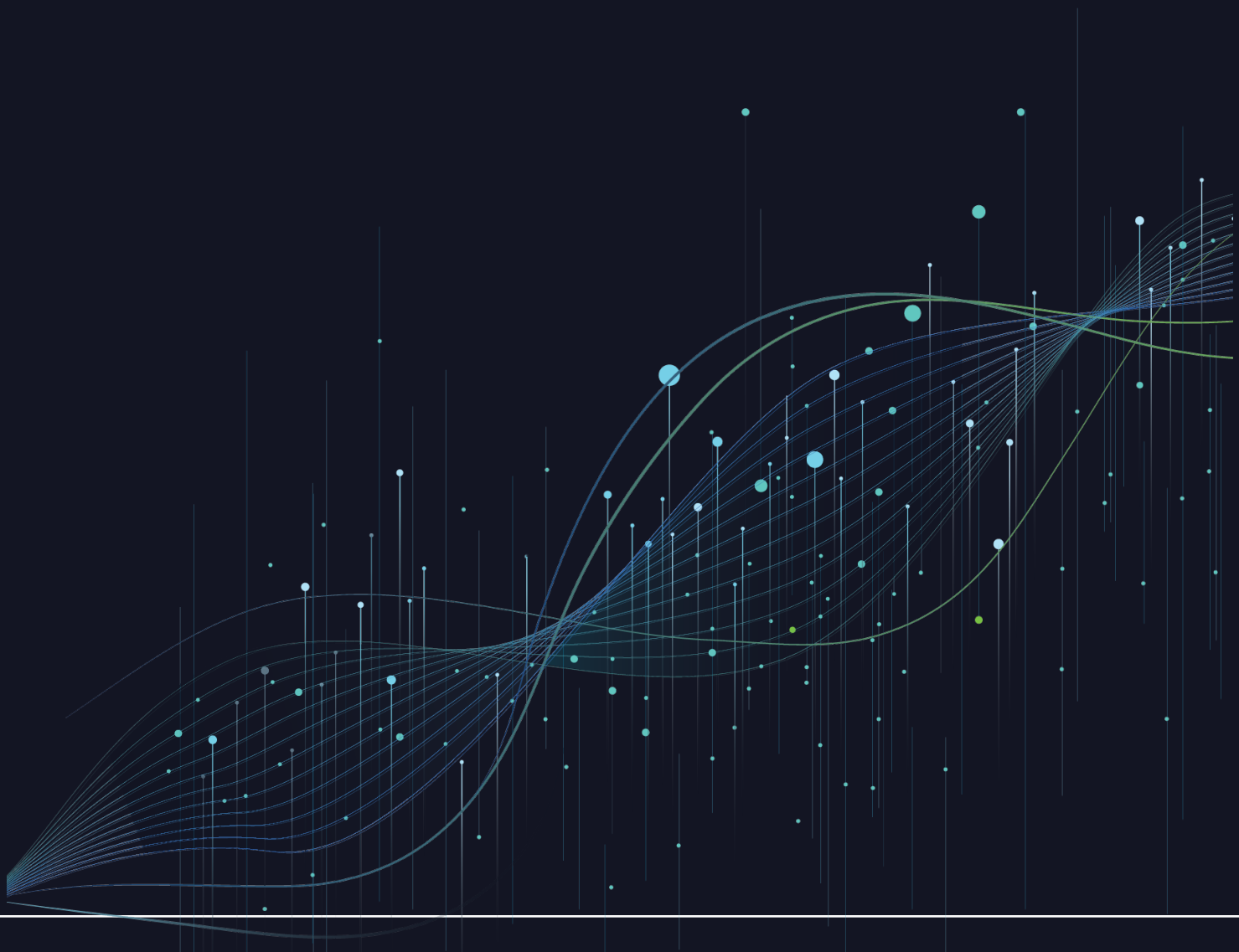
OMNY

Regulatory Compliance for the OMNY Platform



Our Healthcare Data Platform

Introduction

The recent exponential transformation of technology in healthcare settings has generated a wealth of data, much of which is directly tied to individual patients. The increase in data can lead to improved data-based decision making for healthcare providers and healthcare product manufacturers. However, it is important to use data that is Protected Health Information (PHI), in accordance with HIPAA. This white paper will review some of the rules and regulations of concern in more detail and explain the privacy and security controls

OMNY has implemented measures to ensure patient's data remains private. As your trusted, compliant intermediary, we ensure that you and your patients are fully protected in marketplace transactions through compliance with HIPAA.

At the same time, in the past, health systems have legally been unable to directly transact with third parties such as pharmaceutical companies. Pharmaceutical companies thus have been reliant on data aggregators to gather data from health systems, providers and pharmacies.

OMNY allows health systems to share in this revenue opportunity while remaining compliant with Anti-Kickback Statute and Stark Law. The OMNY platform provides multiple controls that guard against violations of the Anti-Kickback Statute (AKS) and Stark Law.

HIPAA

In the United States, there is no centralized law governing protection of data. Rather, a mixture of laws is tailored to oversee the handling and disclosure of specific types of personal data. The primary law that protects patient privacy is the Health Insurance Portability and Accountability Act, as revised by the Health Information Technology for Economic and Clinical Health Act, and its implementing regulations (collectively "HIPAA").[1]

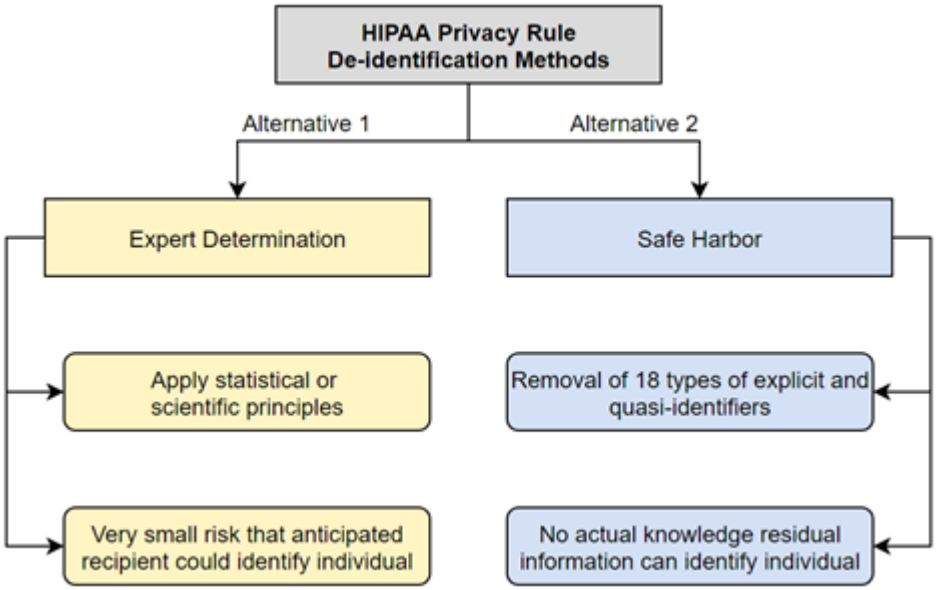
HIPAA has four sets of rules that apply:

- HIPAA Privacy Rule: Sets standards to protect patients' medical records and limits disclosures of PHI without patient consent
- HIPAA Security Rule: Sets administrative, physical, and technical safeguards for electronic protected health information (ePHI) for covered entities and business associates
- HIPAA Breach Notification Rule: Sets requirements for reporting unauthorized uses and disclosures of PHI to patients and to the Office of Civil Rights (OCR)
- HIPAA Enforcement Rule: Sets guidelines for how complaints and violations will be investigated and consequences for violations

HIPAA Privacy Rule

The Privacy Rule regulates the use and disclosure of all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.[4]

In addition to many common identifiers (e.g., first name, last name, residential address, and Social Security Number) that are considered PHI, potential "quasi-identifiers" (e.g., birthdate and specific zip codes of residence) may be considered "individually identifiable" since a recipient of the data may be able to determine the identity of the corresponding subject.



Data is "de-identified" and is not protected by the Privacy Rule, if health information does not identify an individual, and if there is no reasonable basis to believe that it can be used to identify an individual.[6] Under the Privacy Rule, organizations have two routes by which health data can be de-identified:[7]

- **Expert Determination:** a qualified statistician (i.e., someone with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable) may determine that the risk is very small that the information could be used by an anticipated recipient of the information, alone or in combination with other reasonable information, to identify a patient; or
- **Safe Harbor:** identifiers can be removed.[8] To build de-identified data sets out of a covered entity's data, OMNY acts as a business associate and enters into HIPAA business associate agreements (BAAs) with its covered entity partners. De-identification of data is a "Health Care Operations" function under the Privacy Rule, and thus may be done by a business associate on behalf of a covered entity.[25]

OMNY does not provide or disclose data to data recipients unless the data has been fully de-identified in compliance with the HIPAA Privacy Rule. Because some HIPAA identifiers are essential to the data recipient use of data (particularly the date and time of administration of a pharmaceutical product) OMNY has engaged an expert statistician under the Expert Determination de-identification method. Under the statistician's guidance, OMNY platform utilizes multiple techniques to de-identify data:

HIPAA Privacy Rule (Continued)

- **Date/Time Shift:** Dates within OMNY are shifted or obfuscated by a random amount with a set floor and ceiling. These thresholds keep transactions within the same month and before the reporting date while anonymizing them.
- **Aggregation:** OMNY holds and aggregates records, rather than sending patient-level records.
- **Thresholding:** OMNY implements a technique called thresholding, which requires the analysis of the type of data to determine a threshold level. The threshold level determines the minimum number of data records required for aggregation to ensure de-identification and significantly reduced the probability of re-identification.

Based on the expert's opinion, applying these techniques has sufficiently mitigated the risk of the date of administration field and has reduced the percentage of unique records that can be re-identified to a "very low" likelihood of identifying individuals within the data set.

Much research has been done on re-identification of health information devoid of explicit identifiers[1314151617181920] such as the "detective-like investigations cited by Malin[21] or "game theory" cited by Wan et al.[22] However, the key point in much of this research is that there is a significant difference between the ability to re-identify data and the likelihood of an adversary in the real world actually committing re-identification.[23] The HIPAA Privacy Rule does not preclude the dissemination of data that could be re-identified; but rather, states that the extent of de-identification must account for the identity of the recipient and the intent of the recipient. Through its contracts with data recipients, OMNY prohibits recipients from efforts to re-identify individuals within data sets. That contractual relationship gives an extra layer of assurance that the de-identified data sets will not result in the re-identification of individuals.

Once de-identified, OMNY then runs data analytics regarding the prescribing and purchasing of pharmaceutical products, which is useful information for pharmaceutical companies, research institutes, and other organizations that better data yields better decisions and better patient outcomes. OMNY is able to share revenue from this process with the data sources; because only de-identified information generates revenue, this process does not constitute the "sale" of PHI under HIPAA (see 45 C.F.R. §164.502(a)(5)(ii)). OMNY acts as the contractual intermediary between data sources and the data recipients handling pricing, contracting, and payment to ensure overarching legal and ethical compliance.

HIPAA Security Rule

The Security Rule, found at 45 CFR Part 160 and Part 164, Subparts A and C, sets standards for protecting the confidentiality, integrity, and availability of electronic PHI ("ePHI") through administrative, physical, and technical safeguards for covered entities and business associates. The Security Rule sets a minimum standard to follow, allowing covered entities and business associates the flexibility and scalability to meet the rule's minimum standards in a variety of ways.[9] The OMNY platform promotes HIPAA compliance and data security through a series of Privacy Protection Controls that are implemented into the marketplace experience.

Suite of Policies and Procedures

To fully comply with the Security Rule, we have implemented a full and comprehensive suite of policies and procedures that address the technical, administrative, and physical safeguards required:

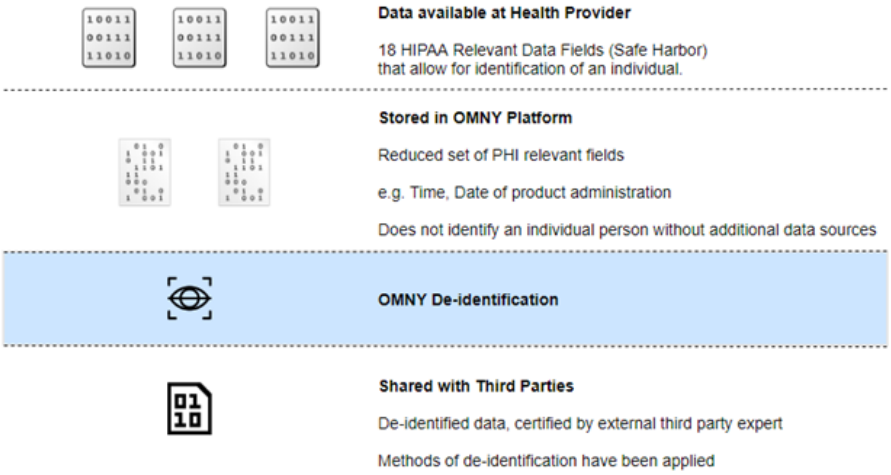
- **Administrative Safeguards:** OMNY operates with a privacy officer and a security officer, and together, they are responsible for maintaining and enforcing all of OMNY's compliance policies and procedures. These procedures and policies identify how OMNY handles any PHI it receives from Covered Entities or Business Associates and how to manage that data. With the help of the OMNY engineering team, the privacy officer and security officer have conducted a security risk assessment and implemented risk mitigation plans. The risk assessment will be reviewed every six months, at minimum. In addition, all employees at OMNY are required to receive training and review all compliance policies and procedures annually, at a minimum.

- **Physical Safeguards:** OMNY has facilities in San Francisco, California and Atlanta, Georgia. Both facilities are locked down and require authorized entry to gain access. In addition, OMNY's Asset Management Procedure covers asset management practices for device management, account provisioning, and data management.

- **Technical Safeguards:** Any file that OMNY receives from data sellers is access-restricted to the OMNY delivery team. The delivery team is responsible for reviewing all received data and minimizing the PHI before loading into the platform. This same team is responsible for de-identifying the data before it is shared with a data recipient based on the de-identification methods described above.

- **Utilizing Secured Encryption**: In accordance with the Privacy Rule and Security Rule, business associates must maintain full control over the access to data and minimize disclosures of PHI. OMNY achieves this with our platform, which uses encrypted and secured datastore technology. This platform is fully encrypted according to NIST+ standards and ensures that even malicious attackers would be unable to access the data. The OMNY Fidelity Data Marketplace Feature provides assurance that the data you place in the marketplace is not altered or tampered with. In addition, data shared with paying data buyers is shared encrypted, at rest and in transit.

- **Storing Minimal PHI**: To minimize any accidental disclosure of individually identifiable health information in accordance with the Privacy Rule and the Security Rule, OMNY limits the PHI stored within the platform. Files provided by data sources are thoroughly reviewed by the OMNY delivery team who are highly trained in HIPAA compliance.



Of the eighteen fields considered PHI, the OMNY team will strip most PHI fields before loading them onto the OMNY platform. All data on the platform must be reviewed and approved by OMNY and confirmed as de-identified before a data recipient can access the data.

HIPAA Regulations

The HIPAA breach notification requirements are found at 45 CFR Part 164, Subpart D. This sets the expectations for covered entities to report an unauthorized use or disclosure of PHI that constitute a “breach” to patients and to OCR, and sometimes to the press in a large data breach. These regulations also require business associates to report breaches to the covered entities whose PHI they handle.

OMNY complies with the Breach Notification Rule and has communication procedures in place, that are invoked if a breach ever occurred.

HIPAA Enforcement Rule

45 CFR Part 160, Subparts C, D, and E set forth the process for handling complaints, requirements for cooperation, and penalties for violations. The responsibility of enforcement resides with the U.S. Department of Health and Human Services (HHS). Covered entities and their business associates must cooperate with any investigation or compliance audit by providing records and access to information.[11] The consequences of HIPAA violations can be significant. The number of fines reached an all-time high in 2018 with the largest settlement going to Anthem with a fine of $16 million for a 78.8 million-record breach.[12]

OMNY complies with the HIPAA Enforcement Rule and has communication procedures in place, that cover the cooperation with any investigation or compliance audit by providing records and access to information. OMNY ensures the fidelity of data on the marketplace via the OMNY Fidelity Feature, which provides full transparency into records and data as sold on the marketplace.

Closed Marketplace

The OMNY Marketplace is a closed marketplace, meaning that OMNY only engages with known data sources and data recipients. The marketplace experience is not open to the public, and data available on the OMNY platform is not accessible by parties that have not signed agreements with OMNY. The OMNY marketplace and services are designed to enforce highly principled actions from participants, reducing the likelihood of attempts to re-identify data.

- **Legal Agreements:** OMNY relationships are governed by BAAs with data sources and data use agreements with data recipients. The agreement between OMNY and the data recipient prohibit resale of the data or use to re-identify an individual.
- **User Centered Design.** OMNY practices user-centered design. Our product and engineering teams take the time to fully understand our users’ intents, goals, and pain points from both sides and design the experience to meet those users’ needs.
- **High Touch Services.** We employ an experienced delivery team that offers high touch services. From integrating your technological systems and ingesting your data to creating data offerings, our team will make the time to answer all your questions and maximize your experience with OMNY, further bolstering our strong partnerships with both data sources and data recipients.

AKS Compliance

The Anti-Kickback Statute ("AKS") prohibits the exchange of remuneration (anything of value) in exchange for referrals for services that are paid for by federal programs, including Medicare. OMNY has a variety of controls in place to assure data sources that bill federal programs, that any shared revenue to data sources does not violate the AKS. Each of these controls are explained below:

Contractual Intermediary

OMNY is a contractual "middle-man", contracting directly with data sources and data recipients (i.e., data sources will NOT be contracting with pharmaceutical companies and others that purchase de-identified data). OMNY will not disclose the identity of the data recipients to the data sources. If a data source does not know what entities are buying the data, the payments cannot influence formulary decisions by the data source. Furthermore, a data source provides OMNY access to all relevant data for all drugs in a category, so the data source will not know which particular drug resulted in revenue for the data sources

Payment Volume-independent

OMNY's payments to health systems are not tied to volume of data sold. Rather, they are affected by the amount of data made accessible through OMNY, the size and type of the data source, and number of parties that have agreed to purchase the de-identified data. D basis. The revenue sharing for the data source does not scale with volume of OMNY business with data recipients (i.e., the data source does not receive more revenue due to an increase in volumes bought, handled and administered by a hospital's pharmacy). Shared revenue to the data source increases only if they: 1) provide OMNY with more data, 2) add affiliates that contribute data, such as through a merger, or 3) have an increase in the number of third parties purchasing their data.

No Formulary Influence

Data sources must ensure that their decision makers do not have a direct influence over formulary buying decisions. This further ensures that hospital buying patterns are in no way impacted or influenced by the data agreements put in place through OMNY. Data sources contractually represent that no data source employee who is involved in the OMNY arrangement should be involved in the data source formulary decisions or deliberations. Of course, as the amount of drug data increases, the AKS risk to data source decreases substantially. Data sources therefore are encouraged to provide OMNY with supply chain data for multiple therapeutic areas. By having access to this larger data set, OMNY can further conceal the specifics of manufacturers buying access.

Summary

OMNY fully complies with HIPAA and AKS regulations and has a full set of controls implemented. These controls cover business processes, privacy and security measures as well as controls to be AKS compliant. With OMNY's marketplace, healthcare organizations now have a secure means for sharing their de-identified data and receiving revenue for that de-identified data. You have a trusted partner in OMNY, which will allow you to fully unleash the power of your data.

Endnotes

1. 45 C.F.R. § 164
2. https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html
3. https://www.hipaajournal.com/relationship-between-hitech-hipaa-electronic-health-medical-records/
4. OFFICE FOR CIVIL RIGHTS, US DEPT. OF HEALTH AND HUMAN SERVICES.
5. 45 C.F.R. § 160.103; § 164.514(a)
6. 45 C.F.R. § 164.502(d)(2)
7. OFFICE FOR CIVIL RIGHTS, US DEPT. OF HEALTH AND HUMAN SERVICES. Guidance regarding methods for de-identification of protected health information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. November 26, 2012.
8. https://healthitsecurity.com/news/de-identifcation-of-data-breaking-down-hipaa-rules
9. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
10. OFFICE FOR CIVIL RIGHTS, US DEPT. OF HEALTH AND HUMAN SERVICES. Guidance regarding methods for de-identification of protected health information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. November 26, 2012.
11. https://www.law.cornell.edu/cfr/text/45/160.310
12. https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/
13. SWEENEY, L. Weaving technology and policy together to maintain confidentiality. Journal of Law, Medicine, and Ethics. 1997; 25(2-3): 98-110.
14. EL EMAM,K. et al. Evaluating common de-identification heuristics for personal health information. Journal of Medical Internet Research. 2006; 8(4): e28.
15. K. EL EMAM, P. KOSSEIM. Privacy interests in prescription data, part 2: patient privacy. IEEE Security and Privacy Magazine. 2009; 7(1): 75-78.
16. LOUKIDES, G. et al. The disclosure of diagnosis codes can breach research participants' privacy. Journal of the American Medical Informatics Association. 2010; 17(3): 322-327.
17. BROWN, L. BROWN, D. KORFF. Limits of anonymization in NHS data systems. British Medical Journal. 2011; 342: d973.
18. CIMINO, J.J.. The false security of blind dates: chronomization's lack of impact on data privacy of laboratory data. Applied Clinical Informatics. 2012; 3: 392-403.
19. SOLOMON, A. et al.. Uniqueness and how it impacts privacy in health-related social science datasets. Proceedings of the 2nd ACM International Health Informatics Symposium. 2012: 523-532.
20. ATREYA, R., et al. Reducing patient re-identification risk for laboratory results within research datasets. Journal of the American Medical Informatics Association. 2013; 20: 95-101.
21. BRADLEY, M. A De-identification Strategy Used for Sharing One Data Provider's Oncology Trials Data through the Project Data Sphere® Repository
22. WAN, Z. et al. Game Theoretic Framework for Analyzing Re-Identification Risk,
23. MALIN, B., KARP, D., SCHEUERMANN, R.. Technical and policy approaches to balancing patient privacy and data sharing in clinical and translational research. Journal of Investigative Medicine. 2010; 58(1): 11-18.
24. https://med.stanford.edu/content/dam/sm/sm-news/documents/StanfordMedicineHealthTrendsWhitePaper2017.pdf
25. 45 CFR § 164.501(6)(v)
26. EL EMAM, K. , et al. A systematic review of re-identification attacks on health data. PLoS One. 2011; 6: e28071.