Perspective

Crossed Wires: How Yesterday’s Privacy Rules Might Undercut Tomorrow’s Nationwide Health Information Network

The emergence of the Nationwide Health Information Network presents challenges to current privacy laws.

by Michael D. Greenberg, M. Susan Ridgely, and Richard J. Hillestad

ABSTRACT: More than a decade after passage of the Health Insurance Portability and Accountability Act (HIPAA), concerns about the privacy and security of personal health information remain a major policy issue. Now, the emergence of the Nationwide Health Information Network (NHIN) presents deeper underlying privacy challenges, which will require renewed attention from policymakers as federal and state privacy rules need to be revisited. This is necessary because the current framework of privacy laws is not well suited for regulating a transformed healthcare system, where computer networks supersede conventional communications media. [Health Affairs 28, no. 2 (2009): 450–452; 10.1377/hlthaff.28.2.450]

Concerns about privacy and security of personal health information remain widespread today, more than a decade after passage of the Health Insurance Portability and Accountability Act (HIPAA). Those concerns have been driven in part by new technology development, and by a shift in federal policy emphasizing the implementation of the Nationwide Health Information Network (NHIN). The formation of regional health information organizations (RHIOs) has now become an initial, incremental step in building this national network; RHIOs have been a testing ground for new privacy and security initiatives. Deven McGraw and her colleagues and Linda Dimitropoulos and Stephanie Rizk describe laudable efforts to address continuing privacy concerns, such as through trusted network design characteristics, multistate collaborations, and targeted legal reforms.1 In our view, though, the emergence of a nationwide network presents some deeper, underlying privacy challenges, which will require renewed attention from federal policymakers.

The privacy regime under HIPAA involves two basic problems. First, neither the HIPAA privacy rules nor state laws on privacy were written in contemplation of the movement from traditional, bilateral contacts between providers toward widely distributed, network-based record keeping. Networked communications offer many potential benefits, but they also invoke serious privacy issues that the current HIPAA framework neglects to address. Second, the HIPAA privacy rules also...
failed to anticipate the development of an interoperable, national network. Unfortunately, concerns about privacy within the future NHIN have led to political resistance to one important network design element: a unique patient identifier (UPI). An implication of the unresolved privacy concerns has been the adoption of a “patchwork” model for the NHIN, with less interoperability and the prospect of fewer functions and less-advanced automation.

Privacy And Transformation

Despite all of the ambiguities and shortcomings of the current HIPAA privacy law framework, that framework is at least basically aligned with a traditional model of medical communications, wherein one provider communicates directly with another in sharing records, ordering tests, and so forth. Medical communications have traditionally involved oral or written contacts with built-in validation features; the nature of the media involved fundamentally restricted the risks of interception or inadvertent disclosure.

■ Expanded, rapid access. The great promise of health information technology (IT), however, involves a transformation of conventional communication practices. In principle, networked computers and electronic record keeping can give providers rapid access to far-flung records. This kind of access should make it easier for providers to obtain information and to build more-complete health records to support clinical decision making. As networks expand, providers should be able to obtain records from more distant locations, with increasing rapidity, seamless access, and automated consolidation across various facilities, institutions, and computer platforms. Ultimately, as access to networked records becomes ubiquitous, providers might become increasingly dependent on uploading to and downloading from the network as a basic aspect of medical practice.

■ Lack of oversight. Current privacy rules under HIPAA (and under state laws) are not framed to deal with this kind of communications model, where everyone relies on a widely distributed network infrastructure to do their jobs. To give one example of a related problem, does the Treatment, Payment, and Operations (TPO) exemption under HIPAA apply to providers who share new medical records through a fluid, widely distributed network—and if so, how? In contrast to old-style medical communications where the sharing of information occurs mostly in response to specific queries that are self-validating (for example, a nurse calls the pharmacist to request a prescription), new-style communications will increasingly involve feeding the network and trusting that the subsequent users of information are legitimate and themselves compliant with the privacy and security obligations of all applicable laws. There is no clarity under HIPAA about how TPO should apply to this sort of network communication. Nor is there clarity under state law regarding the “due diligence” obligations of providers to ensure that queries for information through a distributed network are legitimate and secure. And that’s just one of many ambiguities.

Only two aspects of the future seem clear. First, the larger the networks grow, the weaker local controls over information (for example, point-of-access restrictions) are likely to become. Second and by corollary, this seems to be a recipe for the erosion of existing privacy protections, unless laws are updated to accommodate the new communications model.

Privacy Drag On The NHIN

Elsewhere, commentators have reviewed the privacy and technical concerns surrounding proposals for a UPI as an element of a national network. The UPI has been controversial, but it is potentially a linchpin technology, in that it would help establish the architecture...
for querying and retrieving records across systems. The recent reviews of the UPI have suggested three basic findings: first, far from weakening privacy, the UPI could improve privacy, depending on the technical features of the computer networks in which it is embedded. Second, efforts to build the NHIN have continued in the absence of the UPI but have centered on incremental affiliations among local and regional institutions. And finally, large-scale, patchwork networks that eschew UPIs in favor of more piecemeal methods for retrieving records will very likely entail increased privacy risks, and perhaps new clinical risks as well (as a result of errors in record matching).

Fundamentally, we think that the debate over the UPI has been misdirected and more accurately reflects underlying privacy concerns surrounding the development of an interoperable, national network. As discussed above, there are major ambiguities in how existing legal standards would apply to such a network and, consequently, the potential for significant degradation of existing privacy safeguards. Does the patchwork-model NHIN involve greater privacy risks than would a hypothetical, more-unified NHIN architecture? That question is difficult to answer without speculation. But in at least some technical respects, such as the likelihood that a patchwork NHIN will depend heavily on Social Security numbers as identifiers for matching records, the superficial answer appears to be “yes.” Meanwhile, the patchwork-NHIN model also implies that the individual sites that constitute the national network will be more idiosyncratic and segregated, and less standardized and interoperable, than they otherwise might be. By implication, privacy concerns have already had a major impact on policy decisions about what kind of NHIN to build, in ways that may be less than optimal.

**Policy Implications**

In 2009, privacy continues to be a major driver of health care policy, in the shadow of the emerging national network. We suggest that the current framework of privacy laws is fundamentally ill-suited for regulating a transformed health care system, in which computer networks begin to supersede conventional communications. Fears of exactly this future have contributed to questionable policy choices on both privacy and in the piecemeal design for the NHIN. We believe that there is an urgent need for policymakers to revisit the basic contours of privacy law in light of the new communications paradigm. Absent such review, we foresee major ambiguities in how privacy law will be applied in the future; the likelihood that legal safeguards for personal health information will deteriorate; and the distinct possibility that the NHIN will evolve to be less robust than it ideally should be.

**NOTES**


5. The UPI would more likely improve privacy within a network with other robust security features, such as encryption, audit trails, digital signatures, and strong access restrictions. By contrast, if we assume a network architecture that includes none of these, it becomes less clear whether the UPI would improve privacy.