FAIRWARNING®

September 30th, 2013

Deven McGraw, Chair
Paul Egerman, Co-Chair
HIT Policy Committee's Privacy and Security Tiger Team
Office of the National Coordinator for Health IT

Testimony of Kurt Long, Founder and CEO, FairWarning®

Virtual Hearing Regarding Accounting of Disclosures

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.

The questions addressed by FairWarning®'s Vendor Perspective testimony today are related to the following questions:

<u>Question 1 and 6 of Goal 2</u>
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?
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?

2. **<u>Question 1 of Goal 3</u>**
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?
3. **<u>Question 1 of Goal 4</u>**
Regarding access reports, what information do you collect besides the basic information collected in an audit log?

FairWarning® has focused exclusively on healthcare access reporting and user activity monitoring since 2005. Our expertise and testimony today is focused on the value of access reports in general, and the practicality of generating patient-facing access reports specifically.

Beginning in 2005 through the present, the first use case required by our customers has always been to support a simple, internal-use access report. Simple access reports are in use by customers representing 1,100 hospitals and 4,000 clinics and facilities throughout the United States, Canada, the United Kingdom and Europe, 85 % of these are in the United States.

An internal-use access report details access to a given patient's records across all applications used in healthcare treatment, payment and operations, usually over a specific date range, and includes:

- Date & time of access
- User name, identifier and department
- Patient name and identifier
- Function and purpose of access
- Many other details may be included such as facility, floor, bed as well as descriptive detail of access. However, the availability, details and formats in Access Logs vary dramatically between applications used in healthcare.

Common care provider uses of internal-use access reports include:

- Investigation of a patient complaint brought directly to the care provider
- Investigation of a patient complaint directed through HHS
- Response to external legal discovery
- Forensics research in support of information security investigations
- Investigation of patient access as part of a health information exchange
- Legal documentation for defense against civil lawsuits, such as unlawful termination, which are routinely brought against care providers
- Increasing support of law enforcement investigations, particularly cases involving the theft of patient identities for use in false IRS income tax returns as well as medical identity theft.

While the ability to conduct simple access reports and associated user activity monitoring is invaluable, Access Report as defined in the Proposed Rule is technically infeasible due to the lack of wide-spread availability and detail contained in the Access Logs produced by application vendors.

Further, for the Proposed Rule to be practical, a highly simplified patient-facing format would be required. In the opinion of FairWarning® the Proposed Rule as written would have a large untold burden to care providers in explaining every access by every care worker. An overly detailed access report would create patient confusion and stress, unnecessarily injuring patient trust in electronic health records.

FairWarning® has examined and documented Access Logs generated by 519 different applications used in healthcare, when versions are considered, the number grows to nearly 1,000.

I will summarize our findings from the last eight (8) years. First the good news;

- Since 2009 we have documented an increase of applications routinely supporting Access Logs from 60 to well in excess of 200 today

- Every major electronic health record vendor with considerable market-share produces an Access Log that care providers can use to produce an internal-use access report

- Secondly, Meaning Use criteria requiring electronic health record vendors to include activated Access Logs by default has greatly improved the consistency, availability and robustness of Access Logs for MU certified technology

- For applications that are not subject to Meaningful Use certification, nearly 50 %, or just under 250 of the 519 applications we have examined produce an Access Log that is suitable for the production of an internal-use access report

- The Office for Civil Rights HIPAA audits and definition of User Activity Monitoring in their audit protocol has heightened care providers' attention to the need for the centralization and use of Access Logs for compliance, privacy and security. The net effect on application vendors is they are beginning to embrace the need to deliver basic security features such as Access Logs at no-charge and by default

- Care providers attesting for Meaningful Use are giving more attention to their privacy, information security and HIPAA compliance programs, with current and pending governmental audit programs serving as highly motivating factors. We believe that the permanent HIPAA audit program is essential to transitioning from "attention to privacy, security and compliance" into a cycle of "investment in privacy, security and compliance"

These are positive trends; however, considerable improvements are still required before the Access Report as defined in the Proposed Rule is feasible:

- Over 250 of applications used in treatment, payment and operations do not routinely produce an Access Log that is capable of supporting even a simple access report

- Further, a select number of application vendors have attempted to charge as much as $ 20,000 just to activate Access Logs.   When this occurs, care providers are frozen from moving forward with their compliance initiatives for the application in question

Access Logs are foundational to compliance, privacy and forensics and there is a clear need for a robust, ubiquitous and practical standard for application vendors involved in United States healthcare.

Going forward FairWarning® offers the following recommendations:

- Build upon the successful work of the ONC in requiring certified electronic health records to produce an Access Log by default, extending this requirement to all applications used in the course of healthcare
- The availability of Access Logs by default should be included in vendor base pricing and result in no line-item charge to care providers
- Produce and publish a robust, ubiquitous and practical standard for the production and contents of Access Logs
- Dramatically simplify the information required in a patient-facing Access Report

Sincerely,

Kurt J. Long

Founder and CEO, FairWarning®