Written Testimony of

Robin K. Omata, J.D., Ph.D.

Practice Leader

Kaiser Foundation Health Plan, Inc.

On behalf of the Kaiser Medical Care Program

Before the

Policy Committee, Office of the National Coordinator
For Health Information Technology

U.S. Department of Health and Human Services

Accountability Requirements of HIPAA Covered Entities And Adoption of Electronic Health Records

September 18, 2009

Introduction

Dr. Blumenthal, Dr. Tang and other distinguished members of the committee, thank you for the invitation to participate in today's hearing. I am Robin Omata, Practice Leader for Privacy and Security in the National Compliance Ethics, and Integrity Office of Kaiser Foundation Health Plan, Inc. and Kaiser Foundation Hospitals.

Kaiser Foundation Health Plan, Inc. is a nonprofit health plan that is an integral part of the Kaiser Permanente Medical Care Program. The Kaiser Permanente Medical Care Program is the largest private integrated healthcare delivery system in the United States and in addition to Kaiser Foundation Health Plan, Inc., includes the Kaiser Foundation Hospitals, and the Permanente Medical Groups, independent physician group practices that contract with the health plan to meet the health needs of Kaiser Permanente's approximately 8.7 million members in nine states and the District of Columbia.

My testimony today is directed to the transparency and accountability requirements of HIPAA covered entities and the adoption of electronic health records. The main points presented today are:

- Healthcare dollars must be directed to value-added investments that provide measurable benefits to patients;
- Accountability and transparency of HIPAA covered entities are already largely accomplished through existing privacy and security compliance requirements;
- We respectfully suggest that the new American Recovery and Reinvestment Act of 2009 (ARRA) disclosure accounting requirement does not add value relative to the costs of implementing the requirement; and
- We also recommend that the Meaningful Use measure that uses a confirmed HIPAA privacy or security violation as the basis for measuring privacy and security protections of the EHR be revised or eliminated.

Background on the Kaiser Permanente Medical Care Program

I list a few statistics about our organization to provide an overview of the scope and scale of our work and the exigent demands to deliver timely, complete, and accurate information to support clinical decision making at the point of care. These needs are coupled with the demands for business, administrative, regulatory, and other types of information processing and storage to facilitate healthcare delivery. Altogether these needs and demands require increasing reliance on and investment in robust, efficient and secure information systems and technologies that must enable reliable online availability to patients and providers of care.

The Kaiser Permanente facilities include 35 hospitals and 431 medical office buildings. We have physician offices in each of the nine states and the District of Columbia where our physicians practice. In areas where we do not have hospitals, we contract with hospitals to provide inpatient services. Kaiser Permanente physicians also refer patients out for certain types of ambulatory and hospital-based care.

In 2008, Kaiser Permanente had 167,338 employees, including 94,000 union-represented employees; 14,641 physicians; and 40,451 nurses.

That same year there were 36.7 million provider office visits; 547,338 surgeries; 129 million prescriptions filled; 1.1 mammograms performed [1]; and 1.6 million colorectal cancer screenings performed at Kaiser Permanente.

In 2008, 2.7 million members used My Health Manager, Kaiser Permanente's online health record. My Health Manager allows patients to securely access their health records from home, as well as e-mail their physicians, refill prescriptions, make, change, and cancel appointments for themselves or for family members, and view lab results, at no extra charge.

Each month, more than 600,000 secure e-mail messages are sent to Kaiser Permanente doctors and clinicians, more than 1.6 million lab tests were viewed online, and 1.4 million requests for appointments were made online via My Health Manager.

EHRs Serve the Core Mission of Delivering Patient Care

Kaiser Permanente is deeply committed to the use and improvement of our electronic health record (EHR) system, KP HealthConnect™ and supporting ancillary care systems, and we continue to make substantial investments in capital and human resources to improve the performance of our information systems. These systems are essential to our mission to deliver high quality healthcare at an affordable cost. We take seriously our obligations to comply with professional and regulatory standards, laws, and regulations in pursuing this mission.

Care delivery is our focal point for improving the utility of the EHR and supporting ancillary care systems (such as lab, radiology, and pharmacy) and their current and future uses. As an integrated healthcare delivery system, Kaiser Permanente's workflows are extensive, complex, and support a wide variety and volume of information exchanges, both internally and externally.

KP HealthConnect™ and its supporting systems must provide links among office-based and hospital-based physicians in all medical specialties, clinicians, nurses and other health care professionals; labs and pharmacies; quality reviewers and analysts; and researchers across settings of care, within and across our regions throughout the country.

This systems-supported integration of care delivery and care records allows a more complete, detailed picture of the patient's treatment history and status, and also allows for timely coordination of care. Our integrated systems also provide data to conduct research on quality and patient outcomes. These uses provide real and significant benefits to our members, patients, and the communities that we serve.

No EHR or its supporting systems have an infinite capacity to process and store information, and EHR technical capacity is an expensive commodity. Competing demands for new functions or features continuously vie for the limited resources available and test the physical or technological limits of the systems themselves. There

[1] Mammograms performed on women ages 42 to 69 years of age.

are always inevitable choices to be made among competing demands for new specific functions or features, such as processing speed, new reports or views of the patient record, or new tracking and documentation requests. However, the overriding consideration should be the ultimate benefit to the core objective of delivering high quality healthcare services at an affordable cost.

In principle, any demand on the EHR and its supporting systems that can compromise our ability to meet the core objective must be carefully evaluated and provide a compelling business case to decision makers. The business case must demonstrate measurable value to the primary clinical enterprise, patient outcomes, and organizational performance in correspondence with the magnitude of the effort and expense of the demand/request in order to justify investment.

Accountability of HIPAA Covered Entities and Privacy/Security Compliance

Kaiser Permanente takes its responsibility to protect the privacy and security of members' and patients' protected health information (PHI) seriously. We provide protections for individually identifiable information consistent with applicable federal and state laws, regulations, and other professional/industry standards and requirements. To this end, we continue to invest significant resources to implement security and privacy practices.

Our program includes ongoing risk assessment and workforce training, as required by the HIPAA Security Rule, as well as compliance with other required and addressable standards of the administrative, physical and technical security safeguards.

Our privacy and security compliance regimen specifically involves revision of our privacy and security practices, policies and procedures to reflect the new requirements set forth by the American Recovery and Reinvestment Act of 2009—HITECH (ARRA HITECH) provisions and the recently published HHS Interim Final Rule on Breach Notification for Unsecured Protected Health Information.[2]

Meeting these high standards requires transparency and accountability—from our regional Organized Health Care Arrangements to each of its constituent covered entities, including all of our workforce members, and as applicable, our Business Associates.

Kaiser Permanente maintains detailed policies and procedures to implement security and privacy protections over PHI throughout. We periodically inform and educate our members about their privacy rights and our responsibilities.

Our privacy and security framework and procedures include ready processes to enable individuals to exercise their rights under HIPAA and other applicable laws and regulations. We believe the regulatory and compliance framework for privacy and security is comprehensive, extending from federal and state regulators, to professional certification and licensing authorities, and most importantly to individuals who are our members and patients.

---

[2] American Recovery and Reinvestment Act of 2009-Pub.L.No-11, 123 Stat. 115 (2009) Title XIII-Health Information Technology, Subtitle D: Privacy; Breach Notification Rule for Unsecured Protected Health Information; Interim Final rule, 74 Fed. Reg. 42739 (Aug. 24, 2009) (to be codified at 45 C.F.R. parts 160 and 164).

The improved enforcement provisions contained in Section D: Privacy of ARRA HITECH provide clear rights and remedies to persons who wish to pursue administrative relief under the law and regulations, and to States and the U.S. Department of Justice to pursue civil or criminal actions for violations of the federal Privacy Rule. [3]

In addition, the recent Federal Trade Commission's publication of a final rule regarding breach notification requirements for vendors of personal health records (PHRs) that access, handle or maintain personal health information - not considered covered entities under HIPAA and not otherwise subject to the federal Privacy Rule if they are not Business Associates of a covered entity- begin to close the gaps in the protection of PHI.[4]

At this time, the goal of widespread adoption of certified, interoperable EHRs by physicians and hospitals covered by the federal Privacy Rule and other laws and regulations, and the meaningful use of EHRs, can be served without imposing additional, non-value-added compliance requirements for transparency and accountability either for privacy or security compliance.

Disclosure Accounting Imposes Excessive Burdens Disproportionate to Benefits

The new ARRA Accounting of Disclosure requirement that covered entities account for and collect information on each disclosure made through an EHR for the purposes of treatment, payment and health care operations (TPO) requires the Secretary to promulgate regulations regarding the reporting requirements.[5]

We respectfully request that this Committee do the following in support of the promulgation of regulations as required by ARRA:

1. Provide a definition of what constitutes a reportable disclosure;

2. Provide a definition of what it means to use, maintain, and collect protected health information **through** an EHR;

3. Provide a definition of what constitutes an EHR for the purposes of disclosure accounting that is more detailed than the current definition contained in ARRA;

4. Conduct a survey of covered entities to understand the national experience and costs associated with the accounting of disclosures as practiced prior to the enactment of ARRA, and to understand the effect that the new requirement will have on covered entities; and

5. Exempt disclosures as defined under the HIPAA Privacy Rule between covered entities within an Organized Health Care Arrangement.

---

[3] American Recovery and Reinvestment Act of 2009-Pub.L.No-11, 123 Stat. 115 (2009).Title XIII-Health Information Technology, Subtitle D: Privacy, Sections 13409, 13410, 13421.
[4] Health Breach Notification Rule; Final Rule, 74 Fed. Reg. 42962 (Aug. 25, 2009) 16 CFR 318.
[5] American Recovery and Reinvestment Act of 2009-Pub.L.No-11, 123 Stat. 115 (2009). Title XIII-Health Information Technology, Subtitle D: Privacy, Section13405 (c).

Without further clarification as requested above, we believe this requirement will impose significant, burdensome compliance requirements and added, excessive costs on covered entities without producing meaningful benefits to members, patients, clinicians, or regulators.[6] We respectfully request that the requirement be clarified and modified to provide relief in relation to the extreme administrative burden and lack of meaningful benefit.

At the present time, we do not see a clear benefit to patients for whom this new requirement and resulting obligations have been imposed. Neither do we glean from the legislative history any evidence that industry experience and the cost of implementing this requirement were taken into consideration. There is no documented record of an effort to conduct a cost-benefit analysis of any kind or results reported from research that would lead one to arrive at the determination that the requirement serves demonstrated patient needs, rectifies a proven negative industry practice, or satisfies a valuable industry compliance need at any level of regulatory oversight. We do not see a problem that needs fixing.

As an integrated healthcare system, Kaiser Permanente largely provides care within our regional Organized Health Care Arrangements, consisting of multiple covered entities. However, in regions where the care cannot be provided within our system and in our facilities, patients must be treated or referred outside of the Kaiser network for ambulatory or hospital-based care, or for laboratory tests.

These visits and admissions may require the transmittal of PHI from the EHR to another covered entity for the purposes of treatment, payment or health care operations. Under the new requirements, Kaiser Permanente would have to record as disclosures the transmittal of this treatment information to be in full compliance.

Based our very preliminary estimates, the extent of these disclosures as newly defined by ARRA may involve as low as 2%-3% of current out-of-network visits/admissions in the region which has the lowest out-of-network referrals, to as many as 100 percent of admissions for hospital-based care in regions of the country where Kaiser Permanente does not maintain hospitals.

Cumulatively, this may amount to approximately 18%-20% of total annual visits and admissions. Although a rough estimate, this is a non-trivial number that would impose real and substantial costs on Kaiser Permanente and its members.

In addition, depending on interpretations in rulemaking and implementation, routine data exchanges for TPO purposes between covered entities within a single Organized Health Care Arrangement could be considered disclosures and would then be required to be accounted for as well. This would augment exponentially the number of disclosures that an entity such as Kaiser Permanente would need to account for, document, and report in the event a member or patient requested such accounting.

---

[6] Breach Notification for Unsecured Protected Health Information; Interim Final rule, 74 Fed. Reg. 42739 (Aug. 24, 2009) (to be codified at 45 C.F.R. parts 160 and 164).

The Accounting Side of Disclosures

Since the implementation of the HIPAA Privacy Rule in 2003, Kaiser has adhered to the requirements on the recording of disclosures. These disclosures include such items as the reporting of identifiable information to public health agencies, health oversight agencies, law enforcement and others.

With the implementation of the new ARRA requirements, we may be required to account for all treatment disclosures done through our EHR, including all referrals, lab orders, pharmacy prescriptions, and others. Depending on the definitions that we request to clarify what it means to "disclose" PHI "through" an "EHR", the accounting of disclosures could conceivably include payments such as all claims payments, eligibility inquiries and responses, referral authorization transactions, coordination of benefit transactions, etc. as well as all disclosures done for health care operations purposes, including quality assurance, utilization reviews, fraud and abuse, auditing, and others.

The sheer volume of such transactions, the type and amount of information to be captured for each of these disclosures, the granularity of the information required, the development and refinement of information security mechanisms and procedures across our EHR system to identify and document such disclosures, and the allocation of costs and human capital to monitor and ensure such disclosures are being appropriately identified and documented would be a daunting and expensive ongoing endeavor.

Considering that approximately 18%-20% of our annual care delivery activities are performed by organizations outside of Kaiser, when aggregating all of our treatment-related encounters such as medical visits, admissions, inpatient and ambulatory surgical procedures, lab tests, radiology diagnostic and treatment procedures, dental and ancillary services visits, home health and long-term care visits, and pharmacy prescriptions filled, we would need to begin to account for over 60-65 million Kaiser Permanente transactions per year across the organization.

If the definition of a disclosure through a EHR under the new requirement were to include all of our related financial transactions performed for payment purposes for the clinical encounters described above as well as all of the administrative and management transactions performed for health care operations purposes, approximately 80-85 million Kaiser Permanente transactions per year would need to be accounted and stored for possible reporting, that are not so tracked today.

This number could double if we have to account for disclosures between our various covered entities within each of our regional Organized Health Care Arrangement structures.

The overall cost and amount of resources that would be consumed is difficult to estimate, but including human capital that would need to be devoted to first preparing our systems for such a large endeavor, second, maintaining year after year such a system of accounting of disclosures, and third, ensuring that at least three years worth of such disclosures are readily available for reporting could run into the 100s of millions of dollars. The costs of such extensive new technical operations may inevitably consume funds that otherwise would be spent on improving the quality of care.

The Reporting Side of Disclosures

Based on our experience from calendar years 2003 through 2008, and using the more narrow definition of disclosures reportable prior to the issuance of the ARRA HITECH new requirements, we believe that consumer/patient demand for accounting of disclosures today is less than negligible.

Kaiser has recorded fewer than 350 requests cumulatively for accountings of disclosures during that **six year period**. That's approximately 0.00004% of our membership during the six years from 2003 through 2008.

With the implementation of the ARRA accounting of disclosures requirements, we are not able to predict the rate of increase for requests for an accounting of disclosures. Nonetheless, our systems would need to be ready to handle any such requests by the compliance date. Based on our experience as documented above, we sincerely believe that the number of individuals who may request the accounting of disclosures will be very small, and disproportionate to the work effort implied by the requirement as well as to the results that would be produced.

Neither the objective of enhancing transparency nor improving accountability is served by the new accounting of disclosures requirement. We firmly believe that the new requirement if implemented would present a significant diversion of limited capital and human capital resources at a critical stage of EHR adoption and enhancement.

It is possible that this misdirection of resources could be enough to curtail adoption by some organizations due to limitation of funds and staff resources to accomplish the work/rework to satisfy the requirements by the compliance date. At the very least it would represent a material increase in the overall costs of EHR adoption.

Incidence of the Costs of Disclosure Accounting and Barriers to EHR Adoption

If we assume that the requirement as published will not be defined sufficiently to meaningfully bound the reporting obligations on covered entities, then the cost for the required work/rework on EHRs to allow a covered entity to produce the required reporting should not be borne solely by the covered entity. At the very least, there may be a requirement that any vendor offering a qualified certified EHR would have to upgrade and offer existing products to provide the reporting functionality and storage of reports in order to maintain certification.

For physician practices and hospitals that have not yet adopted EHRs, it is highly unlikely that cost-effective reporting, tracking and storage features are readily available in existing products and systems. They will have an earlier compliance deadline to meet without the assurance that products can be delivered at costs that are affordable.

Similarly, the requirement that any vendor who offers a qualified EHR must upgrade and offer the required reporting, tracking, storage functionality for accounting of disclosures may prove to be a limited overall benefit to Kaiser Permanente and to healthcare systems who have already adopted EHRs. Most covered entities, like Kaiser Permanente, maintain a hybrid system of EHRs so the true rework would require the reengineering of vendors' products as well as Kaiser Permanente's legacy and home-grown systems to achieve unification of reporting functionality. Nevertheless, we urge

the committee to consider where the very substantial prospective cost to reengineer existing EHRs and supporting systems can be spread across a broader range of market participants than the lone covered entity.

To implement the new reporting requirements as under discussion today, Kaiser Permanente would need to develop a large program-wide project devoted to the effort. We would have to design and program methods to flag, capture, and store the relevant information involved in the disclosure at each interface and through each system.

Complete redesign, programming, and reengineering associated with producing a report on disclosures would require additional computational capacity, reducing overall transactional speed given our current system configurations and adding materially to existing data center infrastructure requirements. Additional storage space would need to be secured to store the 3 years of accumulated reporting, at further expense to the organization.

At a minimum several hundreds of millions of dollars would be spent to put into place a function and report that would at best be used by a tiny fraction of members for whom no observable benefit of a clinical or privacy nature would result. Neither will Kaiser Permanente benefit from the accumulation of this internal information generated within our regional OHCAs.

Meaningful Use Provisions 2011-2015: Privacy and Security Metrics

Kaiser Permanente supports the further refinement of Meaningful Use provisions associated with the Medicare and Medicaid incentive payments for adoption of EHRs.

Specifically, we recommend that the measure that uses a confirmed HIPAA privacy or security violation as the basis for measuring privacy and security protections of the EHR be revised or eliminated.[7]

We believe that this measure bears no direct relationship to privacy or security protections of any EHR that exists today, or that will exist in 2011, the compliance target date for this and other measures.

The existence of a resolved privacy or security violation settled by OCR may arise from a variety of circumstances completely unrelated to the underlying technical security in the EHR.

At the very least, we suggest alignment of security certification requirements for the EHR as suggested elsewhere by the HIT Standards Committee and its work groups.[8]

---

[7] HIT Policy Committee Meeting, July 16, 2009; Meaningful Use Workgroup, Recommendations, Privacy and Security; revised wording: "recommend that CMS withhold meaningful use payment for any entity until any confirmed HIPAA privacy or security violation has been resolved"

[8] HIT Policy Committee, August 16, HIT Policy Committee, HIT Standards Committee: Certification/Adoption Workgroup Recommendations; Ibid; Privacy and Security Workgroup, Status Report,

We also suggest selected privacy and security standards that apply within an organization be clearly delineated from those that apply for the purposes of health information exchanges—where data leaves the covered entity's internal systems.

It is our understanding that the standards recommended by the Privacy and Security Work Group of the HIT Standards Committee, and approved by the Standards Committee, were adopted primarily to support secure and interoperable exchanges of health information between organizations. At the same time, these standards may apply to the internal operations of a single enterprise. We believe it will be important to clarify when and how those same standards are expected to be applied inside an organization/covered entity to ensure that health information is securely collected, used, maintained and disclosed.

The work of the HIT Standards Committee together with the HIT Policy Committee may usefully coordinate their efforts to consider applicable security standards for the security of the EHR consistent with the overall approach and design of standards certification.

The focus should remain on the objective security features and attributes of the EHR and supporting technologies and not on the administrative or management systems that implement the privacy and security compliance regimen for the covered entity.

Conclusion

Kaiser Permanente respectfully requests that the Policy Committee consider the following in the promulgation of regulations regarding Disclosure Accounting:

- Provide a definition of what constitutes a reportable disclosure;
- Provide a definition of what it means to collect protected health information through an electronic health record;
- Provide a definition of what constitutes an electronic health record for the purposes if disclosure accounting that is more detailed than the definition contained in ARRA;
- Conduct a survey of covered entities to understand the national experience and costs associated with the accounting of disclosures as practiced prior to the enactment of ARRA, and to understand the effect that the new requirement will have on covered entities using the definitions to terms requested above; and
- Exempt disclosures as defined under the HIPAA Privacy Rule between parts of a single Organized Health Care Arrangement

Without further clarification as requested above, we believe the new Disclosure Accounting provisions of ARRA will impose significant, burdensome compliance requirements and added, excessive costs on covered entities without producing meaningful benefits to members, patients, clinicians, or regulators.

We respectfully request that the requirement be clarified and modified to provide relief in relation to the extreme administrative burden and lack of meaningful benefit.

Furthermore, Kaiser Permanente recommends that the Meaningful Use measure that uses a confirmed HIPAA privacy or security violation as the basis for measuring privacy and security protections of the EHR be revised to account for the troubling issues mentioned above, or eliminated.

Thank you for your attention, and we look forward to working with you to achieve the goals of the Office of the National Coordinator.