September 25, 2013

Mr. Omar Rehman
Center for Transforming Health
MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

Re: Written Testimony for Virtual Hearing on Accounting of Disclosures

Dear Mr. Rehman:

Intermountain Healthcare appreciates the opportunity to submit written comments in advance of our testimony in the September 30, 2013 virtual hearing.

Intermountain Healthcare is a not-for-profit, community-based integrated healthcare delivery system headquartered in Salt Lake City, Utah that operates 22 hospitals and more than 185 clinics. Intermountain has approximately 34,000 employees and has about six million patients in our longitudinal Electronic Health Record (EHR). SelectHealth, Intermountain's health insurance company, covers more than 500,000 individuals. Intermountain employs approximately 800 physicians and has another 2,500 affiliated physicians who practice at its facilities. Intermountain is recognized for its success in the provision of high quality, efficient clinical care. Intermountain is also recognized for its pioneering work in the development and use of clinical information systems, which are critical in enabling the provision of this efficient, high quality care.

Thank you for the opportunity to participate in this virtual hearing and for the opportunity to provide this written testimony to the ONC Security and Privacy Tiger Team.

Sincerely,

Jutta Williams
Chief Privacy Officer, Intermountain Healthcare
801.442.1505 (office)
jutta.williams@imail.org

CC:

Marc Probst, Chief Information Officer, Intermountain Healthcare and Member, HIT Policy Committee

Stan Huff, MD, Chief Medical Informatics Officer, Intermountain Healthcare and Member, HIT Standards Committee

Accounting for Disclosures Virtual Hearing September 30, 2013
Questions for Panelists and Responses from Intermountain Healthcare

Goal 1: Gain a greater understanding of what patients would like to know about uses, accesses, and disclosures of their electronic protected health information (PHI).

1. What are the reasons patients may want to learn who/what entities have used, accessed or received their PHI as a disclosure? What are the reasons they might want to know about internal uses or accesses?

   Intermountain Answer: The Intermountain corporate compliance privacy office provides oversight for all privacy related inquiries, concerns or complaints received from patients and employees at our 22 hospitals and 185 clinics. It has been our experience that patients, with rare exception, are interested in requesting an investigation of access and are not interested in learning about routine uses or routine disclosures of PHI. Most (over 90%) of investigation requests include a specific user suspected of inappropriately accessing or sharing PHI.

2. What information would patients want to know about such use, access, or disclosure? For example, is it important to know the purpose of each, or the name or role of the individual involved?

   Intermountain Answer: It has been our experience over 12 years of performing privacy investigations in response to patient concerns that patients not interested in the name of each individual, but they are interested in understanding whether information was used or accessed appropriately or inappropriately. They want to know that a complaint was thoroughly investigated and appropriate action taken in cases of inappropriate access. Intermountain does not reveal the name or title of employees involved in HR related actions to the patient complainant generally. Patients in general have not expressed dissatisfaction with this practice and we have not experienced requests by patients for information on how information has been appropriately accessed or used for routine treatment, payment or hospital operational purposes.

3. What are acceptable options for making this information available to patients? (report, investigation, etc.)

   Intermountain Answer: Intermountain supports informing patients about investigational outcomes in a general sense though we do not believe that employee names or private HR related actions should be detailed. Should inappropriate access be identified as a part of an investigation request, breach notification processes provide important information to patients about the nature of the incident and what it means to them. Note, however, that breach notification rules do not require inclusion of employee names.

4. If there are limitations to the information about uses, accesses or disclosures that can be automatically collected given today's technologies, what are the top priorities for patients?

Intermountain Answer: It is very challenging to develop systems that can convert security logs into a human readable report. It requires integrations between user identity management systems, patient indexing services and the systems performing access logging. No system we have evaluated can add contextual information like the "purpose" for the access today.

It has not been our experience that patients seek a list of employees who have accessed their record. Rather, patients want to be able to understand if a specific, unauthorized access occurred. A patient reading such a report will not be able to derive context or purpose for access even if HR title were to be included. The goal of transparency is to provide clarity. It is Intermountain's position that currently available technology will not answer the question of "why" only the question of "who" as it relates to employee access. We do not believe that without purpose or context, current technology delivers information that provides patients transparency.

The information available from inquiry audit logging – which we must highlight is not universally available in clinical systems - does allow a trained professional to identify those users who have accessed records and with whom further discussions might be necessary to validate that access was appropriate. Context and purpose for access, in our environment, requires human evaluation and is not available using technical tools alone.

5. If patients have a concern about possible inappropriate access to or disclosure of their health information, what options currently are available to address this concern? What options should be developed for addressing or alleviating that concern?

   Intermountain Answer: Investigation of inappropriate access to or disclosure of PHI in our environment relies on a number of tools and processes. We utilize security audit logs and data correlation tools to identify potentially inappropriate access and then conduct in-person interviews to understand the purpose for access. Unfortunately, not all clinical applications deliver inquiry (read) level access logging at the patient record level.

Goal 2: Gain a greater understanding of the capabilities of currently available, affordable technology that could be leveraged to provide patients with greater transparency re: use, access, or disclosure of PHI.

1. What capabilities are currently used to enable transparency regarding (or to track or monitor) each use, access, or disclosure of PHI? To whom (and for what purpose) is this information communicated?

   Intermountain Answer: Some functions within a hospital are not as automated as others. With regard to access that occurs within mature information systems like our proprietary EHR systems, we can track and monitor uses and disclosures by analyzing inquiry audit level security logs though this data is kept only for13 months. However, many disclosures that are allowed without a patient authorization like those made as required by law (e.g., patient overdose reporting to the State of Utah) or those performed as permitted for the purpose of public health reporting (e.g, CDC survey disclosures) are often performed using database queries rather than by directly accessing a patient record. For database queries, access to and

delivery of specific patient data is not logged at the individual record level but rather is limited by current database technology to only record the query script itself. This does not help us identify individual patient data disclosed as part of a query. For the disclosures that use database queries, analysts must manually prepare and deliver spreadsheets to the privacy office. For some CMS reporting not related to direct payment, for example, our Quality department manually prepares and delivers a spreadsheet each quarter that includes all patient record data delivered to meet quality measure reporting requirements.

For individual patient record requests that do not require an authorization such as those that are delivered in response to a subpoena or court order, Intermountain tracks and monitors each request and record delivery by manually inputting data into a proprietary release of information application.

2. If you currently do not track each user that accesses a record internally along with the purpose of that access, what would it take to add that capability from a technical, operational/workflow, and cost perspective? What would it take to add that capability for external disclosures?

   Intermountain Answer: Inquiry (read) access is tracked for some systems but not for all. Many legacy systems cannot accommodate the processing impact that turning on such functionality, even with the existence of the underlying software code – which is not assured since this is not required by law. We inquired of the cost associated with developing such code for one of our more modern systems that is considered part of our Designated Record Set. The supplier responded that they would be happy to deliver a solution as a consulting arrangement and suggested that such services would cost on the order of $3M to complete. We estimate that in order to upgrade all systems considered part of our Designated Record Set as proposed would cost Intermountain upwards of $100M to complete.

   Many legacy systems could not be upgraded to meet such a technical requirement and would need to be replaced should this level of auditing be mandatory. Intermountain would encourage regulators to consider the importance of the flexible approach within the Security rule for other, addressable security requirements. Not all systems are capable of meeting all requirements; in this case we urge ONC and OCR to consider making an auditing requirement addressable such that older, less sophisticated, and lower risk systems may implement a reasonable and appropriate control.

3. Is there is any "user role" or other vehicle that can be utilized to distinguish an access by in internal user from an external disclosure? Can it be determined, for example, that the user is a community physician who is not an employee of the healthcare organization (IDN or Organized Health Care Arrangement (OHCA))? If not, what are the obstacles to adding this capability?

   Intermountain Answer: Potentially; if read-level auditing is available and a user serves in one capacity or the other, an access might be defined as either by an employee or by a non-workforce member. However, many of our users wear multiple hats so it is not simple to understand what role they are serving at a specific point in time. It is easier to establish

policies for how to flag access for non-OHCA users – who would presumably have less reason to have direct access to patient records in any case.

4. Does the technology have the capability to track access, use, or disclosure by vendor employees, like systems' administrators, (for example, who may need to occasionally access data in native mode to perform maintenance functions)? Do you currently deploy this capability and if so, how?

   Intermountain Answer: For some high-risk systems, this functionality is enabled to track all access; however, it does not natively determine the employment status of a user so does not automatically make a differentiation between a use or a disclosure. This determination would require use of a separate security audit management software product which is not widely employed in the healthcare industry today.

5. Are there certain uses, access, or disclosures within a healthcare entity that do not raise privacy concerns with patients? What are these uses and disclosures? Can the technology distinguish between these others that might require transparency to patients?

   Intermountain Answer: Typically those uses and disclosures made for routine treatment, payment and hospital operational purposes are not of interest to patients. A patient receives notice of how information will be used and disclosed for these routine purposes. Importantly, a number of transparency-related rights afforded to patients have been augmented and/or created since the Access Report was proposed in May 2011, including a more detailed notice of privacy practices statement, specific criteria for notifying patients of a breach of their PHI, and the delivery of records and care team information through Meaningful Use Criteria.

6. Do you have the capability to generate reports of access to, uses of, and disclosures from, a medical record?

   Intermountain Answer: Yes for a very limited number of systems; particularly for the systems we consider part of our legal electronic medical record. However, this report does NOT generate and could never generate an understanding of why a record was accessed.

   - How frequently are the reports generated, and what do they look like?

     Intermountain Answer: Intermountain has shared a copy of such a report. It is voluminous and confusing. An access report for one patient for one month from one system was nearly 900 pages long. When shown to patients, this report was identified as confusing and useless.

   - How granular are these reports? Are they detailed by aggregate data categories, individual type of data, or individual data element, or in some other way?

     Intermountain Answer: We have built our reporting to be granular in nature so we can use it as an investigative tool. Reporting can be built to be aggregated by data categories

(i.e., all clinical notes rather than a specific clinical note) however, it cannot be aggregated across multiple systems with our current technology. Even these aggregated reports, however, cannot derive context or purpose for access. They can be used only to support an investigation, not to complete one.

- Can they be generated automatically, or do you use manual processes?

  Intermountain Answer: Some portions of the report can be created automatically but others require highly manual processes that includes hours of human assessment and evaluation.

- Do you integrate reports across multiple systems?

  Intermountain Answer: No. We prepare separate reports from different systems. There is no standard for how audit data is created so each system requires a custom report to parse and convert the proprietary system log data into a human readable format.

- What is the look-back period?

  Intermountain Answer: We retain 13 months of data. We store and must process approximately 70 million security logs per month. While data storage may be relatively inexpensive, processing and correlating larger quantities of data is not possible with our current hardware and software.

Goal 3: Gain a greater understanding of how record access transparency technologies are currently being deployed by health care providers, health plans, and their business associates (for example, HIEs).

1. How do you respond today to patients who have questions or concerns about record use/access/disclosure? What types of tools/processes would help you improve your ability to meet patient needs for transparency regarding record use/access/disclosure? Have you ever received a request from a patient (or subscriber) that requested a list of every employee who had access to PHI?

   Intermountain Answer: We conduct a thorough investigation that begins by running access reports for those systems that have inquiry audit logs available. If access is identified that appears to be inappropriate or if a specific user was identified by the complainant and access by that user is identified, an interview is conducted by a privacy official assigned to that user's facility. A strict sanction policy is applied for all inappropriate access. Notice is provided to the patients as appropriate. For those investigations that result in no findings of impropriety we inform complainants. With rare exception, our patients appear satisfied with this process.

   In 12 years, we have had one request for a list of everyone in our workforce who had looked at this patient's record. We have never been asked for a list of everyone who has accessed

(internal uses and external disclosures). In speaking with the patient about his concern and purpose for asking for such an access report, he identified that his request was aimed at collecting proof of inappropriateness to use as evidence in a civil action involving his ex-wife, our employee. Our offer to conduct an investigation into his ex-wife's access and notify him of the outcome of our investigation seemed to satisfy the patient.

2. What types of record use/access/disclosure transparency or tracking technologies are you deploying now and how are you using them?

   Intermountain Answer: We have just signed a contract with a firm to replace our aging, home-grown tools used to report on access to our EMR. In our integrated health care delivery system that serves millions of patients our legal electronic medical record systems include about four distinct systems compared to the much larger number of systems included in the very broad designated record set definition. While we hope that new systems will be able to monitor access within more systems than our current systems, we do not believe that integration with the >30 systems classified as a DRS will be possible even with the new tools. We are also investing in new security tools for our Enterprise Data Warehouse to improve tracking for database queries to PHI.

3. For transparency, what do you currently provide to patients regarding use/access and disclosure, and do you see any need to change your current approach?

   Intermountain Answer: It has been our experience that thorough investigations of patient privacy concerns or complaints provide the best form of transparency for patients and employees who feel something inappropriate may have occurred. The current AOD report for non-routine disclosures has been identified by patients as having less value, but is another form of reporting that we plan to continue to provide. Based on the positive track record we feel we have with our patients, we do not see our approach changing unless required to do so.

4. Do you have any mechanisms by which patients can request limits on access? For example, if a patient had concerns about the possibility that a neighbor employed by the facility might access his/her record; is there a way for this to be flagged?

   Intermountain Answer: This is a very challenging thing to accomplish technologically and we have investigated the feasibility of doing such a thing. To prevent access, it would require that our EMR and likely other commercial products add access control lists to each patient record. As a detective control, it is possible to prepare an access report on a periodic basis to flag access as inappropriate after such an access has already occurred. The detective, rather than preventative method, is how commercially available tools that monitor patient access function today.

Goal 4: Gain a greater understanding of other issues raised as part of the initial proposed rule to implement HITECH changes.

1. Regarding access reports, what information do you collect besides the basic information collected in an audit log?

Intermountain Answer: We collect identity information and demographic details (like home address) for employees and patients so we can derive answers to questions like are they neighbors. We also collect time-card information and conflict of interest information to identify whether employees are serving in secondary roles when accessing information. We collect patient encounter histories to identify if a patient was seen in a facility on or around the time of an access event. We also collect and correlate payment related activities to help explain why revenue cycle employees may be accessing information on patient encounters. There are many other sources of information that help us to derive as much knowledge as possible about the potential purpose or context for an access event prior to sending out an interview request. Interviewing employees about access when it is appropriate has a negative impact on morale so we attempt to find any and all information to explain an access event and reduce false positives in our proactive audit processes.

2. What would be involved in obtaining access information from business associates? Do current business associate agreements provide for timely reporting of accesses to you or would these agreements need to be renegotiated?

   Intermountain Answer: It would be very challenging operationally to collect information in a timely way. It would also be arguable that we have a right to ask for this information. Our agreements require access to investigate security incidents and data breach concerns. We also require timely reporting of inappropriate accesses and to account for disclosures to other 3rd parties. However, it would be challenging to require delivery of access information for appropriate internal uses under current BAA terms and conditions. Renegotiation would be necessary.

3. What issues, if any, are raised by the NPRM requirement to disclose the names of individuals who have accessed/received copies of a patient's PHI (either as part of a report of access/disclosures or in response to a question about whether a specific person has accessed)? What are the pros and cons of this approach?

   Intermountain Answer: We feel the proposed right to an access report introduces a new and significant threat to the safety of Intermountain's healthcare workers. Intermountain has made a risk-based decision to not include last names on our badges in order to limit our employees' exposure to potential harm or harassment by patients. By requiring access reports to include the names of employees, the NPRM exposes the named employees to risks, particularly in rural areas, of being tracked down.

   Intermountain has an obligation to protect its employees from unnecessary harassment. Further, Intermountain feels strongly that a court order should be required to supply employee names in cases of both appropriate and inappropriate access. Accordingly, Intermountain feels that employee names should not be included in a patient- requested access report. Because of the lack of contextual information in an access report that explains why a healthcare employee may have accessed a record, a patient may feel justified in contacting the healthcare employees directly to ask why they saw the patient's PHI. If a patient raises a privacy concern based on an AOD or access report, then the covered entity

should be responsible for investigating that concern for the patient and reporting back to the patient. This gives us the opportunity to address patients' concerns, make any needed adjustments to our privacy processes, and take appropriate disciplinary action.

In addition, an increasing number of Intermountain's investigation requests relate to domestic or civil disputes. On many occasions, Intermountain's privacy-compliance investigators become de-facto enlistees in supplying evidence in legal cases. One of the reasons we do not name employees involved in breach notification letters today, which we are not required to do under current law, is to limit the degree to which investigation requests provide evidence in legal actions. Intermountain suggests that the prime beneficiary of an access report containing employee names would be litigants.

The proposed access report would have significant adverse effects on state peer review immunity and the conduct of quality improvement activities. Many states have enacted laws that protect healthcare employees from litigation when performing investigations, surveys, audits and other business activities to improve healthcare quality. The purpose of the immunity, of course, is to encourage providers to improve healthcare quality without the fear of litigation. Intermountain relies on this immunity to conduct quality improvement projects that have directly resulted in both reduced costs and better clinical outcomes for our patients. In recognition of Intermountain's use of information technologies and its data-driven quality improvement projects, President Obama honored Intermountain as a leader in providing quality care at low costs during his 2009 address to a joint session of Congress on healthcare.

The NPRM would provide attorneys a "back door" to uncover more detail about the reason or purpose for access, thereby nullifying any privilege or immunity for quality improvement projects. While a covered entity could request a protective order from the court to protect these projects and their data, the covered entity's administrative burden to do that would be significant.

The NPRM would increase litigation costs as attorneys and litigants seek to obtain copies of detailed access reports. And because the access report provides little information about the purpose of the access or what part of the record was accessed, a follow-up deposition or subpoena seeking more detailed information would likely follow an access report request. In an extreme case, an attorney could choose to interview all persons who had accessed a patient's record for information. So both these added fees and the added risks to the safety of healthcare workers argue against adoption of the access report provisions of the NPRM.

4. How do you think current mechanisms to allow patients to file a complaint and request an investigation regarding possible inappropriate uses or disclosures are working? Could they be enhanced and be used in lieu of, or in addition to receiving a report?

   Intermountain Answer: We believe this would be a very reasonable approach to providing patients with transparency. We have conducted such investigations for 12 years with very favorable feedback from the patients we have been able to help.

   - Should entities be required to do such an investigation – if so, what should be the scope?

Intermountain Answer: If a patient provides vague or incomplete information about their concern, it diminishes our ability to investigate. If patients were to be afforded such a right, it would be necessary that we receive some specifics before we can investigate a complaint – either a specific period of time during which access may have occurred, a specific location where an inappropriate event occurred, or a specific employee of concern should be supplied to ensure we can investigate the complaint.

- Should entities still be required to produce a report if the patient wants one?

  Intermountain Answer: No. The report requirement is fundamentally flawed and represents a safety risk to employees. Given the costs involved and the lack of value to the patient, the access report does not appropriately meet the patient benefit/provider burden balancing test required by the statute.

- What recourse does the patient have if he/she is not satisfied with the response?

  Intermountain Answer: If the patient feels that a covered entity has not met its obligations to investigate and respond appropriately, they have the right to appeal to OCR. While we agree that OCR is not a customer service oversight organization, we believe the OCR is best suited to evaluate if a covered entity has established a fair and appropriate process for investigating privacy complaints.

- What options do entities have if patient's transparency requests cannot be honored?

  Intermountain Answer: If it is not feasible to accommodate the patient, we can seek guidance from OCR to identify an appropriate response.