A National Health Information Network—What Are the Real Privacy Issues?

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 mandated the development of a unique patient identifier (UPI) for “every individual, employer, health plan, and health care provider.” UPIs were intended to serve as central building blocks for new health information technologies and to enable physicians, hospitals, and other authorized users to share clinical and administrative records with greatly improved efficiency. But in the years since 1996, Congress has consigned UPIs to legislative limbo, responding to concerns that federal privacy policies are not adequate to protect the personal health information associated with a UPI.

RAND analysts Michael Greenberg and Susan Ridgely examined the privacy implications of UPIs in the context of an emerging national health information network (NHIN). They suggest that UPIs plausibly might be privacy enhancing rather than privacy degrading. More important, they assert that the controversy over UPIs distracts from the key privacy issues connected with an NHIN: namely, the need to strengthen HIPAA privacy rules and to reconcile current state laws on health information privacy.

Strengthening HIPAA Privacy Rules
The United States has adopted an incremental approach to developing an NHIN, in which regional health information organizations (RHIOs), established at the state and community levels, will gradually develop electronic links and rules for exchanging health information across state boundaries. This patchwork approach accommodates the reality that there are no national UPIs. Therefore, health information is subject to lots of different local schemes for indexing and accessing records.

Greenberg and Ridgely note that HIPAA’s privacy rules are not adequate for an NHIN, regardless of whether the network involves a uniform national system or a patchwork arising from RHIOs. For example, HIPAA applies only to “covered entities,” such as physicians and health plans. But many other organizations—including suppliers, employers, and insurers—may become involved in collecting and using health records in an NHIN. Moreover, all medical providers will actively contribute protected information to an NHIN, but no provider will have direct control over how and to whom protected information is distributed downstream. Meanwhile, privacy advocates are also concerned by the fact that the U.S. Department of Health and Human Services, the chief federal regulator, has not enforced HIPAA rules strongly to date, relying instead on cooperation from covered entities. None of these privacy concerns is directly related to, or affected by, UPI technology.

Reconciling State Laws Regarding Health Information Privacy
HIPAA allows states to enact more-stringent privacy protections than the national (HIPAA) standard. It comes as no surprise, then, that state privacy laws are quite heterogeneous. This diversity may slow evolution of an NHIN—for example, RHIOs in state A may decide to restrict or foreclose sharing of health information with RHIOs in state B, because the latter state does not provide adequate privacy protection. Legal scholars believe that a patchwork approach to health privacy may limit and degrade the functionality of a national network, but to date, potential conflict of state privacy laws has not been a major part of the public discussion.

This fact sheet is based on Greenberg MD and Ridgely MS, “Patient Identifiers and the National Health Information Network: Debunking a False Front in the Privacy Wars,” Journal of Health & Biomedical Law, Vol. 4, No. 1, 2008, pp. 31–68.
Many reforms to increase health privacy have been suggested. Possibilities include the following:

- Extend HIPAA privacy rules to RHIOs, an NHIN, and basically any organization that collects, stores, transmits, or uses health information.

- Enact federal legislation against misuse of personal health information—for example, criminalize unauthorized access to it.

- Enact federal rules to govern operation of an NHIN as well as strong enforcement procedures.

- Build privacy protection into an NHIN architecture—for example, let patients decide whether they want to participate in the network, or let them restrict access to certain types of health information, such as mental health or infectious disease.

The current discussion about UPIs is peripheral to the basic privacy issues raised by implementing an NHIN. It is these issues that urgently need public attention.