

## **The American Recovery and Reinvestment Act of 2009 Health Information Technology Privacy Summary**

### Background

On February 17, 2009, President Obama signed the American Recovery and Reinvestment Act of 2009 (hereafter ARRA). One of the many goals of the ARRA is to encourage the adoption of electronic medical records by doctors and hospitals. One of the most significant barriers to this process is the lack of powerful existing safeguards for patient information. In poll after poll Americans, both doctors and patients, harbor worries that their personally identifiable medical data will not be protected.

Medical records privacy is currently protected pursuant to the Health Insurance Portability and Accountability Act (hereafter HIPAA). Unfortunately the HIPAA regulations contain numerous exceptions which allow for widespread access, sale and use of medical records. Patients have almost no control over how information is used, to whom it is disclosed or even the ability to learn about these disclosures after the fact.

If electronic medical records are to come into widespread use, these problems must be fixed. The protections contained in the ARRA begin that process by tying funds appropriated by the Act to a series of extensive privacy and information technology security conditions. The process will continue through an extensive regulatory process mandated by the Act and convened by the Secretary of the Department of Health and Human Services.

The ARRA remedies a number of problems with HIPAA, at least for medical records. Its provisions include limitations on the sale of records and the use of records for marketing and fundraising. It also gives patients the ability to learn who has viewed their record and when it has been accidentally or purposely disclosed. It extends the legal reach of HIPAA to everyone who handles medical records (from legal work and accounting to management and administrative functions) not just doctors and insurers.

Many of the provisions described below are important first steps; however they also contain exceptions, extended implementation dates and other loopholes. They could be significantly weakened or strengthened depending on the language of the final regulations implementing them. The ACLU has been closely monitoring HIPAA and its privacy protections for more than 10 years and we were [involved in the crafting](#) of the protections embodied in the ARRA. We will remain active as the regulatory process implements these provisions and fight to assure that the provisions outlined in the ARRA are implemented in a robust manner, one that fully protects patient privacy.

### Specific Provisions

ARRA makes changes to existing privacy protections in a number of key areas.

#### **Sale of medical records**

While HIPAA prohibits the disclosure of health information by doctors, insurers and other covered entities, it does not forbid the sale of such information to entities that are authorized to receive it under HIPAA or sale by entities – such as data aggregation

companies – that are not covered by HIPAA. Because HIPAA has so many exceptions, a market has sprung up allowing entities who have no direct interest in specific medical records to buy them anyway. This leads to the resale and repackaging of patients' records and personally identifiable information from non-covered entities to other corporations, including employers, insurance companies, for-profit and not-for-profit researchers, and pharmaceutical companies. This is a multibillion dollar industry which traffics in prescriptions, personal health information and other coverage information.

This sale of records has led not only to a widespread invasion of privacy but also potentially increased health care costs and affected medical decisions. Some of the key purchasers of medical information are the data aggregation companies that collect information on what medication doctors prescribe, analyze this information and then sell it to pharmaceutical companies. This information allows those companies to target particular doctors and encourage or reward them for prescribing particular medications. This process encourages the sale of more expensive drugs and may distort a doctor's decision making.

Section 13405(d) creates an express prohibition on the sale of electronic health records or protected health information without a valid authorization from the patient. This provision is an important step for privacy, a long overdue stipulation that recognizes that intimate information about patients' health is not a commodity to be bought and sold. However it also contains a number of exceptions, some of which are potentially problematic and must be monitored as part of the regulatory process.

Key exceptions include:

- *Consent.* Because medical information can be sold with patient permission, consent must be gained in a clear, informed manner;
- *Health surveillance.* Public health authorities and employers will be able to purchase information in order to monitor public health (the price of this information can be limited by the Secretary);
- *Treatment.* Information can be purchased if the buyers and sellers can justify that the transaction is undertaken as part of that HIPAA defines as "treatment." Because the concept of what constitutes medical treatment can be particularly elastic, this exception will require careful scrutiny.

## **Marketing**

While the existing HIPAA regulations theoretically bar marketing to patients, the definition of marketing contains enormous exemptions. Specifically, covered entities are allowed to describe products or services they provide or to "direct or recommend" alternative treatments without engaging in marketing. 45 CFR §164.501. This allows drug companies and other entities to conduct unlimited marketing of health related items to patients as long as the marketing is conducted on behalf of a covered entity like a pharmacy or health plan. There is no time limitation or opt out from this marketing. In addition, hospitals and doctors may use the personal information they collect from patients to fundraise.

Section 13406 of ARRA contains some important limitations on these practices. It limits the use of information for marketing to only currently prescribed drugs and restricts the fee a marketing communication firm is allowed to pay. This provision alone will significantly impact the "prescription reminder" practices of certain entities that are disguised as patient education, but in actuality are simply advertisements intended to confuse patients into purchasing certain products or pharmaceuticals. It also requires covered entities like pharmacists to receive consent from patients in order to send them

marketing materials. However, it does not seem to require consent if those materials are sent from a business partner of the pharmacy or doctor. Finally, the section allows patients to opt out of having their patient information used by hospitals and other for fundraising.

Strong regulations, especially tight limitations on payments, could substantially reduce the amount of marketing materials. If substantial payments for marketing continue there will likely only be a limited reduction in this practice.

### **Breach Notification**

Under current federal law health care providers, insurers and their business associates are not required to notify patients if there is a breach in the privacy, security or integrity of their personal information. This has left providers with little incentive to disclose when records are improperly accessed, lost or accidentally exposed. A patchwork of state laws provides only limited disclosure.

Section 13402 institutes a comprehensive disclosure requirement, requiring notification, generally within 60 days, anytime unsecured information is accessed, acquired or disclosed as a result of a breach. Disclosure is necessary both when breaches are intentional (i.e. the result of computer hacking) or unintentional (due to an accident). Notification must be by first class mail (or electronic mail at the patient's preference) and public notification must occur in the case of a breach involving more than 500 persons. No breach notification is necessary if the information is secured by a method, such as encryption, that is specified by regulation.

Section 13407 extends these same protections to the breach of personal health records. Personal health records are records of prescriptions, laboratory results, physicians' reports and lab images created by individuals and held by companies like Google or Microsoft.

### **Business Associates**

Under current regulations, HIPAA only applies to covered entities like hospitals, doctors and insurers, not other entities, called business associates, who perform a variety of services for them – from legal work and accounting to management and administrative functions. These business associates are only limited by the contracts they have signed with covered entities, not civil or criminal law. This loophole has led to a number of troubling and outrageous practices. In one instance a dispute over fees led a business associate to threaten to publish personal medical information.

Sections 13401 and 13404 fill this gaping loophole, requiring business associates to comply with HIPAA's security provisions for transmitting information and applying HIPAA's criminal and civil penalties to business associates in the same manner it applies to covered entities like doctors.

### **Audit Trails**

While current HIPAA regulations theoretically allow individuals to receive an account of who has viewed their medical record, access to these audit trails is littered with exceptions. One of the most gaping of these loopholes allows covered entities such as insurers to refuse to make disclosures when information was released "to carry out treatment, payment and health care operations." 45 CFR §164.528.

Section 13405(c) substantially narrows this exception. Doctors, hospitals, health insurance providers and others who treat patients and pay for health care, as well as

their business associates, will be required to provide an accounting of who has viewed a patient's electronic medical record over the past 3 years. The only concern raised by this provision is that the ARRA allows these disclosures to be substantially delayed by regulation, in some cases for as long as eight years. Audit trails are a critical step in safeguarding patient privacy because they represent the first step in determining whether patients' records have been inappropriately accessed, and if, so, by whom. Monitoring the development of these audit trails will be an ongoing concern in order to assure that disclosures are reported as quickly as possible.

### **Right to Restrict Information Sharing**

Under current HIPAA regulations an individual has the right to request that a provider restrict the use or disclosure of particular health information. However the health care provider or insurer is not required to agree to the restriction. Section 13405(a) changes this, allowing a patient to restrict disclosure of information regarding a specific health care item or service, if that item or service was paid for out-of-pocket. This provision gives patients another option for keeping particular health procedures private, such as contraceptive care or mental health services.

### **Advisory panels**

Two key bodies– the Health Information Technology Policy Committee and the Health Information Technology Standards Committee – will create the rules that govern precisely how electronic medical records are to be used and controlled. Section 3002 requires the Policy Committee to consider privacy concerns. It also requires that membership on this body include individuals with expertise in privacy and data security as well as members expressly charged with safeguarding the rights of patients and consumers. Finally the Office of the National Coordinator (which is the entity within Health and Human Services specifically tasked with writing regulations) must have a Chief Privacy Officer.

### **Enforcement**

Since its inception enforcement of the HIPAA has been lax. Under current law civil violations of HIPAA are enforced by the Health and Human Services Office of Civil Rights (OCR), which tends to favor a collaborative approach with covered entities rather than investigation and stiff penalties. Criminal enforcement has also been limited due to the Department of Justice (DOJ)'s conclusion that only a covered entity (not an individual) can be criminally prosecuted under the law. Sections 13409 and 13410 amend the enforcement provisions of HIPAA for privacy violations by, increasing civil penalties, allowing criminal enforcement against individuals, requiring formal investigations and automatically triggering fines in cases of "willful neglect" and allowing for civil enforcement in cases when the DOJ decides against criminal prosecution. Additionally, fines collected for violations of HIPAA will be turned over to OCR for enforcement or given to individual victims who have been harmed. Finally, ARRA would also authorize state attorneys general to enforce civil provisions of HIPAA.

### **Impact on state law**

The default rule for HIPAA remains in effect – namely that HIPAA supersedes contrary provisions of state law unless those provisions are more protective of the privacy of personally identifiable health information. Section 13421.