



Q&A Session for New Privacy and Security Provisions (including amendments to HIPAA regulations) in the American Recovery & Reinvestment Act 2009

Speakers:

Deven McGraw, Center for Democracy & Technology
Kurt Long, FairWarning®

Session number: 669438167

Date: March 9, 2009

Related documents:

Full presentation and replay available [here](#)
CDT Summary document available [here](#)

Questions & Answers

Q: What is the definition of electronic health record? Many companies have different definitions of this.

A: There is a definition in the stimulus legislation (ARRA) – it is “an electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff.” (Section 13400) This definition is relevant to the new accounting for disclosure requirements (which only apply to covered entities who use electronic health records) and the requirement to provide individuals with an electronic copy (which also applies only to entities with EHRs). HHS will likely need to provide further clarification of this definition in regulations or guidance.

Q: Does "unsecured" PHI in ARRA for purposes of notification cover non-electronic PHI?

A: Unsecured PHI is PHI not protected by a technology or methodology that makes the data unreadable, unusable, or undecipherable. It's hard to imagine how to make a paper record protected under this standard – thus I don't think it covers non-electronic PHI.

Q: Are these new rules published in one place or are they scattered throughout the ARRA? Where can I find these new rules?

A: They are in one place – Title XIII, Subtitle D.

Q: In Deven's presentation on non-covered entities, what is meant by PHR?

FairWarning®, Trust but Verify®
www.FairWarningAudit.com
webinars@FairWarningAudit.com



A: PHR is the acronym for personal health records. A personal health record is defined in ARRA to be an “electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.” The term “PHR identifiable health information” includes “identifiable health information” as defined in the HIPAA privacy rule, as well as “information that is provided by or on behalf of the individual, and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.”

Q: Does this define EHR?

A: See the answer to the first question above (an EHR is an “electronic health record”).

Q: When are the regulations expected to be available? And is there a written resource we can refer to now?

A: The regulations will likely not come out until later this year. The first set of regulations will be on the breach notification provisions, and those are expected no later than August (and may come out sooner). Other regulations are likely to come out this summer or fall. Various law firms and trade associations have put out summaries of the new provisions; you should have received one from Fair Warning® that I developed at CDT.

Q: Please clarify what is the time frame for when these new changes must be in place.

A: Most of the provisions go into effect on February 17, 2010, but a few go into effect earlier and some have later effective dates. Please see Appendix A of my summary for a timeline.

Q: Please confirm that the "Minimum Necessary = Limited Data Set" standard is not effective until 2/17/2010.

A: That is correct, although I disagree with how you have interpreted the language. A limited data set is strongly encouraged for meeting the minimum necessary standard – but a limited data set is not required if it cannot be used to effectively meet the purposes of the particular use or disclosure of the data.

Q: Is there a comment period for any of the regulations? The enforcement dates are varied and I am curious if there is any possibility of regulation modification with the new rules with ARRA/HITECH Act?

A: There will be a comment period for each regulation, which is required under federal law. However, any rules that are released as “interim final rules” (which is the case for breach notification) will go into effect when they are published. There will still be a comment period, and then the rules could be

FairWarning®, Trust but Verify®

www.FairWarningAudit.com

webinars@FairWarningAudit.com



modified based on those comments (although not before they are effective). The other rulemakings in the legislation will likely be full notice and comment rules, likely requiring a 30-60 day comment period (plus response by the agency to the comments) before they are final.

Regulations can provide clarity to the statutory language but they cannot change the statute. Only Congress can do that.

Q: Is there a retroactive breach notification for breaches related to "safe harbor" technologies that are no longer secure? If so, how long would it go back?

A: This will need to be addressed in regulations – it is not covered by the language of the statute. As I read the language, entities would have to notify if they found out about unauthorized access to the data and that data is no longer protected by a technology that has been approved by the Secretary – and there would be no limit to how far back that could go (although the notification requirement is only triggered when the entity hears of the unauthorized access or breach).

Q: Does the product support IHE ATNA or HITSP T15 (Collect and Communicate Security Audit Trail Transaction)?

A: Yes. Out-of-the-box.

Q: How do the new requirements affect a covered entity with regards to determining the security of third parties? Can we expect a greater degree of security compliance on their part?

A: Business associates now have to directly comply with most of the requirements of the security rule – so I assume you can expect a greater degree of security compliance on their part because they can be penalized by federal or state authorities for failure to comply.

Q: Does the EHR definition include all surrounding systems (e.g. ancillaries, HIM, etc.)

A: Depends on how HHS interprets the definition (see first answer above).

Q: I was taking notes, so didn't catch what company Kurt Long is from or how to reach him if I have questions later about his presentation.

A: FairWarning®, Kurt@FairWarningAudit.com

Q: where is EHR defined? Subtitle "D"?

A: Section 13400 of Subtitle D.

Q: Since the inception of HIPAA regulations - are additional regulations added periodically?

FairWarning®, Trust but Verify®

www.FairWarningAudit.com

webinars@FairWarningAudit.com



A: The HIPAA regulations were finalized in 2000, and then some were changed in 2002 – but regulations have not typically been added on a periodic basis.

Q: Would you put together a grid of all of the changes, effective dates and/or what must take place in order for an effective date to be issued

A: See Appendix A of my summary for a timeline of effective dates/regulatory timeframes.

Q: Do HIPAA enforcements apply to business associates that are outside of the US (e.g. Canada, etc.)? They would have to assist with AOD tracking?

A: Technically yes, although U.S. authorities may have difficulty reaching overseas business associates.

Q: How often have you seen HIPAA audits review the infrastructure logs (i.e. Servers, firewalls, etc)

A: HIPAA audits performed by the government or by private entities? The government has done few HIPAA audits. I'll let Kurt and Shane answer this based on their private sector experience.

Q: Does pdf format constitute "electronic copy" of a patient's EMR for right to access purposes?

A: Depends on how HHS interprets that right.

Q: How do you see the Business Associate (BA) changes affecting the covered entities obligation to obtain a BA agreement prior to disclosing PHI?

A: Covered entities will have to obtain business associates with RHIOs and other health information exchange entities before they can exchange data with or through them. In some cases they may have to enter into BA agreements with PHR vendors where the vendor is offering a PHR on the covered entity's behalf. But beyond that ARRA made no changes to the HIPAA privacy rule provisions setting forth when business associate agreements are required. Covered entities may be more motivated to require BA agreements since those BAs can now be held directly responsible for complying with relevant HIPAA regulations (versus today where the covered entity's might be held responsible for a BA's failure to comply with the rules in certain instances). The more clear division of liability may motivate covered entities to seek business associate agreements in more cases; of course, companies seeking to do business with a covered entity may be reluctant to enter into a BA agreement for the same reason.

Q: When do we anticipate the results of the study on this legislation's impact on the cost of healthcare, and how will this already strapped industry be recompensed?

A: The study is due within five years of enactment. Some of the provisions that industry has raised the most concerns about from a cost perspective (such as the accounting for disclosures provisions) do not go into effect until 3-5 years post enactment, so it makes sense for this study to be timed in this way.

FairWarning®, Trust but Verify®

www.FairWarningAudit.com

webinars@FairWarningAudit.com



Q: State AG's will be involved with enforcement. Does this mean they can do audits as well?

A: ARRA does not expressly provide them with this authority. However, the authority of State AG's is also governed by state law – so they may have this authority explicitly or impliedly in some states.