September 25th, 2013

HIT Policy Committee – Privacy and Security Tiger Team:

Epic appreciates this opportunity to provide testimony related to accounting of disclosures and access reports from electronic health records. We are an electronic health records (EHR) developer that creates software that will be used by over 200,000 physicians when all current implementations are complete. Our software offerings include features for access logging during both clinical and non-clinical workflows and an integrated module for capturing and reporting on disclosures. Our testimony is based on our experience of developing and implementing EHRs and is focused on the technical and usability implications of this proposed rule.

Vendor Perspective, Question #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?

Types of Access

Our software offerings include features for access logging during both clinical and non-clinical workflows and an integrated module for capturing and reporting on disclosures. When discussing access logs, it is important to note the different types of EHR data access that can occur:

- **Deliberate Access**: A user deliberately accesses a patient's information by searching for the patient by name, by medical record number, or some other method. With deliberate access, the user is aware that he is accessing that patient's record.

- **Incidental Access**: A user sees patient information incidentally while completing other work in the EHR, such as a physician running population-based reports, nurses or billing workers using a list of patients to plan and prioritize care or work, or IT staff troubleshooting unexpected system behavior. In these cases, a small amount of similar patient information appears for a large number of patients.

The software is designed so deliberate accesses of patient information are logged and could be included in a report with little burden on the covered entity. However, areas of the system where incidental accesses occur are typically designed to use other security measures to effectively protect patient information.

Access Logging and Disclosures

Security and compliance professionals perform audits and investigate claims of inappropriate accesses using access log reports. These reports are often voluminous. Storage of access logs commonly takes up more than 50% of an organization's reporting database capabilities. While clinical audit trail features are enabled by default and cannot be disabled, healthcare organizations fine tune what types of other events are most useful to their investigations to meet their needs and avoid expensive data storage of information they are not using.

Many users of our EHR also use the software's integrated disclosure logging module. This module is used in multiple workflows in both a manual and automated fashion. For example, a medical records user would use the disclosure logging module to document that a records request had been made including who has made the request and for what purpose, to select which portions of the patient's medical record will be provided (particular visits, provider notes, medications, etc.), to create a copy of those portions of the chart in the requested format, and then to track the date at which the copy is provided.

The module can also be configured to automatically record a disclosure when particular actions occur in the EHR. For example, when a summary of care document is transmitted via our interoperability platform to another health care provider using a different system, a disclosure is logged automatically. Because the interoperability platform is used to exchange records for the purpose of treatment of the patient, the purpose is logged in the disclosure as treatment. Over time, we anticipate adding to the software similar automatic logging for other transmissions, such as case reports to specialty registries.

Automatic logging of transmitted data is not typically used in interface-based exchanges of data between the disparate systems a single organization may have in place (EHR, Lab, Radiology, Registration, Billing, etc.).

A list of patient disclosures, whether manually or automatically logged, is available to Health Information professionals on demand. These users can produce the accounting of disclosures to fulfill patient requests as needed. Users of our software tell us that they rarely if ever receive requests for an accounting of disclosures. More commonly, patients contact them with concerns regarding particular users (neighbor, ex-spouse, or other acquaintance) accessing their record inappropriately. These requests can be better served by a security or compliance professional performing an investigation and reporting their findings to the patient.

To summarize, healthcare organizations using our software store the information they need to perform security and compliance investigations. Given the low volume of requests, the voluminous quantities of data in an access log, and the effort necessary for a patient to parse such a log, organizations consider having their staff perform the investigation the most prudent course.

Vendor Perspective, Question #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?

External Disclosure

Purpose is recorded when the integrated disclosure logging module is used. Purpose can be logged manually by the user. When a disclosure is logged automatically, the purpose is recorded by default based on knowledge of the workflow triggering the disclosure.

The software does not distinguish when a system access could be considered an external disclosure because the user accessing the system is not part of the covered entity owning the EHR. These accesses are logged in the access log and audit trail, but not in the disclosure log.

Capturing Purpose for Access

Purpose is not captured along with each access to the patient record.

In order to properly answer this question we have contemplated adding such a capability. The challenges of such a capability are illustrated with the following examples:

Example 1: User performing multiple functions related to his role

One approach to capturing a purpose that we have considered is to infer a purpose based on the user's role and the information they use within the system. For example, could a physician user accessing a patient's lab results be assumed to be providing treatment to the patient?

While such an assumption might be true a large portion of the time, a physician user could also look at a patient's chart while performing peer review of another physician's work, while monitoring the overall quality of their clinic or group, or while investigating a question the patient had about his bill.

A secondary problem with inferring based on user role and information accessed is that not all information has as clear of a purpose as lab results. The primary use of lab results is likely treatment. But is the primary purpose of a quality dashboard, for example, treatment or operations?

Even if great regulatory flexibility is permitted in inferring a purpose, and allowances are made for situations where the wrong purpose is inferred without penalizing the healthcare organization, the approach presents configuration challenges. Each organization creates custom forms, views, reports, and other screens within the system. To match up user roles, system uses, and infer a purpose in each case would be a large mapping project for healthcare organizations.

Doing this proactively does not seem worth the effort when the volume of requests is low and it can be investigated retrospectively by a Health Information professional as needed.

Example 2: User performing multiple roles

Yet another challenge with inferring the purpose is that it is common for workers in some areas to take on multiple user roles. The manager at a small family practice clinic will often perform tasks related to scheduling, billing, and other operations. He covers the front desk area checking in patients as they arrive, often entering the patient's record and updating patient registration data. After the visit has ended, he might enter the record to print a visit summary and schedule follow-up visits. Later in the day, he might review billing data for previous visits ensuring that the proper charges were captured. Using a default purpose per user fails to capture accurate reasons for access and ultimately provides little if any benefit to the consumer of the access log.

Documenting a Purpose on Access

The challenges with inferring a purpose lead to consideration of prompting the user for their purpose upon each access to a patient record (or each portion of a patient record, as we have established that the same user can have multiple purposes).

Users' days and workflows can be so varied that they are the only reasonable source for a purpose for their actions. From an operational/workflow perspective this would be extremely onerous. Some potential impacts:

- **Delay.** End user workflow would be continually interrupted by prompts asking for purpose, potentially delaying patient care.
- **Inaccurate**. Purposes would need to be well codified and easy to understand. Even if the choices are very clear it will be typical that the end user would simply pick the first or easiest option, quickly making the data meaningless.
- **Usability.** Users have given feedback that such prompts would be extremely frustrating interruptions to their workflow.

Vendor Perspective, Question #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 OHCA)? If not, what are the obstacles to adding this capability?

Internal users and external users are not distinguished in the software today. Community physicians and physician employees of a healthcare organization are likely to have similar user types because they need access to similar types of information and tools within the EHR.

Distinguishing employees and external users in the system seems feasible. However, we are very concerned that if external users are expected to log a purpose upon each access to the system, that this is extremely impractical for the reasons cited in the earlier question.

Dual Employment

If attempting to distinguish employees from external users, note that some users do work as both external entities and as employees of the health system, and have a single login used in both capacities. Users would be frustrated if expected to use different logins. For example, users specify their own preferences within the system and would consider it a usability issue if they needed to do this twice for each preference.

Access vs. Disclosure

We would like to raise a larger question of whether the distinction of employees of the covered entity and community physicians is a priority. If a health system extends their system to family practice clinics whose users would be considered non-employee community physicians, it is hard to imagine that that family practice physician's patients would consider their doctor's access to provide primary care as an external disclosure. We urge an approach that focuses on existing audit logging available to such shared systems and does not consider certain users as disclosure recipients.

Vendor Perspective, Question #6

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

- **How frequently are the reports generated, and what do they look like?**
- **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?**
- **Can they be generated automatically, or do you use manual processes?**
- **Do you integrate reports across multiple systems?**
- **What is the look-back period?**

As mentioned above, the system can generate access log reports as well as patient disclosure reports. Access logs and disclosure reports are separate mechanisms that are not combined into a single output.

- **Frequency & Appearance**: Both access reports and patient disclosure logs are generated on demand. Organizations tell us they seldom or never need to generate these types of reports to present to a patient. They do typically use the access log reports to perform necessary audits. Access logs contain: date/time, user, action, and optionally activity.

Disclosure logs contain: date, recipient, purpose, type of data released. Organization analysts can modify how these reports appear to suit their individual needs.

- **Granularity**: Aggregate data category.
- **Generation**: Automatic, though would require manual combination if a single report of both accesses and disclosures is necessary.
- **Integrated**: No.
- **Look-back**: Configurable. Clinical audit trails cannot be deleted. Typically healthcare organizations never purge disclosures. Organizations set an access log retention period in compliance with state laws and their security needs.

We hope this testimony is helpful. We also urge consideration of our comments on your Proposed Rule (Ref: 45 CFR Part 164, RIN 0991–AB62) issued on May 31, 2011. I have attached our commentary for reference.

Eric Cooper
Epic
1979 Milky Way
Verona, Wisconsin
ecooper@epic.com

Appendix A: Excerpt of Original Comment

We have carefully reviewed the proposed rule, and we support your efforts to limit the documentation burden on physicians and other EHR users. We understand that you proposed the Access Report as a compromise intended to alleviate some of the burden on covered entities discussed in previous requests for information on disclosures. We appreciate this effort and agree that any modifications to HIPAA disclosure requirements must be a proper balance of expanded patient rights and limited burden on covered entities. However, discussions with organizations that use our software have included significant concerns with the proposed Access Report, indicating that as written, the rule would require major changes to software (both EHR and other systems), policies, and hardware investments.

We believe that the discrepancy between the proposed rule's expectation of minimal burden and the concerns of organizations using our software can be attributed to two main reasons.

- First, the proposed rule incorrectly assumes that the current HIPAA Security Rule requires all accesses to information to be logged; when in practice, current systems employ a variety of security measures to protect patient data. This proposed rule seems to add an unintended burden of requiring significantly more access logging by covered entities than is currently used.

- Second, the expansion of the access report requirements beyond disclosures made "through the EHR" (as HITECH is limited to) to all uses of information throughout the entire designated record set increases the burden by including vastly more systems to a complex new requirement for which many systems were likely not designed.

Our response is based on our experience of developing and implementing EHRs and is focused on the technical and usability implications of this proposed rule.

Unclear and Potentially Unreasonable Access Logging Requirements

We have discussed this proposed rule with a number of organizations using our software, and we have identified two possible interpretations of the access logging requirements based on statements such as the following:

> *"We believe that this is reasonable since all such covered entities and business associates are required by the Security Rule to maintain access logs and, therefore, should be able to provide this information to individuals in response to requests. We believe that the administrative burden on*

covered entities who are complying with the HIPAA Security Rule will be reasonable, in light of their existing obligation to log access to electronic protected health information."

This statement can be interpreted in two ways:

1. Upon request, the covered entity must now provide the patient with a report of the access log information that the covered entity is currently collecting. The covered entity does not need to implement additional access logging features where that covered entity has determined that other security features protect the data more appropriately and efficiently in accordance with the standards set forth in the Security Rule.

2. The covered entity must implement access logging features for all uses and disclosures of electronic health data, including areas of the system where the covered entity, using the standards defined in the Security Rule, has determined that access logging is not necessary to sufficiently protect the data, and provide this information to the patient on request.

We consider the first interpretation to be most in line with the proposed rule's stated goal to provide patients with more information while limiting the burden on covered entities. If you decide that the final rule must include some form of the Access Report requirements, we recommend that the final rule affirm this interpretation.

However, to ensure that the final rule does not impose extensive burdens, we are framing our comments based on the more burdensome second interpretation. We are concerned that these requirements would make it exceedingly difficult for a covered entity to be compliant with HIPAA and also use an EHR. The level of difficulty would be so high as to provide a disincentive to further adoption of EHRs and a challenge for covered entities currently using an EHR.

Examples Where Patient-Level Access Logging is Not Practical

In this letter, we will make the distinction between two types of accesses to EHR data:

- **Deliberate Access**: A user deliberately accesses a patient's information by searching for the patient by name, by medical record number, or some other method. When doing a deliberate access, the user is aware that he is accessing that patient's record.

- **Incidental Access**: A user sees patient information incidentally while completing other work in the EHR, such as a physician running population-based reports, nurses or billing workers using a list of patients to plan and prioritize care or work, and IT staff troubleshooting unexpected system behavior. In these cases, a small amount of similar patient information appears for a large number of patients. (We've included detailed examples in the following sections.)

Many deliberate accesses of patient information are logged and could be included in an access report with little burden on the covered entity. However, areas of the system where incidental accesses occur are often designed to use other security measures to effectively protect patient information. Consider the following specific examples.

Example 1: Population Management and Outreach

A physician runs a report to review his diabetic patient population so that he can provide outreach to patients in poor control of their condition. The report might include the patient's most recent hemoglobin A1c result, LDL cholesterol, weight, age, and other basic information. If the physician has a large diabetic population, hundreds of patients might appear in this report each time it is viewed.

When reviewing the report, the physician sorts on the recent lab results and observes one patient whose results indicate her diabetes is in poor control. The physician opens the patient's chart to review her condition and recent treatments in more detail. When he deliberately opens the patient's chart to review her entire record, his access is logged.

For the remaining patients on the list, the physician observes that their recent lab results indicate their condition is being well controlled, and he takes no action. Because he likely runs this report frequently, it's unlikely that he made decisions on any of these individual patients while reviewing the report but rather that he made a decision to take no action on this population of patients as whole. Access is not logged for these patients.

In this example, the covered entity employs several measures to protect patients' privacy:

- It controls access to the population reporting feature of the EHR to only appropriate users, who must authenticate themselves when logging in.
- The entity's security staff periodically reviews reporting activity in the system, such as which users are running which reports and how frequently. Security staff cannot see what patient information is revealed to each user when they run those reports, but staff can follow up if any suspicious uses of reporting features are detected.
- When the physician deliberately opens the individual patient's record to review the full chart or to place a follow-up order, the physician's access to the patient's chart and order placement is recorded in the access log.

This scenario demonstrates how a covered entity might comply with the HIPAA Security Rule without logging access to all electronic PHI in the designated record set. In this scenario, the information needed to generate the Access Report would be collected for only the subset of patients who received outreach from the physician. The information of the other patients included in the report is protected by the standard authentication and security features of the EHR.

When considering what information would be of most interest to patients, the patient would likely find a report containing a list of people who deliberately opened his chart of more use than a report that included likely thousands of additional incidental accesses from users who might have seen only a small subset of his information. These patients might be misled by seeing the physician on an access log, since the physician did not actually review their full chart or make any deliberate action or decision.

Physicians have also shared with us that they are particularly concerned about the responsibility implied by being listed in the access log for all patients in the report because they did not fully review the patients' information or make decisions on any patient as an individual.

Example 2: Lists of Patients

In a hospital setting, nurses commonly use a home screen that shows a list of patients on their unit. This list might include information such as the patient's name, age, and principle diagnoses for admission. Nurses log in and out of the system frequently as they move from the nursing station to patient rooms. Because of the high login frequency, this patient list is accessed hundreds of times by each nurse on each shift. If access logging is enabled for this feature, hundreds of individual accesses would be recorded for each patient from each nurse on the unit.

The hospital in this example secures patient information by requiring users to authenticate themselves when logging in and by limiting access to information on patients in the unit to only appropriate users. When a nurse is caring for a particular patient and documenting in that patient's chart, access logging of the nurse's activity is also used.

Similar activities occur in scheduling offices, billing offices, and other areas of the covered entity. For example, a billing worker might work from a list of patients that displays minimal information for a large number of patients. If access logging were to be required for incidental accesses, each time the billing worker returns to the work list (which occurs hundreds of times each shift), additional accesses would need to be logged for each patient in the list.

Example 3: Technical Support

To support the system, various IT personnel (either from a covered entity or from a business associate providing software support) might need to access the data in the system directly (by which we mean using a method other than through the ordinary end-user interfaces for which access logging occurs) to troubleshoot issues, implement upgrades or patches, or perform other support activities.

For troubleshooting or resolving other system support issues, IT personnel might generate and review lists of data from multiple patient records to discern which data elements or combination of data elements are causing the unexpected system behavior. As is the case with the reports and lists described in Examples 1 and 2 above, the IT staff member might see

isolated amounts of PHI for many individuals. Depending on the method used to analyze and troubleshoot the data, patient-level access logging might not be used.

To secure the patient's information from inappropriate access by IT personnel, the organization limits access to the system support direct data access means to only the necessary IT support members and requires a unique authentication code to access the system in this way.

Brief Additional Examples

In an effort to limit the length of our response, we will briefly summarize other areas of the system where access logging can be problematic:

- Data sent through an electronic interface to business associates. For example, an organization outsourcing claims coding might send data directly from their system to the billing system of coders. While this example clearly is an electronic disclosure, it would still require access logging for an extremely large number of records.

- Extracts of large amounts of data. Organizations extract data from their EHRs for numerous purposes. Some examples:

    - For use by the covered entity. An organization might extract all orders, lab results, charges, and other key pieces of clinical or financial data to a data warehouse or other reporting database. Depending on the uses of this data, covered entities might or might not consider them part of the designated record set. It's unclear whether the extract of the data to that system would require an entry in the access log. Requiring such a log would vastly increase the size of the access log and the patient access report leading to the same issues as described in our previous examples.

    - For use by business associates. An organization might outsource part of their billing process, such as insurance or self-pay follow up. As in the previous example, the volume of the data is a concern. Also, it is unclear whether it would be considered a non-electronic disclosure (and thus be excluded from the accounting of disclosure because it is for payment purposes). If it were considered as electronic disclosure and thus need to be included in the access report, it would lead to similar concerns as previous examples.

    - Compliance with state or local regulation. For example, organizations might send billing information to government agencies to allow those agencies to identify trends or set cost and reimbursement levels. Additionally, they might send patient-identifiable data for quality measure reporting.

Burdens of Implementing Patient-Level Access Logging in These Examples

Expense

While the size of a single access log entry is negligible, the cumulative number of entries generated in these areas of the system would flood the access log with information. In response, the covered entity would need to undertake the financial burden of increasing their data storage capacity. The expense of storing this huge volume of data outweighs the limited value of the information.

Other security measures effectively protect patient data in some areas with fewer burdens

To protect patient data in general and avoid the data storage burden of extensive access logging, organizations will commonly implement the following measures (and likely other measures):

- Train employees on general security and HIPAA policies.
- Enforce sanctions against employees that violate HIPAA.
- Verify credentials of new employees before providing access to the system.
- Implement physical security measures to ensure both workstations and servers are secure.
- Configure workstations to automatically logout after a period of inactivity.
- Implement strong password policies, such as complex passwords, frequent changes of the password, and locking out of a user after a number of incorrect attempts.
- Complete detailed security audits.

Increasing the volume of access logs reduces their usefulness

As shown in example 1, it would be difficult to discern deliberate accesses to information from incidental accesses (such as through a population-based report based on the minimal information in the Access Report). If the access report is flooded with incidental accesses the access log becomes a much less valuable feature. When writing the final rule, we urge you to consider whether these incidental reporting accesses (which are of comparatively less value to deliberate accesses where the user looked up the specific patient's record) are worth this negative impact. We strongly feel that the small benefit is not worth the impact.

Not all access to information can be logged

Even if access logging were enabled in all areas of the system, the log would not provide a complete list of all people who viewed the patient's information. Healthcare is often a collaborative process and several users might view information on the same workstation at the same time while discussing a patient's care. Because only one user can be logged in, that user is the only person who is captured in the access log. With scenarios such as this, even if access information were logged every time patient information appears on the screen, the patient would still be unable to definitively know whether a person not listed in the access report saw his information.

Our Recommendation: Eliminate or Vastly Reduce the Scope of the Access Report

Given the confusion around what is intended to be included in the proposed Access Report and the potential for the requirements to have vast scope and extensive burden on covered entities, we urge careful reconsideration of the Access Report and the underlying assumptions in the proposed rule.

If the proposed rule intends to add additional access logging requirements for covered entities, such as in the examples we have described above, then we are significantly concerned that this rule would place excessive burdens on all healthcare providers. The proposed rule states that there are situations where access logging is overly burdensome (as in the case of paper records), and we suggest that the final rule provide consideration for areas where electronic access logging is also too burdensome. Additionally, we feel that such extensive access logging would make the Access Report less useful for patients because it would be more difficult for patients to discern who deliberately accessed their information.

We recommend that any inclusion of an Access Report in the final regulation include explicit exclusions for the following instances:

1. Incidental viewing of a patient's information that is seen and reviewed in conjunction with similar information of other patients, such as in reports and patient lists.

2. Viewing of a patient's information by IT personnel that is for system support activities and that does not occur through channels for which access logging ordinarily occurs.

We note that other security measures (including physical and administrative, as well as technical measures) can be employed by covered entities to protect patient privacy violations with respect to such activities.

Closing Thoughts

We strongly urge caution when implementing any access report requirements to ensure that burdens are not unintentionally placed on organizations and physicians who are using the capabilities of EHRs to provide better care for their patients. To avoid unnecessary burdens, we feel the best approach would be to define a very narrow scope for any new disclosure or access report requirements and to expand that scope only after thorough research and evaluation is completed on the impact that expanding the scope would have on healthcare effectiveness, cost, and security.

We suggest further research and analysis on the following points:

- The volume of accesses that would be included in the report for each type of access that you would want to include. Understand the implications of recording access when a single action shows small amounts of data for many patients.
- The frequency that each volume of accesses occurs. A small volume of accesses that occurs every few minutes can be more troublesome than a large volume that occurs monthly.
- The capability of current hardware and software to process and store the volume of data that would be generated.
- The number of systems that would be commonly included in the designated record set beyond the EHR system and the effort required to combine the data from potentially dozens of systems into a single access report for a patient.

Again, we appreciate the intent of OCR to limit the burden on covered entities. However, we want to make sure that the access report requirements do not require covered entities to invest unreasonable technology resources to capture and store additional access log data for all patients, when that data likely provides little value for a very small number of patients who request it.

Our comments cover concerns related to the feasibility of the Access Report proposal from a technical perspective. We also urge you to carefully review the comments submitted from healthcare organizations that describe additional administrative and operational concerns regarding these requirements.