U.S.C. 17931, to require that "recognized cybersecurity practices" be considered by the Secretary of Health and Human Services in determining any Health Insurance Portability and Accountability Act fines, audit results, or mitigation remedies.

If you have any questions about any of the information above, please contact the DHA PCLO at:dha.ncr.admin-mgt.mbx.dha-privacyguidance@mail.mil.