Accounting for Disclosures Virtual Hearing

Cerner Corporation Response

September 26, 2013

Cerner Corporation appreciates the opportunity to provide testimony to the Tiger Team on the accounting of disclosure requirements outlined by the ARRA HITECH statute and as proposed by the Office of Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS). We have been asked to comment from an ancillary system perspective. Where possible, we are trying to present the state of the market considering legacy ancillary system portfolio and our experience with what we have observed in the market. We focused on specific questions from the list given to panelists that we felt most germane to ancillary systems for our testimony. As we use the term in our comments, we take access to mean any online access to ePHI. We use the terms use or disclosure to have the same meanings as they do in HIPAA regulation.

We summarize our observations as follows:

- Ancillary systems may serve both as contributor systems to a consolidated reporting for the access report or accounting of disclosures when in a hospital or large ambulatory provider setting or they may be the main clinical system in a provider setting such as a independent reference lab or diagnostic imaging center
- Legacy systems will have been implemented with usernames/IDs, security roles, event types/names for ePHI accesses and event meta data by whatever manner they exist in those systems – consolidation and normalization of these references will require post processing that will be time and labor intensive to develop a singular reporting to the patient
- Consideration also must be given to external business associates who perform diagnostic testing on behalf of the ancillary department that may also need to be incorporated into access reporting/accounting of disclosure reporting (e.g. independent reference labs)
- Some information like purpose of use may only be able to be implied from other meta data
- Ancillary system log data may be drawn from several potential log sources – security audit logs, clinical result report distribution logs, interface logs, public health submission logs and files and possibly other sources
- Informing the patient of machine operations common to ancillary systems such as for interfaces between an LIS and diagnostic instrumentation may not be value to the patient and only serve to be confusing. Clarity is needed on what OCR proposed as to including logging of machine operations and server to server events and activity but we believe focus on natural person end user accesses is the key.
    - Inclusion of additional meta data in the reporting such as source system or device ID/IP address/point of access can help provide the patient information on how their information has been propagated throughout the enterprise

- Best practice guidance on the process of consolidating log data into a singular report that addresses normalizing security identities, roles, operations and data types will be essential in implementing the access report/accounting of disclosures requirements

1. **Goal 2, 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?**

   Ancillary systems such as an RIS or an LIS need to have the ability to both function as self-contained or to contribute data to a more centralized security audit function depending on the implementation context. In some situations such as for an independent reference lab or a diagnostic imaging center, the LIS or RIS may be the main clinical system in use. In a hospital or large ambulatory provider clinic context, they may be in the role of a contributor to an overall security audit function. Considering legacy system inventory, there are several potential source logs that should be considered for the different purposes defined by HIPAA for logging and reporting for both what OCR has defined in their NPRM as the access report and the accounting of disclosures.

   - Distribution logs of routine diagnostic test reports that are generated out of the system. These audit trails include information about when the distribution occurred, to whom it occurred and in what format they occurred. There usually is no explicit why, and the "user" may have been the server or entity distributing the information and not a human. The format of the report could indicate the what, and to some extent, the why of what was distributed. These audit trails may be temporary in nature and persisted for a period of weeks or months, and would require configuration changes or would have to be moved to longer term storage to be persisted.
   - Access or security audit logs for HIPAA Security – these audit trails should contain meta data about the user identity and role, the event, the application function/task used, the operation performed, the patient record and data type accessed, the point of access or machine used (e.g. IP address, network ID) among other information. These audit trails usually will not contain explicit information about why information was accessed or about the party receiving the disclosure as that is usually presumed to be the user, and not a third party. The "why" may be implicit through information such as the user's role, the application task, the data type and the operation performed (e.g. using a result entry task as a medical technologist for a micro data type). The information about what was accessed may contain metadata such as internal OIDs or identifiers or clinical data types accessed. These audit trails may be maintained separate in log files or within data tables present within the ancillary system. The ability to harvest data from them for reporting purposes such as for the access report or accounting of disclosures may be based on what the system can provide for audit reports or extracts. This information may require manual extraction to generate on demand for contributing to a centralized reporting function for the access report.

- Interface audit trails of transactions that involve outbound interfaces to other entities or for diagnostic testing instruments – these audit trails may involve logging of whole transaction data as they are principally intended to support the integrity of the transmission of the transaction in case retransmission is needed, and would not serve as a good long term retention source for disclosure logs. More useful to the purpose would be some manner of disclosure event audit log that included metadata about the interface event.
- Submission files or logs for reporting of information on reportable public health data. These often will be large batch submissions of records. Logging may be quite limited to information about the submission event, and retention of information about included patients may require "shadow" runs of the qualifying criteria for the submission or retention of the submission set to support reporting for the purposes contemplated by ARRA HITECH and the OCR. Compilation of that information in a specific patient context may require significant effort to review submission logs and data files.

2. **Goal 2, Question 2 - 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?**

   Said another way, this question asks can the system tell the difference systematically between an employee user and a business associates such as contractors using the system. One must acknowledging constraints that come from existing systems in use and whether or not they have been implemented in such a way that any available means are in place useful to tell employees from business associates. It would seem that at a surface level, two mechanisms could serve this purpose. User roles could be if they were defined to distinguish employee roles from contractor roles. User account IDs or usernames might also be able to be able to be used for this purpose. Other metadata such as the facility association of the user, machine or IP address that was the point of access, location of the user or other user attributes likely are not terribly useful as the contractor may be on site and even in a similar labor role as an employee. The usefulness of any role or identity based mechanism depends on whether or not it has been implemented in the portfolio of systems in use today. Used in context together, there may be value.

   We suggest that additional data columns may be needed for the access report if available from the source system to get at this kind of discernment. If limited to username/identity, role, date/time and the operation performed in the access event, the utility of the available data from an ancillary system may not be great in terms of addressing questions of whether an access was "proper". If the meaning of the user identity or the user role does not lend itself to distinguish an access as a use or as a disclosure, questions such as knowing whether or not the access was proper may not be able to be answered very completely. For example, a patient may want to know about accesses to their record that were carried out outside normal operating hours by physician users or medical technologists who are not

employed by the hospital lab. In that situation, an employee user who accessed the data as a "use" internal to the employed workforce from a device located inside the facility may be acting properly. A user who accessed the data as a "disclosure" from a device outside the entity off hours may not be acting properly. In the current state of legacy systems, both users could be in the same role indistinct as employees or contractors by their user identities. It may only be additional information such as the device used for the access and the time of day of the access that would lend any context the access at least was one that might be regarded as improper.

We also suggest that consideration be given to the role of external business associates such as independent reference laboratories in their relationship to a hospital ancillary department. The access report or accounting of disclosure report requirements would extend to activities carried out by the independent reference lab on behalf of the hospital lab for diagnostic testing it performs. The OCR NPRM did indicate that the covered entity may send the patient directly to the business associate to obtain such reporting, but they also may desire to consolidate it in with what they would give to the patient. Issues of normalizing reportable data columns on user identity, event/operation names, data types accessed and purpose of use apply to the use of any log data provided from such external business associates to the covered entity as well.

3. **Goal 2, Question 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?**

   In their proposed rule, OCR included language that seemed to require the inclusion of uses and disclosures that involve internal exchange between applications, servers and devices that may be maintaining electronic personal health information (ePHI) as part of the logging required for the access report. We understand it may help the patient understand how their information is propagated to multiple systems within a covered entity, but we believe that could be done by reporting on natural person accesses. Taken to extremes, a requirement of this kind might suggest logging of activity between an LIS and medical instrumentation used to perform diagnostic testing. The potential for a numbing volume of activity aside, we are uncertain of the additional value provided to the patient of the logging of medical device interface related events or ATD events between a registration system and the LIS. It may prove confusing to the patient to understand how those events add value or are distinct from the other audit events they will see on the access report. The patient would already be able to understand their record is being accessed by different kinds of care providers for different kinds of purposes from logging of natural person accesses that would be a part of any access report. If OCR wishes to still provide for that kind of accountability in the access report, we suggest that OCR consider identification of the source system as an "if available" requirement for the access event as a data column in the access report so the patient may know which system was used for a given access event when done by a human end user.

4. **Goal 2, 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?**

   Our system makes use of all the manner of logging discussed in response to Goal 2, Question 1 but relies on a companion external security audit log for logging and reporting of end user access events to ePHI. Reporting is available for all the manners of logging discussed in different forms, but out of the box, only the security audit reporting is available in a patient specific context. The security reporting is on demand. The distribution logs are generated from operations jobs that produce the diagnostic test reports daily. The transaction logs are real time and the public health submissions are based on the timing of the reporting as required by the external agency. For distributions of diagnostic test reports, public health submissions and for interface related transaction logging, the logs are intended for other purposes primarily. The security audit logs are retained long enough to meet look back period requirements but the other logs are usually retained for a shorter period of time as befits their operational purpose. The logs are generated automatically. The security audit log has reporting capability built in, and also export capability of a .csv format or the audit events may be made available using an xml format. Aside from the security audit logs, reporting from the other kinds of logs available would require additional steps to make them available both for longer retention purposes to match to the access report/accounting of disclosures requirements proposed by OCR, and/or to harvest information from them useful for reporting in a patient specific context.

   We believe that ancillary systems especially as used standalone will have challenge with making data available easily from source logs of all the varieties we describe in our commentary. Aside from security audit logs, they may be designed to serve other operational purposes and someone would have to bear the cost of developing extraction routines or export capabilities to make effective use of them. We comment further on particular issues of "post processing" of data from any such extractions in response to Goal 4, Question 3.

5. Goal 4, Question 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?

This question is aimed perhaps more at questions of sensitivity in revealing the names of those who carry out such accesses or receive such copies. Assuming those can be overcome, we still see some challenges with providing for this kind of reporting across systems.

The most obvious issue would be normalizing the username, identity and/or role(s) across all the systems that would have to provide information to the consolidated reporting that would be given to the patient. Ancillary systems would use usernames or identities in whatever manner they are defined stemming from their implementation. As a part of the consolidation of this information, some manner of external mapping of usernames or identities and role information would need to be addressed outside the ancillary system. It may not have the ability to provide plain language user names and roles and even if it could, there is no guarantee they would be in the same format as would be the case for other systems.

Secondarily, any other metadata that would be a part of the reporting requirement would be subject to similar vagaries of what is available in source systems and in the particular case of ancillary systems, very likely in need of "post processing" to really be made sense of in consolidation with data from other systems to compile into a singular report to the patient. This includes:

- Information such as purpose of use would have to mostly be implied or assumed to be "for treatment" based on the application task used, the action performed and the data type accessed. So for example, a user in a medical technologist role enters/performs a lab test result using a result entry program. The security log of the ancillary system may know the user name/id, role, task used, operation performed, date/time accessed and data type accessed. Such systems are not going to ask for an explicit "why did you access this record".
- Source systems would likely not be synchronized as to a common NTP/time service and so interleafing of events from different source systems would be subject to potential chronological integrity issues especially as the covered entity tries to tell a story around a user and a patient and the sequence of events in their proper order
- The meaning of system operations to create, perform, modify, verify, error correct or output ePHI are only going to hold semantic meaning within the source system, and likely would require significant vendor assistance to develop into some coherent frame of reference that could then be normalized into common meaning across systems as a consolidated reporting is presented
- Likewise, user roles are not going to hold semantic meaning across systems without a similar effort

Finally, making sense of what the report would tell the patient would require support and education by the provider to help the patient understand just what it is they are looking at without raising red herrings. A patient would need a significant amount of help understanding and interpreting what they are looking at. A more usable way of presenting the data may include collapsing down the report to eliminate redundancy such as to show a row for each unique individual user acting in a given role who accessed the patient's record on a given day, and educating the patient about their options for receiving the report in a manner that answers their main interest in requesting it.

We appreciate the opportunity to provide this testimony to the HITPC SPTT, and we look forward to the opportunity to answer any questions the Tiger Team may have.