Vang, Khoua@CDII

From: Ohanian, John@CDII
Sent: Tuesday, June 27, 2023 8:55 AM
To: McCallin, DeeAnne@CDII; Cothren, Robert@CDII
Cc: Hansen, Courtney@CDII; Vang, Khoua@CDII
Subject: FW: Business Associate Agreements & Individual Access

Follow Up Flag: Follow up
Flag Status: Flagged

From: Deven McGraw <deven.mcgraw@invitae.com>
Sent: Monday, June 26, 2023 4:01 PM
To: Ohanian, John@CDII <John.Ohanian@chhs.ca.gov>; Hansen, Courtney@CDII <Courtney.Hansen@chhs.ca.gov>
Subject: Business Associate Agreements & Individual Access

Hi John and Courtney,

Hope you both are well. I missed the last DxF P&P Subcommittee meeting (#7), but I heard from someone who attended that a question was raised about whether HIPAA business associate agreements would trump data sharing requirements in the P&Ps. I understand that this came up in the context of the policy requiring responses to individuals (e.g., patients) requesting copies of their information from a provider/entity required to comply with the Framework.

I may not have the facts/context right, so forgive me if this seems out of left field! But I thought I would send both of you a note, because a conclusion that the BAA would trump a framework participant data sharing requirement didn't sound right to me based on my knowledge of, and experience with, HIPAA.

45 CFR 164.502(a)(3) of the HIPAA Privacy Rule makes clear that a HIPAA business associate "may use or disclose [PHI] only as permitted or required by its business associate contract or other arrangements pursuant to 164.504(e) *or as required by law*." (emphasis added) This means that if a business associate is required by other law - such as the Framework P&Ps - to disclose PHI, the business associate is expressly authorized by the Privacy Rule to make that disclosure. The purpose of the BAA is to govern how the business associate is permitted to use and disclose PHI in circumstances where law (either federal or state) permits such uses and disclosures -- but in the case where a law requires such disclosure, the Privacy Rule makes clear that the business associate can comply with that law.

In other words, if the Framework P&Ps merely permitted disclosures to individuals - but didn't require it - the terms of a business associate's BAA could constrain that business associate from making that disclosure. But where the law requires such a disclosure? 502(a)(3) expressly allows the business associate to comply.

I don't think there's a question that the P&Ps that are in effect constitute law, at least w/r/t the entities required by CA law to sign the Framework Agreement. The statute requires certain entities to sign the Framework Agreement, and the Framework agreement requires compliance with then current P&Ps.

Again, my apologies if I am off base in terms of what was discussed at the prior meeting - but if I can be helpful on some of these HIPAA questions, I'm happy to do so :)

Deven

--

Deven McGraw (she/her/hers)
External Affairs/
Data Stewardship & Data Sharing
O/M: 202-368-2603
@healthprivacy
invitae.com

You can find a detailed explanation of our privacy practices here.