



Maintaining Privacy and Security of Individual EHRs

Overview

The American Recovery and Reinvestment Act's (ARRA) provisions for healthcare include significantly stricter and broader rules for maintaining the privacy and security of individual Electronic Health Records (EHR). Among key items, "business associates" are now subject to the same rules as covered healthcare providers for maintaining the security and privacy of private medical information as well as notification requirements and penalties in the event of a breach.

On November 30, 2009, the regulations associated with addressing the privacy and security concerns with the electronic transmission of health information took effect.

Summary of Key Provisions on Privacy

Privacy Regulations and Penalties Now Extend to Business Associates

Privacy and security provisions that apply to covered healthcare entities will also be applied to business associates working with those entities. The two parties must have a contract in place that includes the security and privacy requirements. A business associate that violates any of the security provisions will be subject to the same criminal and financial penalties as a covered entity.

Exceptions: Despite this definition, a breach has NOT occurred if:

- The unauthorized person exposed to the information cannot reasonably retain this information.
- The event was unintentional and occurred in good faith as part of an authorized person's duties on behalf of a covered healthcare provider or its business associate, and there is no further unauthorized activity with the information.
- An otherwise authorized individual inadvertently discloses protected information to an authorized individual at the same facility, and there is no further unauthorized event.

New Notification Requirements Established

Upon discovering a breach:

- A covered entity must notify each person whose information has been — or is reasonably believed to have been — improperly accessed, acquired or disclosed.
- A business associate must notify the covered entity and must include the identification of each individual who is confirmed or believed to have been affected.
- Notifications must be made no later than 60 calendar days after discovery.
- Affected individuals must be notified in writing.
- If 10 or more affected individuals have out-of-date contact information, the notification must be posted on the covered entity's website or announced in major media serving the likely geographic residences of the affected individuals.
- If a breach affects more than 500 people, the covered entity must notify prominent media as well as the HHS secretary.

Individuals Can Request Their Records and Information About Disclosures

A covered entity that uses EHRs must provide a copy of an individual's EHR to that individual (or a third party the person designates) upon that individual's request. The fee for this may not exceed labor costs for handling the request.

Furthermore, covered entities and their business associates must be prepared to give an accounting to individuals about disclosures of that individual's health information. However, the covered entity is only required to provide three previous years of health information from the date of the request.

Within six months of the Act's passage, the HHS secretary will decide what information must be retained about each disclosure.

Enforcement and Penalties

Breaches are subject to investigation and fines for alleged criminal violations of HIPAA's Privacy and Security Rule. Depending on the severity of a breach, fines can range from \$100 per violation (with a \$25,000 cap for the same type of violation in a calendar year) up to \$50,000 per violation with a \$1.5 million cap. Affected individuals can be eligible to receive a portion of the fine. In addition, state attorneys general may bring civil actions on behalf of residents.

Personal Health Record Vendors Must Notify FTC of Breaches

Personal Health Record (PHR) vendors must notify affected individuals as well as the Federal Trade Commission (FTC) of a discovered breach. The FTC then must notify the HHS secretary. Violations will be treated as unfair or deceptive acts or practices.

Regional Office Privacy Advisors, Education Program

Within six months of enactment, the HHS secretary will direct regional offices to offer guidance and education to covered entities, business associates, and individuals on their rights and responsibilities regarding protected health information. Within 12 months, the Department's Office for Civil Rights will develop and deploy a national education initiative on the privacy of protected health information.

For more information about any of our service offerings, please contact your Dell representative or visit dell.com/services.

Expanded Privacy Definition and Coverage

The ARRA significantly expands the scope and enforcement of HIPAA privacy protections and requirements of patient data including personal information and medical records.

The legislation also expands the rules to make "business associates" subject to the same penalties and establishes notification requirements in the event of a data breach.

Dell Services Can Help

Having served the healthcare industry for more than 20 years, Dell Services has the depth of experience necessary to understand the unique challenges facing healthcare organizations as they seek to fully implement EHRs. Using our extensive industry expertise and innovative solutions, we can help your organization maximize the opportunities available through this landmark drive to implement EHRs for every American by 2014.