



Claim vs. Reality – HIT and Privacy in the Economic Recovery Package

Claim: Accounting for Disclosure Requirement will be overly burdensome for providers while offering little benefit to consumers.

Reality: For patients, having an ability to track disclosures from their medical records is important to building trust in health IT and is consistent with the transparency and accountability principles that are the hallmark of fair information practices. Today consumers have that right to know who has accessed the financial information in their credit report; such a right is just as important for their sensitive health information. Some charge that the current bill's requirements are prohibitively burdensome. But this provision is carefully crafted to strike the right balance between consumers' right to know and not imposing overly burdensome mandates on industry. The accounting for disclosures requirement only applies to disclosures, which by definition occur outside of an entity. It also is only imposed on those who have electronic health records (EHRs), technology that could be engineered with the ability to automatically track disclosures without a significant imposition on staff time or resources. To further minimize the burden, the bill requires the Secretary to determine what needs to be disclosed in an accounting, and the requirement will not become effective until a technology standard and regulations are developed and implemented. It also allows a five-year "grace period" for providers who are early EHR adopters to upgrade their systems if they do not have this capacity. By making this a legal requirement, the bill provides a necessary incentive for the EHR market to include this key consumer-oriented functionality.

Claim: Breach Notification Requirement will be both overly burdensome for providers and will result in a deluge of notifications to patients.

Reality: Some industry interests are calling for a "harm trigger" standard to define when a breach of patients' health information warrants notification. But for patients whose health care information has been hacked into or wrongfully disclosed, what constitutes "harm" is often difficult to define. And the entity that held the data is not in the best position to determine whether the release of that data is going to be embarrassing or worrisome to an individual. The bill strikes a careful balance by imposing a duty to notify unless the data is protected by encryption-type technology, and it provides a strong incentive to use technology to make the information inaccessible (to avoid having to notify), which greatly reduces the risk of breach. The bill also provides a safe harbor for employees or agents of providers who unintentionally access patient information without authorization, but do so in good faith and in the course of their professional duties. In those instances, if there is no further disclosure, the entity would not be required to notify patients that a breach had occurred.

Claim: Marketing Restrictions will imperil disease management, consumer education and mail order programs.



Reality: Some industry interests claim that the marketing restrictions are too broadly worded and could preclude patients from learning about important health services and products, such as new disease management programs or potential savings on prescription drugs. The current legislation **in no way** precludes health care entities – pharmacies, health plans, or providers – from using patients’ personal information to inform them of services or products that can improve their patient care. However, if an outside entity like a pharmaceutical company or medical equipment supplier wants to pay a provider, plan or pharmacy to market the outside entity’s products or services to patients, that entity must get prior authorization for those communications.

Claim: Tightening the definition of “Health Care Operations” will limit important health promotion, quality improvement, and care coordination programs.

Reality: Some stakeholders have argued that the proposal would require the Secretary of Health and Human Services (HHS) to restrict the use of personal health information for health promotion, quality improvement, and care coordination programs. This is a complete over-interpretation of this provision. The Secretary is required to review the current definition of “Health Care Operations” – currently a list of over 20 administrative functions– and may require health entities to seek patient authorization for some of those activities, or require that some be performed with de-identified data. However, the Secretary may also, after review, choose to leave the definition of “Health Care Operations” unchanged. Industry and patient groups will have ample opportunity to comment on the Secretary’s review of these provisions to ensure that critical information flows for treatment and health care quality improvement are not disrupted.

Claim: State Attorney General Enforcement of HIPAA will lead to frivolous lawsuits and inconsistent interpretation of federal law.

Reality: Many in industry have expressed concern about allowing State Attorneys General to enforce HIPAA. Yet this provision is a critical element for building consumers’ trust in the emerging nationwide information technology network. Further, there are other examples in federal consumer protection law where Congress has vested enforcement jurisdiction in both federal and state authorities (two examples are federal antitrust laws and CAN-SPAM). At the federal level there has been almost no meaningful enforcement of the HIPAA Privacy and Security rules. In fact, the HHS Office of Civil Rights has yet to impose a single civil monetary penalty for HIPAA violations. States’ Attorneys General have a strong incentive to be advocates for their citizens, and are important members of a network of enforcement. The provision provides only authority for state authorities to enforce HIPAA and does not require them to do so. The provision also includes safeguards to ensure that entities are not subject to “double jeopardy” for the same offense.