



HIT Privacy Provisions in Proposed Stimulus Legislation

Issue

Legislative proposals that would require patient consent for the use of clinical data for “operations” (as defined by HIPAA) could impede quality improvement, comparative effectiveness, and safety surveillance, all of which are critical to fundamentally improving health care delivery. Most proposals to expand funding for health IT are accompanied by well meaning provisions intended to strengthen patient privacy protections.

However, AMGA members have expressed serious concerns about the impact of such provisions on:

- Internal and collaborative quality improvement initiatives; and
- Use of real-world data for comparative effectiveness research and safety surveillance.

More than 80 percent of AMGA member medical groups have adopted EHRs, and use e-prescribing. Both internally and in cross-group collaborations, they are making extensive use of these data for quality and performance improvement. Based on their experience, our members believe that requiring specific patient consent for “operations” would:

- **Introduce serious selection bias into analyses that are essential for quality improvement;**
- **Impose prohibitive administrative burdens, both to track authorizations and exceptions and to provide patients an accounting of disclosures; and**
- **Create a barrier to expanding beyond claims data for quality reporting, pay-for-results, and public accountability.**

More generally, there are serious “inferential gaps” in our traditional evidence base:

- New technologies, including diagnostics and procedural interventions, are being introduced at an increasingly rapid pace;
- Drug trials often exclude elderly patients and those with multiple comorbidities, the very patients who often present the greatest therapeutic challenges and consume a disproportionate share of health care resources; and
- Few prospective studies address models of care and organization of the delivery system.

It is imperative that we take advantage of real-world data to expand our evidence base in these areas. The most powerful methods use PHI to create longitudinal records, combining data that may reside in multiple locations, as a result of our fragmented health care delivery system, and merging them with other data that are often critical for risk adjustment. These longitudinal records are then de-identified, and only fully de identified data are used for analysis and

reporting. Requiring specific patient authorization for these uses, conducted through a trusted intermediary via a cascade of strict business associate agreements, would hobble this resource, which is increasingly important to guide both policy making and clinical care.

Background

The American Medical Group Association (AMGA) represents multi-specialty medical groups and other organized systems of care that collectively provide health care to more than 80 million patients. AMGA advocates for continuously improving patient care through innovation, information sharing, benchmarking, and creation of sound public policy.

Most AMGA members have been early adopters of health information technology (HIT) and have made these investments because it helps them deliver quality health care and streamline administrative processes. The evidence continues to grow that more organized systems of health care delivery and the use of HIT are effective ways to reform the current health care delivery system.

Recent legislative proposals to expand the adoption of health information technology (HIT) have been introduced, notably the PRO(TECH)T Act of 2008 and the Health-e Information Technology Act of 2008. While both of these bills contain provisions that would stimulate and provide incentives for more widespread adoption of HIT, they would also significantly revise portions of the Health Insurance Portability and Accountability Act (HIPAA), especially as it pertains to uses of protected health information for health care operations.

Both legislative proposals have provisions that would require patient consent before their protected health information could be used for health care operations, and would also require a listing of disclosures for the purposes of health care operations in patient-requested accountings of disclosures, which are currently exempted under HIPAA. These provisions apply specifically to health care providers utilizing EMRs.

HIPAA's "health care operations" include conducting quality assessment and improvement activities, population-based activities relating to improving health care or reducing health care costs; protocol development; case management and care coordination; reviewing the competence or qualifications of health care professionals; conducting training programs for students and practitioners; accreditation; certification; auditing; compliance activities; customer service; resolution of internal grievances; and the sale, transfer, merger, or consolidation of all or part of a covered entity, activities that take place everyday wherever health care is delivered. All of these activities may involve data gathering and transmission via electronic infrastructural means such as data registries, EMRs, claims, reports, prescriptions, images, etc.

The utility and societal benefits inuring from such data gathering would be severely constrained if not nullified by imposition of individual informed consent for use of such data. Policy makers should bear these concerns and cautions in mind as HIT advances and legislate and regulate in a fashion that protects privacy, but preserves the ability for public health, quality control, and the many attendant other beneficial uses of electronic transmission of health care information.

Position

Legislative proposals that would require specific patient consent before use of clinical information would be contrary to policy objectives to reform health care delivery, such as comparative effectiveness research and quality reporting.

To understand the impact these privacy provisions would have on medical groups, AMGA queried several of its members. Their responses emphatically indicate that asking their patients to provide explicit consent for use of their protected health information (usually de-identified in any case) would severely compromise the amount and utility of information available for quality improvement initiatives for the following reasons: **evidence-based/outcomes-based data would not provide accurate information if collection was restricted to those patients willing to sign a consent for their data to be used for health care operations; development of clinical guidelines and population-based activities related to improving or reducing health care costs would be compromised; data collection for PQRI could be jeopardized since it relies on data from 80% of a denominator group, which may not be possible to collect. These responses also suggest that comparative effectiveness research, which will compare the clinical effectiveness of a particular service with its alternatives, would be hobbled by the lack of data that is not necessarily statistically valid. The same holds true for other quality improvement activities.**

AMGA members are also greatly concerned about requiring health care providers to include disclosures for the purposes of health care operations in patient-requested accountings of disclosures. From an administrative and resource use perspective, this would require generating enormous amounts of data that has no apparent purpose in improving the way health care is delivered or reducing expenditures.

Current Regulatory Framework

The HIPAA provisions, when properly implemented, provide a solid foundation for patient privacy. For example, the requirement to audit access to protected health information found in the HIPAA security rule provides the basis to enforce a disciplinary policy, up to and including termination, for an employee who accesses a patient's information without proper authorization (a standard found in the HIPAA privacy provisions). The security rule also requires use of access controls, individual passwords, and automatic time-outs for computer screens, all of which contribute to safeguarding patient information.