California Health & Human Services Agency
Center for Data Insights and Innovation
Data Exchange Framework Data Sharing Agreement Policies and Procedures Subcommittee
Meeting 8 Chat Log (10:00AM – 12:30PM PT, June 27, 2023)

The following comments were made in the Zoom chat log by Members of the Data Sharing Agreement Policies & Procedures Subcommittee and staff during the June 27 meeting:

13:06:51 From Matthew Eisenberg to Everyone:

My Title as listed is incorrect. I'm the Associate Chief Medical Informatics Officer (ACMIO) at Stanford Health Care. If we can update the slides, that would be great.

13:14:35 From Steven Lane to Everyone:

Agree that a 10 day review period is going to be a challenge for many.

13:15:00 From Steven Lane to Everyone:

Could we make it 30 days??

13:17:29 From Deven McGraw to Everyone:

Perhaps a definition of administrative change that it doesn't increase burdens (either substantive or administrative) on participants? For example, eliminating the signature requirement reduces burdens so arguably less time needed for it to go into effect — but the opposite, putting a signature requirement in effect, would increase burdens and therefore shouldn't be "administrative."

13:18:10 From John Helvey to Everyone:

+1 Deven

13:18:24 From Deven McGraw to Everyone:

But even a change in contact information, for example (where to report breaches, for ex.) still requires entities have some time to change their systems accordingly.

13:19:46 From Steven Lane to Everyone:

+1 Deven. Another option would be to allow signatories to object to the 10 day timeframe for a given change and then have that push the timeline longer or to a different process.

13:20:11 From Helen Pfister to Everyone:

The definition of administrative change is set forth on the slides that DeeAnne is reviewing, and will be included in the Glossary.

13:22:17 From Steven Lane to Everyone:

The definition is appropriate, but there may be differences in interpretation.

13:23:44 From Elizabeth Steffen to Everyone:

Agree that the 10 days is not enough time

13:24:07 From John Helvey to Everyone:

Agree with Matthew...work life balance

13:24:14 From Morgan Staines to Everyone:

Agree 10 days is insufficient

13:30:01 From Lee Tien to Everyone:

+1 to what Louis said, especially for the non-HIPAA entities, what is their baseline level of privacy and security

13:35:04 From Mark Savage to Everyone:

Applicable law in California is not just HIPAA.

13:35:17 From John Helvey to Everyone:

CMIA

13:35:28 From Diana Kaempfer-Tong to Everyone:

IPA

13:36:13 From Matthew Eisenberg to Everyone:

Of course Mark, but this appears to be focused on HIPAA practices, while still quoting key applicable State Law. My point is that we are already obligated to follow applicable law.

13:37:04 From Lee Tien to Everyone:

I have to note recent major data breaches involving government entities, e.g. https://www.jdsupra.com/legalnews/calstrs-notifies-members-of-third-party-5590368/ (CalSTRS); https://www.kcra.com/article/calpers-third-party-data-breach-california-bpi/44305829 ; https://www.ksby.com/news/local-news/slo-county-office-of-education-latest-california-agency-to-suffer-from-data-breach

13:40:15 From Deven McGraw to Everyone:

If the initial disclosure to the non-covered entity was authorized by law, if that non-covered entity subsequently breaches it, it is not the obligation of the original disclosing entity to report that breach. Instead, the entity causing the breach would have to rely on the breach notification requirements in these P&Ps (I recall there is one), or if state breach laws apply....

13:41:23 From Deven McGraw to Everyone:

(If the receiving entity is a business associate, which then breaches the data, then yes, the obligation to report goes back to the HIPAA covered entity— but if the disclosure is to an entity not covered at all by HIPAA — and that disclosure was authorized by law - the initial disclosing covered entity is not responsible for reporting that breach)

13:42:43 From Steven Lane to Everyone:

Are there specific discussions in flight regarding DxF enforcement through licensing, or is this just an idea that has been floated?

13:43:49 From DeeAnne McCallin to Everyone:

@Steven, in flight. For example, an APL (All Plan Letter) was released, I believe in April 2023.

13:45:47 From Lee Tien to Everyone:

My point to raising breaches is not only about the legal side but also public perception of privacy/security and trust, especially given public concerns for data about who is seeking repro rights and gender affirming care.

13:46:56 From Deven McGraw to Everyone:

Most of the data sharing will not involve BA agreements - and likely won't trigger the need for those agreements except in vendor-type arrangements.

13:51:51 From John Helvey to Everyone:

+1v Deven

13:53:01 From DeeAnne McCallin to Everyone:

https://www.cdii.ca.gov/compliance-and-policy/state-health-information-guidance-shig/

13:53:14 From DeeAnne McCallin to Everyone:

https://www.cdii.ca.gov/compliance-and-policy/state-health-information-guidance-shig/#sharing-food-and-nutrition-insecurity-info

13:55:22 From Matthew Eisenberg to Everyone:

Looks like an incredible resource site! Thanks!

13:56:55 From Deven McGraw to Everyone:

HIPAA guidance - Does HIPAA restrict a covered entity's disclosure of PHI for treatment purposes to only those health care providers that are themselves covered by HIPAA?

No. A covered entity is permitted to disclose PHI for treatment purposes to any health care provider, including those that are not covered by HIPAA. In addition, HIPAA permits a covered health care provider to disclose PHI for the treatment of an individual to a third party, such as a social service agency, that is involved in the coordination or management of health care of that individual. (Last item on this guidance page - https://www.hhs.gov/hipaa/for-professionals/faq/2073/may-covered-entity-collect-use-disclose-criminal-data-under-hipaa.html). FWIW

13:57:31 From Morgan Staines to Everyone:

Support your approach to de-identification

14:00:53 From Morgan Staines to Everyone:

Thanks, Deven, for the reference to add'l fed guidance

14:01:04 From Deven McGraw to Everyone:

Agree with Mark - where disclosures are legally required, such as in accordance with P&Ps, contrary provisions in BAA do not trump that. 45 CFR 164.502(a)(3).

14:07:31 From Matthew Eisenberg to Everyone:

+1 tp Deven. As a HIPAA covered entity/provider, we spend a lot of money doing this. I think the burden on our CBOs will be the real challenge here.

14:07:32 From DeeAnne McCallin to Everyone:

to reiterate that which Courtney just said. After incorporating some changes from today's discussion plus emails received this week, CDII will post, soliciting written public comment

14:10:45 From Morgan Staines to Everyone:

Likewise, Louis. Finding the balance between privacy and security and actually meeting people's needs is a challenge.

14:13:50 From Rim Cothren, CDII CalHHS to Everyone:

NIST 800-88 provides some industry guidance on destroying data, primarily destroying media. Would be interested in comments on whether this is applicable.

14:16:31 From Rim Cothren, CDII CalHHS to Everyone:

In particular, perhaps on whether the NIST "Clear" guidance is an appropriate requirement for "Securely Destroy".

14:20:27 From Mark Savage to Everyone:

Similar to the P&P mention of training, should this include the requirements on risk assessment? Those are specified in regulation, e.g. https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html, but perhaps worth lifting up in the same way as an important preventative measure.

14:23:16 From Rim Cothren, CDII CalHHS to Everyone:

@Eric - Thanks.

14:25:58 From Mark Savage to Everyone:

Quoting from the FAQ on risk assessment listed above:
The Security Management Process standard in the Security Rule requires organizations to “[i]mplement policies and procedures to prevent, detect, contain, and correct security violations.” (45 C.F.R. § 164.308(a)(1).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Section 164.308(a)(1)(ii)(A) states:

RISK ANALYSIS (Required).
Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization].

14:26:28 From Lee Tien to Everyone:

+1 to what Deven is saying about the baseline

14:27:35 From Lee Tien to Everyone:

If you don't have a good map you don't actually know

14:27:50 From Terry Wilcox to Everyone:

Agree with Deven. A security risk assessment is an annual requirement and ensures that all technical, administrative, and physical HIPAA requirements are in place.

14:28:35 From Deven McGraw to Everyone:

Perhaps we should be clear that this does not require hiring of external consultants to do this.

14:29:17 From Deven McGraw to Everyone:

Agree with Michelle - we shouldn't allow entities to require other Framework participants to respond to security questionnaires before exchanging data.

14:31:16 From Deven McGraw to Everyone:

OCR's risk assessment tool specifically designed for small to medium sized providers. Intended to walk people through the process of doing an internal risk assessment. https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

14:37:27 From Steven Lane to Everyone:

+1 Matt. We should always point to federal requirements as we must meet those requirements.

14:38:18 From Steven Lane to Everyone:

That makes sense, Johan. Thanks.

14:38:26 From Morgan Staines to Everyone:

+1 to Matt's comment about not duplicating (and risking deviating from) established federal standards

14:43:04 From Rim Cothren, CDII CalHHS to Everyone:

Great call out Matt. I think there is some clarification around (a) for us to consider.

14:49:42 From Steven Lane to Everyone:

Metadata is a very broad term.

14:50:08 From Deven McGraw to Everyone:

Agree there can be identifiable metadata - for example, in image files, the metadata can include the patient's name and/or DOB.

14:50:31 From Lee Tien to Everyone:

And location data

14:51:15 From Deven McGraw to Everyone:

+1 to Courtney - that makes sense.

14:51:47 From Mark Savage to Everyone:

Think Courtney's comment addresses my question.

14:52:19 From John Helvey to Everyone:

+ 1 Courtney

14:55:45 From Diana Kaempfer-Tong to Everyone:

+1 to Lee

14:55:48 From Mark Savage to Everyone:

Just flagging the obvious, that this will require going back and amending P&Ps that are now deemed final, e.g. Individual Access Services P&P.

14:56:29 From Matthew Eisenberg to Everyone:

From the federal CURES legislation - HIE allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law. I like Steven's idea of harmonizing this definition

15:00:19 From Steven Lane to Everyone:

To Lee's point, EHR vendors are subject to the Information Blocking rules.

15:01:12 From Deven McGraw to Everyone:

Lee, the certified EHR vendors are definitely covered by the federal information blocking rules - and the final rule from OIG regarding enforcement of the rules, and potential imposition of penalties, against certified EHR vendors and health information exchanges, was posted by HHS OIG today.

15:01:33 From Lee Tien to Everyone:

Thanks Deven!

15:01:42 From Deven McGraw to Everyone:

Fwiw - they may not have direct obligations under this Framework but they've got federal obligations.

15:03:01 From DeeAnne McCallin to Everyone:

https://www.cdii.ca.gov/wp-content/uploads/2023/06/DxF_DSA_SignatoryList_062623.xlsx DSA Signatory List that does include subordinate entities that were specified by the organization who signed the DSA, in the DSA signing portal.

15:03:09 From Matthew Eisenberg to Everyone:

+1 to enhancing the language. Sub-participant entities sounds better than subordinate

15:05:47 From Matthew Eisenberg to Everyone:

Also, just want to complement the group on adding the glossary. It's a helpful tool!

15:06:17 From Rim Cothren, CDII CalHHS to Everyone:

Thanks, Matt.

15:06:22 From Jonah Frohlich to Everyone:

Thanks Matt! It was quite an undertaking, but agree it will be very handy and valuable as we amend and develop new P&Ps

15:07:30 From Courtney Hansen to Everyone:

I also want to point folks to Section 14(b) of the DSA which addresses some obligations of third parties.