Testimony of Jeremy Delinsky, Chief Technology Officer, athenahealth, Inc.
Privacy and Security Tiger Team Virtual Hearing Regarding Accounting of Disclosures
September 30, 2013

Co-chairs Ms. McGraw and Mr. Egerman and members of the Tiger Team, I greatly appreciate the opportunity to provide testimony to inform your deliberations on the implementation of HITECH policies and the standards for the accounting of disclosures.

As you know, athenahealth, Inc. ("athenahealth") provides electronic health record ("EHR"), practice management, care coordination, patient communication, data analytics, and related services to physician practices, working with a network of over 40,000 healthcare professionals in every state. All of our providers access our services on the same instance of continuously-updated, cloud-based software. Our cloud platform affords to us and our clients a significant advantage over traditional, static software-based health IT products as we work to realize our company vision of a national information backbone enabling healthcare to work as it should.

General Remarks

We agree that a practical approach to providing patients with greater transparency about the uses and disclosures of their digital, identifiable health information is necessary step toward greater patient engagement. We disagree, however, that transparency for transparency's sake is necessarily a desired outcome. Members of the Privacy and Security Tiger Team, as well as the broader policy community, should begin by addressing a crucial threshold question: will providing patients with accountings of disclosures mitigate the risk of improper access, use and disclosure of patient information in the age of digitized health information?

Based on our experience responding to patients inquiries about access to health information, we believe that patients do not want, nor are they well-served by, an exhaustive accounting of all access, uses, or disclosures of their health information. Effective transparency of use and disclosure information must be meaningful to the patient audience. Inclusion of the entirety of the uses and disclosures related to treatment, payment, and operations inhibits transparency by overburdening patients with business processes that they may not understand and potentially burying truly improper access information. Accounting of disclosures reporting should be focused on the provision of user-friendly audit reports that provide patients with details of specific accesses, uses, and disclosures outside the scope of standard health care operations.

It is extremely important to understand the volume of information that would be included if an accounting of disclosures report for a typical patient contained every access, use, or disclosure of protected health information ("PHI"). The volume of information is staggering, and the resources needed to produce such a report are prohibitive. We estimate that a typical patient will generate between 500 and 1000 unique "touch points" where PHI is accessed per encounter. Each of these seemingly basic tasks may have several line items in an access report:

> front desk staff performing check-in; a practitioner documenting vital signs, the physician documenting the exam; an import of medication history to perform reconciliation; the physician electronically ordering prescriptions; the physician sending a referral for a consult with a specialist; the physician closing the record and signing off on the exam at the end of

the day; a coding specialist entering billing codes; a claims representative from the payer processing the claim; follow up on a denial by a billing specialist; and the physician reviewing the results of the specialist consult.

The magnitude and granularity of this information would overwhelm most patients, obscuring instead of revealing any instance of improper access.

Further, patient demand for a comprehensive accounting of disclosures is low. While this could be due in part to a lack of patient knowledge regarding their rights to obtain this information, in our experience patient requests are more likely to stem from specific concerns rather than a desire for a full scale audit. These specific concerns can be best addressed by more specialized reporting.

Given this low demand, athenahealth's current process for delivering a comprehensive report is largely manual. The data set required to document the access, uses, and disclosures of PHI for the over 40 million patient records on our platform is too large to host in a single environment; a comprehensive accounting of disclosures requires review of multiple securely hosted systems. Accommodating even a small influx of such requests would stifle business innovation by diverting developmental resources from other initiatives to address onerous reporting obligations. Furthermore, to accommodate complete transparency of data for on-demand patient review in one system would require a complete overhaul of our current infrastructure at an extremely high cost, without a clear patient benefit.

Transparency will not be established by requiring a large volume of additional data points, such as the purpose behind each use, access, and disclosure. Given the individualized approaches to managing patient records by providers, tracking the purpose behind each clinical decision would be difficult to standardize. Logistically, to accurately identify this information would require providers take additional steps to explain their medical decision making processes at every step of the caregiving process. This is unlikely to provide complete transparency, however, not least because the process would be controlled by those who may be behaving improperly. Another approach would be to develop vendor automated logic based on a set of inferences about the purpose behind each action taken. Such logic could be inaccurate, however, as the inferences would be based on expected and compliant workflows rather than suspicious behavior, and such misinformation would be forwarded to the patient in an accounting of disclosures.

In order to achieve worthwhile and meaningful transparency, accounting of disclosures must be meaningful to patients. This objective cannot be met if we they are provided with indecipherable audit logs of thousands minor demographic edits, claim follow-ups, provider reviews, and similar routine, necessary, and proper instances of data access.

Responses to Specific Questions

1. **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? (Goal #1, Question #5)**

Patient concerns regarding possible inappropriate access to or disclosure of health information can be addressed in a variety of ways depending on the nature of the request. Our health care

provider clients have access to audit reporting functionality that can report on all modifications made to patient information at the user or patient level. Additionally, our system automatically records access information, including page views and access denials. All available access information is monitored by our security team. To pull a comprehensive report of all uses, access, and disclosures in the system, however, is extremely burdensome as it requires manual review and aggregation of information spanning across a variety of systems.

In addition to the onerous nature of compiling a comprehensive report, we have found that providing such detail to the patient provides little value because the information presented is not intuitively understandable. A patient could not understand the details of such reporting without also having a deep knowledge of both practice and internal athenahealth workflows. As a result, we believe the best functionality to address concerns related to inappropriate access or disclosure of health information would be the creation of user-friendly audit reports that provide patients with higher-level information on how their records have been disclosed, though creating such functionality would be complex and resource-intensive.

2. **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? (Goal #2, Question #1)**

athenaNet, our cloud based platform, contains an active audit log which records the actions of all users, including use or disclosure of PHI, and we also maintain a separate audit log that tracks every time a user accesses PHI but does not take action. Users with proper role-based access can view details of the audit log that tracks action taken on our platform at any time. As a result, when either our health care provider clients or athenahealth employees note a discrepancy in a particular workflow, it can be reported and all actions can be reviewed by all affected parties. Hard copies of audit information can be shared through a chart export, but compiling the log of actions taken and access-only log is a time-intensive manual process, and the resulting report is nothing more than a spreadsheet with hundreds or thousands of rows of data that would be difficult if not impossible for the average patient to parse.

Beyond this transactional based review, our Information Security team monitors internal employee actions, while practices on athenaNet are responsible for managing the logs related to their entities actions and reporting their concerns to athenahealth directly. Any suspicious activity noted by athenahealth is individually reviewed and reported to the client as necessary.

3. **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? (Goal #2, Question #2)**

While our platform does track user access, it does not articulate the purpose of each access. Requiring the purpose as part of an accounting and disclosures report would pose challenges to both vendors and providers. We believe that there are two options by which purpose could be tracked in a vendor system.

First, vendors like athenahealth could be required to build functionality to capture the purpose in current workflows. This would place an enormous burden on providers who would have their patient encounters frequently interrupted with a notice requiring them to state the reason for

their use or disclosure of PHI. Such a burden would undermine a primary goal of federal incentive programs intended to increase the adoption and use of health information technology, by inhibiting and complicating rather than streamlining and simplifying provider workflows. Furthermore, such a requirement would require all athenahealth employees to clearly document the purpose behind their access whether it is for claim review or in an effort to review the existing functionality for enhancements unrelated to the data contained on the page. Allowing providers and employees to track their purpose for every access would provide an overwhelming volume of data points for the patient, and it would not be entirely effective in the instance of suspicious behavior, because the person accessing the information could falsify their underlying purpose.

The second option for gathering this information would be to place the responsibility to infer the purpose of disclosure on the vendors. Although we could infer purpose in many cases—for example a claim or claim attachment would presumably be disclosed for payment purposes—this method would not be 100 percent accurate, resulting in incorrect information given to patients.

Similarly, since we can track all actions taken within athenaNet, disclosures such as printing, faxing, and e-prescriptions can be identified. athenaNet also includes functionality that allows providers to manually document any disclosures made by them within the patient record. Creating an additional functionality to internally track the purpose behind each external disclosure would cause the same concerns as tracking the purpose behind each access, and would either be extremely burdensome for the provider or result in potentially inaccurate inferences by vendors.

4. **Is there is any "user role" or other vehicle that can be utilized to distinguish an access by an 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 OHCA)? If not, what are the obstacles to adding this capability? (Goal #2, Question #3)**

Our platform distinguishes all user access at an organizational level. To ensure security, technical firewalls have been established between all organizations. In addition, once on the platform, clients can further differentiate users in a variety of ways, including organizational affiliation, department, position, role, and position at the entity. Internally, system access and permissions for athenahealth employees are distinguished based on employee demographics and credentials. Thus, if a practice were to grant access to a community physician who is not an employee of the healthcare system, the platform could identify all actions taken by that specific user. Practices are responsible for the provision and monitoring of third party access in compliance with their legal obligations.

Additionally, while our platform can monitor certain types of disclosures by identifying when information has been sent outside of athenaNet, the purpose or end recipient of such information is not always detectable. Adding such a capability would require that providers log all steps taken by those outside of their entity after the disclosure.

5. **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? (Goal #2, Question #4)**

Yes, our platform has the capability to actively track access by our own employees, as well as access by our vendors. Any vendor given access to athenaNet goes through our corporate Vendor Management Program review, and vendors are granted only the access necessary to complete their role. All vendor access provisions are reviewed quarterly.

6. **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? (Goal #2, Question #5)**

In our experience responding to requests from our provider clients and their patients, uses, access, or disclosures related to treatment, payment, and healthcare operations do not generally raise privacy concerns with patients, as they are an expected part of the healthcare process. Required privacy notices given to all patients by providers clearly articulate how entities use and share information as well as patient rights. Additionally, PHI is used, accessed or disclosed for treatment, payment and healthcare operation purposes tens, if not hundreds of times as a result of a brief and basic physical exam. Most patients would be completely overwhelmed by the amount of data they would receive in an accounting of treatment, payment and healthcare operations uses, access and disclosures. For the average patient, finding a potentially concerning atypical use, access or disclosure of PHI among this immense volume set of routine PHI uses would be the equivalent of finding a needle in a haystack.

Distinguishing treatment, payment, and healthcare operations related uses and disclosures is difficult, however, and would require immense provider engagement (see number 3, above).

7. **Do you have the capability to generate reports of access to, uses of, and disclosures from, a medical record? (Goal #2, Question #6)**

We do have the capability to generate reports of access to, uses of, and disclosure from a record within athenaNet, but it is not an automated process, as explained below. Depending on the scope of the request, gathering such information is extremely resource intensive and would take the time of our developers away from other important tasks, such as building functionality for the Meaningful Use Incentive Program or further enhancing our interoperability with other EHR systems.

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

Reports are only generated in response to specific requests. To create a comprehensive report of access to, uses of, and disclosures from a medical record requires a chart export. This process entails copying and pasting all access, uses, and disclosures associated with the patient chart into a spreadsheet. As a result, depending on data elements, a patient could receive an excel spreadsheet with an innumerable amount of technical information in thousands of cells.

- **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?**

The reports can be extremely granular, returning millions of data points, as all changes to patient information within athenaNet are tracked within the audit logs. For example, rather

than noting one access from a provider to complete a patient exam, the report could list separately all changes to specific patient information (e.g., weight, height, etc.), all new notes, all new prescriptions ordered, all new diagnoses, and so forth within that particular encounter. Reports can be detailed by either aggregate data categories, individual types of data, or individual data element based upon the specific request.

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

Currently, a comprehensive report cannot be generated automatically. Given the low patient demand for such information and the fact that automating this process would be a resource-intensive long-term task, there has been no reason to automate the creation of such reports.

- **Do you integrate reports across multiple systems?**

We have not built a tool to integrate reports across multiple systems, since we only maintain and our clients only access one platform. To integrate with other systems used by our clients would require a manual collection process that would be completed by our health care provider clients or our employees. The "interoperability" of the data and reports from disparate systems could be a substantial challenge.

- **What is the look-back period?**

We do not have a specified look-back period for reporting. We allow our health care provider clients (on their own or on behalf of their patients) to request any information accumulated while utilizing our platform.

8. **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? (Goal #3, Question #1)**

We have never received a request from a patient or subscriber to list every employee who had access to PHI. Patients are more concerned about "out of the ordinary" uses of their PHI, meaning uses that are not part of treatment, payment or healthcare operations. We have only ever received one request, from a third party audit and not a patient, asking us to provide a list of every username, including our internal employees, who access PHI.

In fact, patient requests for an accounting of disclosures are extremely rare. Our current process involves working directly with our health care provider clients to determine the necessary information and parameters of the report on an individualized basis. Our health care provider clients have the ability to run reporting that specifies which athenahealth employees accessed patient information.

It would be wrong to assume that simply because patient information is now electronic it is easy and beneficial to patients to produce full accountings of access, use, and disclosure. Patient privacy concerns would best be met with user-friendly reports that patients can readily understand, but patients also need education regarding how their information is used and how many times it may be used in the course of ordinary treatment.

9. **What types of record use/access/disclosure transparency or tracking technologies are you deploying now and how are you using them? (Goal #3, Question #2)**

In addition to extensive user auditing protocols outlined above, we have established internal policies regarding appropriate access, use, and disclosures of patient information. All employees are trained to identify best practices and annually certify to their understanding of requirements including the need to report any suspicious behavior they encounter.

10. **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? (Goal #3, Question #3)**

With regard to the comprehensive use/access/disclosure reports, we currently respond to one-off client requests with a largely manual process. The demand for such reporting is so low, we see no reason to change that approach.

We also provide our health care provider clients with access to auditing tool meant to identify specific suspicious events related to actions or modifications made within our platform, though this tool is not meant to provide a full accounting of uses, access, or disclosures (running such comprehensive reports—potentially millions of data points, depending on granularity—runs the risk of extending the platform beyond our server's capacity).

Finally, access issues are also tracked in a user event log report. This report can identify the actions of any user, including access attempts, actions taken, when access was denied, and password changes.

11. **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? (Goal #3, Question #4)**

Yes, our platform currently includes mechanisms by which patients can request limits on access. For example, our EHR allows providers to restrict access to certain patient charts. Similarly, all privacy notices requested by a patient can be flagged on the patient record within our platform, viewable to all users.

12. **Regarding access reports, what information do you collect besides the basic information collected in an audit log? (Goal #4, Question #1)**

Beyond basic information such as user information and time and date of access, we can audit on a variety of events including almost all changes made not just within a patient chart, but within our platform on the whole. For example, beyond all actions taken by specified users, we can also identify details such as utilized IP addresses and referring provider information.

13. **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? (Goal #4, Question #2)**

Our Business Associate Agreement does not specifically require that business associates provide us with access information. Instead, all business associates are required to implement appropriate access controls in compliance with HIPAA requirements. Additionally, business associates are required to make all internal practices available and provide access at our request to ensure thorough review of any uses or disclosures of patient information by the business associate.

14. **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? (Goal #4, Question #3)**

To compile a report that discloses the names and individuals who have accessed or received copies of a patient's PHI would require extensive provider and vendor communication. Providers would have to track and document all disclosure information directly into the system in any instance that it was not sent directly through our interface (for example, if a provider wrote a prescription on paper rather than ordering it electronically through our system, we would have no way to track that disclosure unless a note was made in our system by the provider). Additionally, all access information would have to be manually compiled by our employees. This would be extremely time-intensive and burdensome, taking developer time away from other projects and the resulting patient benefit may be minimal. Responding to a specific request regarding whether one person has accessed a patient's PHI would be much less burdensome.

Conclusion

It is important that we continue to prioritize transparency for patients among the many health IT policy objectives, but it is equally important that we do so in a well-planned and intelligent way that augments, rather than detracts from, the many other important health IT and health reform goals, and that provides useful access for patients to meaningful information. Thank you very much for the opportunity the engage on this important topic.