How De-Identification Has Turned HIPAA on Its Ear (And Other HIPAA Tidbits Pertinent to Those of Us in Private Practice)

Susan C. Litton

Is It Possible to Be Exempt from HIPAA in 2024?

As soon as I answer "No" to that question, someone would write me, explain their situation, and I'd find myself in the position of needing to write a retraction. So let me just say that at this point in time, I'd be hard-pressed to come up with a scenario of how one might pull that off.

In the past, YES. When HIPAA was enacted in 1996, some psychologists and other healthcare providers opted to abstain from actions that would trigger HIPAA. They kept only paper-pencil records, refraining entirely from creating or storing digital files on any device. They never submitted insurance claims electronically. By taking these precautions, they did not consider themselves to be Covered Entities (CEs).

However, when COVID began, many providers, who had never used electronic tools, felt that taking the digital plunge had become necessary. They started by using video software but may soon have found themselves needing other tools for routine tasks. Although some discretion was allowed in the early stages of the pandemic (Office for Civil Rights [OCR], 2020), providers were encouraged to get HIPAA Compliant products that provided Business Associate Agreements (BAAs), as soon as possible. At the time, getting a BAA was considered "best practices". However, this is the issue:

BAAs are legally binding contracts, but ONLY for Covered Entities. They almost always start with a statement similar to this:

"This document is an agreement between X, a software company and Y, a Covered Entity."

If you've signed a document like that that attests to the fact that you ARE a Covered Entity, you might have a hard time convincing an auditor or a court that you are not. It only takes one such signed document to flip the switch. Once HIPAA is triggered, it's triggered – it can't be undone. There ARE some exceptions when HIPAA Does NOT Apply, such as when the information doesn't constitute PHI, when it's used for specific research or public health activities, or when it's handled by certain entities like schools, employers, or law enforcement. But unless you fall into one of these categories, it's likely safest to assume that you're a Covered Entity.

There's also a somewhat nasty double-bind here:

- If you claim you're NOT a Covered Entity, your BAA is null and void since BAAs only apply to CEs.
- However, if you ARE a CE, you're required to comply with HIPAA.

Not long ago, I would now point out that becoming compliant with HIPAA didn't have to be a heinous or expensive task. Whether you would want a BAA was almost a no-brainer, since BAAs were intended to provide additional peace of mind for both providers and their patients. My suggestion would have been to just bite the proverbial bullet, become compliant with HIPAA, and continue using HIPAA Compliant Software that provided BAAs. However, recently, some healthcare software companies have reworded their BAAs in ways that are contrary to how BAAs were originally intended to be used. Here's the story:

BAAs: What They Were Intended to Be and What They've Become

The concept of a "Business Associate" (BA) was introduced in HIPAA's Privacy Rule in 2002 and 2003 as "a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity" (OCR HIPAA Privacy, 2002, 2003). The definition was expanded in 2009 by the Health Information Technology for Economic and Clinical Health Act (HITECH), requiring BAs to comply with many of the same privacy and security requirements that apply to CEs. The HITECH Act also required BAs to provide CEs with Business Associate Agreements. Finally, the Omnibus Rule of 2013 extended a BA's responsibility to safeguard a CE's Protected Health Information (PHI) such that if there was a breach caused by the BA's company or product, the BA was at fault, not the CE. BAs were also required to specify how they used and intended to use the PHI that had been entrusted to them.

The intent of these laws was to encourage software developers to build secure healthcare products. The logic was that if a company knew it would be held accountable, it would offer safer products and services. It was hoped that the requirement of transparency would encourage ethical business practices. The original purpose of a BAA, then, was to provide a layer of protection for CE and their patients.

Recently, however, certain healthcare apps, including at least one EHR, had to revise their Terms of Service because of updated privacy regulations required by certain states. To meet the new requirements, these companies altered their Terms of Service and BAAs. Although the changes they made were legally compliant, the companies no longer offered the same level of assurance for CEs. In fact, the new Terms did just the opposite. The key to how they managed to do this has to do with de-identified data.

De-identification

De-identification of PHI, by itself, is neither good nor bad. The issues are more about how it's done, whether it's done correctly, and the purpose for the de-identification. We'll look at each separately.

How De-identification is Done

HIPAA is quite clear about how to de-identify data. There are two methods that can be used. The one used most often, which also produces the best results, is called the Safe Harbor Method. According to the provisions outlined in HIPAA's §164.514(b), the Safe Harbor Method for de-identification lists the following 18 identifiers of the individual or of relatives, employers, or household members which must be removed:

A. Names

B. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:

   1. The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and

   2. The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000

C. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older

D. Telephone numbers

E. Vehicle identifiers and serial numbers, including license plate numbers
F. Fax numbers
G. Device identifiers and serial numbers
H. Email addresses
I. Web Universal Resource Locators (URLs)
J. Social security numbers
K. Internet Protocol (IP) addresses
L. Medical record numbers
M. Biometric identifiers, including finger and voice prints
N. Health plan beneficiary numbers
O. Full-face photographs and any comparable images
P. Account numbers
Q. Any other unique identifying number, characteristic, or code, except as permitted by paragraph (C) of this section; and
R. Certificate/license numbers

That SOUNDS like it should be straightforward, but it's not. One issue is that medical records are a combination of structured and unstructured data (also called "free text"). De-identification software products used to scrub medical records and remove identifiers are reasonably good at detecting and removing PHI from structured data. However, PHI in free text sections are not always clearly labeled (Dorr et al., 2006; Uzuner et al., 2007). This might mean, for example, that the clinical notes we enter into our Electronic Health Records or other note-taking software could be treasure-troves of identifying information, even when we're reasonably careful with how we write them. This is because, except for structured questions in the notes, the notes we write would be in free text areas of the application. Another place de-identification software could easily miss identifying information would be on files or forms a therapist might upload into their file storage application or that portion of their EHR. Those kinds of documents – typically PDFs or Word documents – often contain all sorts of information, including assessment results, that could be harmful to our patient if it were to get out.

Whether De-identification is Done Correctly

The difficulty with the de-identification process described above illustrates problems that occur when de-identification is done correctly. However, we may be taking too much for granted when we assume companies are doing it right. For example, some companies claim to use initials to identify patients, citing that as evidence that they're de-identifying PHI (Dalton, 2023). However, according to HIPAA, initials are considered PHI when those initials are maintained in a designated record set (U.S. Department of Health & Human Services, n.d.). It is unclear whether the companies doing this are unaware of correct de-identification practices, or whether they are choosing to ignore them. Either way, each potential identifier that is NOT removed increases the possibility of recognition. De-identified data is not considered foolproof. Even when it is done properly, individuals can sometimes be recognized (Benitez, 2010; Sweeney, 2000). However, even though de-identification doesn't ensure complete protection or confidentiality, it IS legal and – most importantly for our discussion – de-identified data is no longer considered PHI.

The Purpose for De-identifying the Data

This final discussion point – the purpose for de-identifying data – is what has thrown HIPAA on its ear. The issue is not that companies are de-identifying data. It's the rights the companies are assigning themselves by doing it. Companies are claiming that they de-identify all PHI they receive from their subscribers. De-identified data is not considered PHI. The companies argue that because they de-identify all data, the following assertions are true:

- All data entered into their program belongs to them (since they de-identified it, it is now their data, not your PHI).
- As a result, they can do anything they want with it – sell it to any buyer they can find, use it to train AI models, etc. Furthermore, they refuse to disclose how they use this data. It's their data to do with as they please. The fact that the data has been de-identified, they argue, puts it in the realm of an internal business decision, and they are not required to disclose such practices to their customers.
- This may also mean that they are no longer on the hook for breaches. Breaches apply to PHI, but de-identified data is no longer considered PHI. Any mishaps that occur with de-identified data fall into the "unfortunate accident" category. Your clients may have been part of the unfortunate accident – possibly even been identified from it – but it's not a breach. Because it's not a breach, there's nothing the company must do to remedy the situation or try to prevent it from happening again. But what if there IS some kind of incident where patients are identified. What are your legal responsibilities or ethical considerations? Or what if you enter data into the program in the afternoon, the company does routine de-dentification sweeps every night at midnight, but there's a breach during the window before the data was de-identified? Who's responsible for that?

Miller, 2021, further discusses this problem by noting that "de-identified data can easily be re-identified when combined with other datasets, and the only protection from re-identification right now is the recipient of the data agreeing to not do so." In the case of the software companies described above, we clearly do not even have this much. In fact, they are specifically asserting that they do NOT have to tell us what they are or aren't planning to do with the data we enter into their programs. Companies they sell our data to would be within their legal rights to re-identify it.

Clearly BAAs like this, originally intended to help us, no longer do so. Some providers have mistakenly concluded that since these companies are still claiming to be HIPAA compliant, they do not need to worry about the new Terms. This is wrong for several reasons.

HIPAA Compliant Software?

First, technically speaking, there is no such thing as HIPAA compliant software. Software cannot be a Covered Entity, and only CEs can be HIPAA compliant. Using "HIPAA compliant software," means that, assuming you use it correctly and are complying with all other HIPAA requirements, YOU, as the CE, can be in compliance with HIPAA.

Second, although the OCR indicates that healthcare software should be encrypted, it doesn't specify the type of encryption that must be used. This was a wise move for two reasons:

- Technology is constantly changing. Specifying cutting-edge encryption available when HIPAA was enacted on August 21, 1996, would have quickly become outdated.
- The authors of HIPAA were not experts in technology. By not specifying the type of encryption, they were leaving those kinds of decisions up to the experts in the field, which is as it should be.

However, the fact that the type of encryption is not specified has also allowed software developers a great deal of latitude. Some companies, for example, knowingly use encryption that is only secure 80 - 85% of the time (Google Transparency Report Help Center, n.d.). This is legal. Although a bit on the absurd side, technically, if a product is only encrypted 10% of the time, the BA has still fulfilled their HIPAA obligation. When we put this fact together with data that may be incompletely or inaccurately de-identified, the likelihood that our client's data may not be adequately protected by companies using these new all-inclusive Terms is very much in question.

Ethical Considerations

Although companies doing this may well be operating within the law, are they ethical? Can you use these products and still maintain the ethical standards of your profession? All healthcare professions have ethical codes concerning confidentiality. The American Psychological Association's code of ethics, Section 4, Privacy and Confidentiality, includes two standards that are especially pertinent here: 4.01 Maintaining Confidentiality and 4.02 Discussing the Limits of Confidentiality.

These two standards specify that psychologists "have a primary obligation and take reasonable precautions to protect confidential information obtained through or stored in any medium." Furthermore, psychologists are to discuss with their patients "(1) the relevant limits of confidentiality and (2) the foreseeable uses of the information generated through their psychological activities (American Psychological Association, 2017)."

In a blog post by Dr. Keely Kolmes (2023), they provide compelling evidence that using such products may well put us in violation of our ethical guidelines ("It had to be you: When your favorite EHR makes you break up with them," 2023). In addition to confidentiality issues, Dr. Kolmes references APA standards pertaining to the general principles and informed consent.

Conclusion

Although Dr. Kolmes' post pertains to a single product, Simple Practice, my concern is that other products will follow suit, if they have not already. Zoom originally released new Terms that were similar to those released by Simple Practice. After only a few days of receiving a rather large outcry of negative reactions, Zoom reversed their position and instead stated that Zoom healthcare products would be excluded from the new Terms. Simple Practice has made no such retraction. Other companies are mostly remaining mute – leaving me to wonder what I would find if I were to read the current Terms and BAAs of other similar healthcare products.

Obviously, those of us in healthcare professions have no control over the business decisions software companies make. However, our primary responsibility is, and always has been, to the patients, students, and other individuals we serve. The following guidelines may be useful:

- I still recommend using HIPAA Compliant Software that provides a BAA. However, read the BAAs. Don't just assume the company has your best interest at heart and sign. Although that might have been reasonable at one point in time, it no longer is.
- Integrated products such as EHRs may be better choices than stand-alone products, partly because you'll have fewer BAAs to try to make sense of and, thus, fewer potential loopholes.
- When feasible, use products that specify that they do not sell, barter, or trade any patient data, even in de-identified form.
- Special precautions should be taken with products that might use patient data to train AI models, including those that maintain that they will not disclose what they're using your data for.
- If you do choose to use products that are putting your data at more risk, consider discussing this increased risk with your patients, possibly also giving them other options if they do not consent to having their data used in that way.

Unfortunately, I don't feel there are perfect solutions to this dilemma. Although it is still possible to find products that do not de-identify and sell PHI, if you're already heavily invested in a product that does, it may be overwhelming to consider transferring to a safer product. APA's ethical standards require us to "take reasonable precautions" with patient confidentiality. The definition of "reasonable" is a decision each professional will need to make for themselves.

References

American Psychological Association. (2017). Ethical Principles of Psychologists and Code of Conduct (2nd ed.) Washington D. C.: Author.

Benitez, K., & Malin, B. (2010). Evaluating re-identification risks with respect to the HIPAA privacy rule. Journal of the American Medical Informatics Association, 17(2), 169–177. https://doi.org/10.1136/jamia.2009.000026

Dalton, L. [Host]. (2023, August 10). Simple Practice's revamped T&Cs. [Audio podcast episode]. Person Centered Tech. https://personcenteredtech.com/tag/simple-practices-revamped-tcs/

Dorr, D., Phillips, W., Phansalkar, S., Sims, S., & Hurdle, J. (2006). Assessing the difficulty and time cost of de-identification in clinical narratives. Methods of Information in Medicine, 45(3), 246-252.

Google Transparency Report Help Center. (n.d.). Email Encryption FAQs. https://support.google.com/transparencyreport/answer/7381230?hl=en

HHS Press Office. (2019, May 24.) New HHS Fact Sheet On Direct Liability of Business Associates under HIPAA. https://www.hhs.gov/about/news/2019/05/24/new-hhs-fact-sheet-on-direct-liability-of-business-associates-under-hipaa.html

HHS.gov. (2009, rev. 2017, June 16). HITECH Act Enforcement Interim Final Rule. https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html

HIPAA Guide. (n.d.). What is Considered as PHI under HIPAA? HIPAA Guide. Retrieved December 12, 2023, from https://www.hipaaguide.net/what-is-considered-as-phi-under-hipaa

Kolmes, K. K. (2023, September 22). It had to be you: When your favorite EHR makes you break up with them [Blog post]. Dr. Keely Kolmes. https://drkkolmes.com/2023/09/22/it-had-to-be-you-when-your-favorite-ehr-makes-you-break-up-with-them/

Miller, K. (2021, July 19). De-Identifying Medical Patient Data Doesn't Protect Our Privacy. Stanford Institute for Human-Centered Artificial Intelligence (HAI). Retrieved from https://hai.stanford.edu/news/de-identifying-medical-patient-data-doesnt-protect-our-privacy

OCR HIPAA Privacy. (2002, December 3. Revised 2003, April 3.) Business Associates

45 CFR 164.502(e), 164.504(e), 164.532(d) and (e). https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

Sweeney, L. (2000). Simple demographics often identify people uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. https://dataprivacylab.org/projects/identifiability/paper1.pdf

U.S. Department of Health & Human Services. (n.d.). De-identification. HHS.gov. Retrieved from https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#safeharborguidance

Uzuner, O., Luo, Y., & Szolovits, P. (2007). Evaluating the state-of-the-art in automatic de-identification. Journal of the American Medical Informatics Association, 14(5), 550-563.

Op-Ed

Become a Voice of Independent Practice and Run for an APA Board or Committee

Alan D Entin

Division 42 Past-president Peter Oppenheimer sent an important email to our membership, which, unfortunately, is only a fraction of total division membership. It carries a message that is of vital importance to the practice community and bears repeating and amplifying because it requires immediate action. I responded to Peter's post. Eileen Kohutis, IP Editor, thought the issue was of important to the entire membership. She requested I expand on my comment for the magazine to notify and to solicit the participation of the entire membership of the Division. The issue is nominating and electing practitioners to the governance of APA.

Peter wrote: "Service on an APA board or committee is a great experience and a valuable contribution to the profession. It is important that Division 42 members represent the interests of independent practitioners in these groups. We encourage our members to stand for election and serve." APA is also running a series of ads with the same message: Become involved in the governance of APA. Nominate yourself and/or a colleague to APA boards and committees.