Testimony of

Scott Morgan

Executive Director and National Privacy & Security Officer
on behalf of the

Kaiser Permanente Medical Care Program

to the
U.S. Department of Health and Human Services and the Office of the National Coordinator's Health Information Technology Policy Committee Privacy and Security Tiger Team

Virtual Hearing on Accounting of Disclosures

September 30, 2013

Thank you for inviting me to participate in today's hearing. I am Scott Morgan, Executive Director and National Privacy and Security Compliance Officer at Kaiser Permanente.

I am testifying today on behalf of the national Kaiser Permanente Medical Care Program, the largest integrated healthcare delivery system in the United States, which provides comprehensive healthcare services to more than nine million members in nine states (California, Colorado, Georgia, Hawaii, Maryland, Ohio, Oregon, Virginia and Washington) and the District of Columbia. Thus, while we were invited to be on the payer panel, our perspective includes providers as well.

Kaiser Permanente is committed to delivering high quality health care through an integrated delivery system that comprises physicians, hospitals, and health plans**.** As part of our commitment to high quality care, Kaiser Permanente has made a significant investment in developing a secure Electronic Health Record ("EHR") system, KP HealthConnect®, to support the delivery of care, and enhance communications among providers. Kaiser Permanente also conducts and supports a broad agenda of health research. In our research efforts as well as in our delivery of health care, we provide protections to safeguard patient health information against unauthorized use and disclosure.

HITECH Balancing Test
As an overarching framework for our comments, we look to the balancing test prescribed in HITECH that considers both the interests of the individuals in learning about disclosures of their protected health information and the administrative burden on covered entities that must account for disclosures, including those previously exempted involving treatment, payment, and health care operations (TPO).

In our experience, very few individuals request an accounting of disclosures;[1] when they do, their requests focus on specific concerns rather than a desire to see all disclosures or a listing of every access to their PHI. Access log data may be quite extensive and not designed for reporting. Considering how rarely individuals ask for reports and how few instances of inappropriate access or disclosure are discovered, the added benefits to consumers seem small compared to the added cost to automate both TPO disclosure accounting and access reports. The administrative burden would far exceed the actual demand and ultimately would divert valuable, scarce resources that could be devoted to improving patient care.

We have determined that the cost of system upgrades alone to support both the new accounting of disclosure requirements and the access report (not counting the additional

[1] As an example, Kaiser Permanente's Northern California Region, serving over 3 million members, receives approximately 16 requests for disclosure/access information per month. Some requests are withdrawn by the requesting individual after follow up inquiries revealed that the individual wanted something else – generally a copy of the EHR.

labor and technical support) for *only one of our eight regions* would exceed HHS's published estimates of the total cost across all covered entities in all states.

Thus, while it may be possible over time to build the technological capability to track all disclosures for TPO and to provide access reports, we question whether that effort would balance the benefits to consumers and the burdens to covered entities.

One of the goals of this hearing is to gain greater understanding about currently available, affordable technology that could provide more transparency about how PHI has been used or disclosed.

Kaiser Permanente has already implemented robust tools to monitor system access. We institute strong access controls to ensure only the appropriately authorized individuals can access defined categories of each patient's PHI. We have also established alerts to monitor and report instances of inappropriate access, as well as a variety of proactive deterrent mechanisms, including physical, technical, administrative, and policy safeguards to protect PHI.

Because we have already implemented these processes and tools, we are able to respond to specific questions or concerns that patients have about suspected inappropriate uses or disclosures. We believe building additional system capabilities to track internal uses and disclosures of PHI to meet the proposed access report regulations would not lead to justifiable improvements or greater transparency.

One question that is especially important for Kaiser Permanente as an integrated delivery system involves patient expectations regarding certain uses, access, and disclosures.

Integrated Delivery Systems
Kaiser Permanente is an integrated system encompassing clinicians, inpatient and ambulatory facilities, diagnostic services, laboratories, pharmacies as well as health plans and research centers. In each of our regions, the different legal entities represent an organized health care arrangement – or "OHCA," as defined under HIPAA.[2] The HIPAA

[2] *See* Section 164.103 (paragraph 2):

2. An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:
   i. Hold themselves out to the public as participating in a joint arrangement; and
   ii. Participate in joint activities that include at least one of the following:
      A. Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
      B. Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
      C. Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities

Privacy Rule designates exchanges of PHI between OHCA participants as disclosures rather than internal uses. Until HITECH, disclosures of PHI between OHCA members for TPO purposes have been exempted from the accounting requirement. HITECH will now require accounting for a much larger number of disclosures than under the current Privacy Rule, which exempts TPO disclosures from accounting. Because of this consideration, we recommend that exchanges between OHCA components be exempted from the accounting of disclosures requirements.

Kaiser Permanente members' PHI is routinely shared among legal entities within our integrated model (e.g., between Health Plan and Hospitals, between Hospitals and Medical Groups, etc). In our integrated model, much PHI resides on electronic systems that are shared by multiple entities within the OHCA. Retrieval of information from these systems can be considered a "use" rather than a disclosure.

We do not believe that excluding these technical disclosures from an accounting report would raise any genuine issue of privacy or defeat the purpose of removing the exemption. We believe that individuals expect entities within an OHCA to share PHI for purposes of managing and coordinating their healthcare, as outlined by the OHCA's shared notice of privacy practices. In an OHCA based on an integrated delivery system like Kaiser Permanente, joint activities are so extensive and frequent that many records are routinely used or disclosed to support various activities, including disclosures between the OHCA members for TPO.

As the preamble to the HIPAA Privacy Final Rule states, "a key component of these [OHCA] arrangements is that individuals who obtain services from them have an expectation that these arrangements are integrated and that they jointly manage their operations." It follows that these individuals would also have an expectation that the covered entities in an OHCA also share PHI for TPO, and therefore no need for an accounting about those disclosures made between OHCA entities. Our members and patients understand and expect that information is shared for TPO. For instance, when medication is prescribed, it will be obvious to the patient that the Permanente physician shared PHI with the Kaiser Permanente pharmacy and health plan when the patient arrives at the pharmacy, is charged the correct co-pay and picks up the prescription.

The number and complexity of disclosures within each OHCA are far greater than for most covered entities. Because of our integrated nature, we have more shared systems that would fall within the scope of the proposed regulations; even though a request for an accounting may be made to one Kaiser Permanente covered entity (e.g., a Kaiser

---

through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

Foundation hospital), it would entail disclosures to many other Kaiser Permanente covered entities, like physicians, labs, pharmacies, and health plan.

Our members and patients see us as a single organization. They have the expectation (and we have the responsibility for ensuring) that our providers will have the right information at the point of care. An accounting of all of the TPO disclosures that occur as a normal part of care delivery and health plan operations within Kaiser Permanente would be voluminous and likely innocuous to the very few patients or members who may request it, because most disclosures in an accounting would be internal to Kaiser Permanente.

Disclosures between integrated OHCA participants should be expressly excluded from an accounting of disclosures requirement, regardless of the purpose of the disclosure. Without that exemption, the proposed requirement would impose a disproportionate burden on an integrated delivery system holding itself out as a joint arrangement – that by design encourages additional appropriate disclosures among providers to promote coordination and quality of care.

Also, we recommend that the reporting of disclosures for TPO purposes should be flexible, and allow for aggregating repeating disclosures.

Another goal is greater understanding about how covered entities and business associates currently deploy record access transparency technologies.

Access Reports
We fully support an individual's right to ensure that his or her PHI is not accessed inappropriately, but we believe the access report proposed in the May 2011 NPRM is not the right solution. There are more effective, less expensive methods for responding to privacy concerns that utilize currently implemented technologies and procedures, instead of requiring the substantial system remediation that would be needed to achieve the proposed access report requirement. Because of the broad scope of the proposed rule, creating an access report would require capturing and translating very granular data recorded in the normal course of care delivery and reimbursement, but also build the capability to record the purpose of each access. As we note below, access reports would likely be enormous, resulting in less, not more, transparency, because critical information would be buried within large amounts of data.

In our experience, the size of these reports can be unexpected and overwhelming for individuals, even for a targeted inquiry. Typically, access logs we have prepared run 60-100 pages, but for inpatient logs, reports can run 1,000 pages or more. In a specific example that involved a 2-3 week hospitalization, the access report was over 2,000 pages long. As a test, we ran a series of random access reports based on just one year of data from the EHR alone. The average report size was about 500 pages. We have found that providing this information to patients tends to create confusion, even when supplemented by resource-intensive one-on-one review of the log. Patients do not recognize most of the names on the report (there can be several dozen names, especially for hospitalization

records, because of the many instances of legitimate access to PHI by physicians, nurses, technicians, clerks, labs, pharmacies, etc.). Also, patients may not understand that many instances of access involved very limited data, like the few record fields that a registration clerk can see.

When individuals suspect inappropriate access, an investigation by the covered entity will be able to provide more detailed, reliable and responsive information, in a proper context and at a lower cost than an access report. We are concerned about the potential that a lengthy access report may overwhelm the consumer and erode the trust relationship between provider and patient. No other service industry in the country is expected to produce such detailed and granular data upon consumer request.

Patients have a right to make sure their PHI is protected, but the effort and expense to automate and support access reports is unnecessary. Better information can be produced through investigation, which is more patient-centered and capable of delivering information that is tailored to an individual's specific concerns. Therefore, we recommend investigation as an effective alternative to an automated access report.

The proposed rule also raised some other issues.

We have concerns about disclosing the names of all individual employees who have accessed or received a patient's PHI. Giving a list of names and dates in lieu of conducting and summarizing a targeted investigation is not a good way to respond to privacy concerns – and in fact, raises a new set of issues related to employee privacy. Providing the names of individuals who access PHI may subject those individuals to privacy intrusions and safety concerns (and potential liability issues when employees of business associates are involved).

We recommend that if names are provided at all, they be limited to those already identified in the individual's initial inquiry. If the requesting individual provided no name(s), then only entity names should be given in responding to an inquiry.

In summary, we have the following recommendations:

- Provisions for accounting of disclosures should be revised to meet the balancing test in HITECH.
- Exempt disclosures between integrated covered entities within organized health care arrangements from the accounting requirement.
- The access report requirement should be dropped.

Thank you to the Tiger Team for the opportunity to provide this feedback. I would be happy to respond to any questions.