

Congress Should Protect Patient Records Privacy in HIT Legislation

Congress should ensure that patient records privacy and security is a cornerstone of any legislation that promotes the development of health information technology (HIT) in the health care system.

HIT development involves moving the current, mainly paper-based health records system to a national electronic health records system. This change has many advantages. For example, it would allow for the comprehensive management of information and its secure exchange between patients, providers and other entities that use health records. It could improve quality by preventing medical errors and reduce costs through decreased paperwork and increased administrative efficiency. Patients would be helped as they manage chronic diseases. Providers would have accessibility to records in a standard, electronic format for treatment decisions and for payment purposes.

There is a major risk associated with HIT development—health records in a national, electronic system are more susceptible to intentional or negligent disclosure on a massive scale, causing a loss of privacy and other related problems for patients. This is a real concern since records in centralized electronic systems are being compromised on a daily basis. In fact, according to the Privacy Rights Clearinghouse, more than 216,000,000 data records belonging to U.S. residents have been exposed to potential misuse as a result of security breaches since January 2005.

Mental health records need heightened privacy and security protection. Mental health records are particularly vulnerable to disclosure, because they typically contain information that could lead to a patient's embarrassment or stigmatization. For these patients even the potential loss of records' privacy can be devastating. The patient and psychologist must maintain control over the release of these records into the health system since, as the U.S. Supreme Court recognizes in *Jaffee v. Redmond*, their relationship is "rooted in the imperative need for confidentiality and trust" and that the "mere possibility" of disclosure could impede the development of a confidential relationship necessary for successful treatment.

A strong federal HIT privacy and security standard would, among other provisions—

- Recognize a patient's fundamental right to records privacy.
- Preserve stronger privacy, security and related state laws.
- Recognize consent and require patient authorization for psychotherapy and other sensitive records.
- Provide for strong enforcement.

A strong federal HIT privacy and security law must also harmonize with the requirements of HIPAA. Psychologists, like other providers, must currently comply with the privacy and security standards provided through the Health Insurance Portability and Accountability Act (HIPAA). The relationship between the HIPAA standards and HIT privacy and security standards will have to be clearly addressed as the HIT debate moves forward to ensure the strongest protections for patients while providing the least compliance burden for health care providers.

Government Relations Office
February 2008