

COALITION FOR HEALTHCARE COMMUNICATION

Navigating the Health Data Privacy Landscape

A Guide for Agencies

I. Overview 3

II. State Health Data Privacy Laws 4

A. Washington My Health My Data Act 5

B. Other States With Standalone Health Data Privacy Laws 9

C. Comparing Standalone Health Data Privacy Laws to Existing Comprehensive State Data Privacy Laws 12

D. Best Practices For Agencies 15

III. Federal Regulatory Landscape 17

A. HHS OCR Bulletin on Online Tracking Technologies 18

B. FTC Health Breach Notification Rule 20

C. FTC Enforcement Actions Concerning Health Data Privacy 21

D. Best Practices For Agencies 24

E. HHS/FTC Resources Available To Companies 25

IV. Putting Agency HIPAA Compliance into Practice 26

A. The Role Of HIPAA Compliance Software 27

B. Avoid Taking Shortcuts with HIPAA Compliance 27

C. What HIPAA Compliance Software Should Do 28

D. What is HIPAA Compliance Certification 29

I. Overview

The landscape for understanding the compliance space around healthcare and data privacy has changed dramatically in just a few short years. While many of the changes have been driven recently by the Supreme Court's decision in ***Dobbs v. Jackson***, there are other changes happening at the state and local level that are part of a general trend of reigning in the collection and use of any kind of sensitive data, such as consumer health data and any data associated with children.

There are several systemic reasons for the historical gaps in the regulation of consumer health data in the U.S. Prominently, and in contrast to most other nations, the United States lacks a comprehensive or omnibus consumer privacy law at the federal level that would apply a uniform set of rules to the collection and use of consumer health data (and other) data.

While there has long been a loose understanding that consumer health data is either "HIPAA-covered" or "not HIPAA-covered", that prior delineation is increasingly coming into question as new laws and regulations attempt to regulate "HIPAA-adjacent" healthcare data that falls outside of the strict definitions of HIPAA. Some of these new laws and regulations that cover "HIPAA-adjacent" information are driven not just by the growing digitization of all things healthcare-related but also the growing wellness marketplace that seems to be running on a parallel track to traditional categorizations of healthcare.

The purpose of this white paper is to help make agencies aware of the growing tangle of new laws and regulations covering consumer health data and to help them employ best practices in complying with these new laws and regulations. As many of these laws and regulations are very new, what regulators decide compliance actually means will be a process that unfolds in the upcoming years, likely via a series of enforcement actions and "informal" guidance interpretations. But until then, there are certain best practices that agencies can employ to stay on the right side of these new laws and regulations, both for themselves and for their clients.



Please note that the below information is provided to help agencies understand the new healthcare data privacy landscape and is not intended to be legal advice. Agencies should consult their own legal counsel about any case-specific applications or concerns. Because the legal landscape in this area is constantly evolving, agencies should also consult with experts for any new updates following the date of publication.

II. State Health Data Privacy Laws

While 2023 was not the genesis year for new state laws regulating the collection and processing of consumer health data privacy (see the **2008 Illinois Biometric Information Privacy Act**), it was a banner year for the enactment of new state laws that for the first time attempted to address consumer's health data left unconsidered by the federal HIPAA framework and other state consumer privacy laws.

Legal concerns associated with fertility tracking apps post-*Dobbs*, high-profile health data breaches, and heightened press coverage associated with the collection of sensitive location data from consumers visiting healthcare facilities, drove legislators to act aggressively ushering in what is expected to be a new wave of health-specific data privacy bills, separate from the comprehensive data privacy laws seen from the states thus far.

At A Glance - State Data Privacy Laws

In a post-*Dobbs* world, states are recognizing that there is a gap in legal coverage regarding the commercial use of non-HIPAA covered, consumer health data. As a result, states like WA, CT, and NV have enacted new health data privacy laws to govern the collection, sharing, and selling of consumer health data that imposes strict consent requirements and bans the geo-targeting of ads near health facilities. Overly broad definitions of "consumer health data" in these consumer health data privacy laws also mean agencies should review the types of data they and their clients collect that might trigger obligations under the law.

Since 2018, states have been enacting comprehensive state privacy laws in hopes of better protecting American consumers' data privacy rights and giving them more control over how companies collect and use their personal data. The number of comprehensive state privacy laws enacted in the U.S continues to grow-totaling more than a dozen to date. Generally, comprehensive data privacy laws in the states give consumers rights to access, correct, delete, port, and opt-out of targeted advertising and the sale of their personal data. With a few exceptions, opt-in consent is required for the collection of a consumer's sensitive data (defined differently in each state law), which generally covers a narrower scope of health-related data than the state health privacy laws. HIPAA-entity and data-level exemptions and non-profit exemptions may also impact what kind of data and which entities are covered under the law.

As a general trend, we can expect some states to amend their existing comprehensive data privacy laws with new amendments to include stronger protections for consumer health data (i.e. as we have seen in CT), while other states may opt to enact new, standalone health data privacy laws (like those seen in WA, NV, and NY).

A. Washington My Health My Data Act

Background

Washington state's **My Health My Data Act** (MHMDA) was signed into law in April 2023 by Governor Jay Inslee (D-WA). MHMDA aims to "close the gap" between current data industry practices and consumers' understanding of how consumer health data is collected, stored, and transferred. The bill drafters made it very clear that MHMDA was meant to respond to the *Dobbs* decision and the gap in consumer health data not covered by HIPAA.

MHMDA mandates two possible lawful reasons for an entity to process consumer health data: consumer consent or necessity to provide a product or service that the consumer requested from the entity. Either consumer consent or necessity is required for the collection and processing of any consumer health data, and a regulated entity must obtain separate consent or meet the same necessity standard to share that data. Further, selling consumer data requires a special written and signed authorization from the consumer.

Scope of Applicability

Important to note, and contrary to most other comprehensive U.S. state privacy laws, there is no minimum number of data subjects or a specified revenue threshold for companies to fall under MHMDA's scope. As such, the law applies to consumer health data associated with Washington residents and consumer health data related to other persons, if such data is collected by a regulated entity in Washington State.[1] Small businesses do not get a reprieve under MHMDA, other than a three-month compliance extension to most provisions under the law. Under MHMDA, small businesses are defined as entities that collect data of fewer than 100,000 consumers a year, or that derive less than 50% of their gross revenue from consumer data (with data pulled from no more than 25,000 consumers).

Non-profit entities are not exempt from MHMDA, as they are in most existing state privacy laws.[2] There are baked in exceptions for data subject to other existing regulations such as the **Health Insurance Portability and Accountability Act (HIPAA)**, the **Gramm-Leach-Bliley Act (GLBA)**, **Family Educational Rights and Privacy Act (FERPA)**, and the **Fair Credit Reporting Act (FCRA)**, as is the case in other state privacy laws.

[1] A "regulated entity" under MDMA is defined broadly as any legal entity that (1) conducts business in Washington or produces or provides products or services targeted to consumers in Washington, and (2) determines the purpose and means of collecting, processing, sharing, or selling of consumer health data, whether alone or jointly with others. This means that even businesses that are not physically located within the state of Washington may be considered regulated entities as long as they have a commercial nexus to Washington. Further, unlike many other state data protection laws such as the California Consumer Privacy Act ("CCPA"), there is no threshold (e.g., based on revenue or volume of data handled) to be a regulated entity subject to the MHMDA.

[2] Nonprofit organizations are not completely exempt from state data privacy laws. They are typically subject to the same privacy regulations and obligations as for-profit businesses when it comes to handling personal data. The specific privacy laws that apply to nonprofits can vary depending on the jurisdiction where the organization operates. Nonprofit organizations often handle donor information, and many jurisdictions have specific regulations protecting the privacy of donors. These regulations typically govern how nonprofits collect, use, store, and share donor data, as well as donor rights regarding their personal information. State privacy laws can conflict with these non-profit donor laws, which is why many states have opted to provide exemptions for them. The Colorado, Oregon, New Jersey, and Delaware state privacy laws do not offer these broad entity-level exemptions for nonprofits. Nonprofits may fall under the California privacy law if they meet certain criteria. The privacy law in Oregon only exempts (1) a non-profit organization that is established to detect and prevent fraudulent acts in connection with insurance, and (2) the non-commercial activity of a nonprofit organization that provides programming to radio or television networks. The privacy law in Delaware only exempts (1) a nonprofit organization dedicated exclusively to preventing and addressing insurance crime, and (2) personal data of a victim of or witness to child abuse, domestic violence, human trafficking, sexual assault, violent felony, or stalking that is collected, processed, or maintained by a nonprofit organization that provides services to victims of or witnesses to child abuse, domestic violence, human trafficking, sexual assault, violent felony, or stalking.

Definitions

The law's definitions of "consumer", "covered data", and "health care services" found in MHMDA are broad, encompassing a wide spectrum of data and entities into scope. MHMDA provides an extensive list of categories for "consumer health data" that count as "physical or mental health status" such as information about individual health conditions, treatment, diseases, or diagnosis; social, psychological, behavioral, and medical interventions; bodily functions, vital signs, symptoms, or measurements; gender-affirming care information; reproductive or sexual health information, biometric data; genetic data; and precise location information (within 2,000 feet) that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies[3] (see category definitions in MHMDA for more info).

Controversially, "covered health data" under MHMDA also covers a broadly defined bucket of data that includes any "data that identifies a consumer seeking health care services" as part of what is considered consumer health data, drawing into question whether or not the definition includes consumer health data collected through cookies, pixels, or other similar trackers when Washington residents search for healthcare services online. Agencies should note that this issue is similar to the Department of Health and Human Services Office of Civil Rights (HHS OCR)/ Federal Trade Commission (FTC) December 2022 guidance on online tracking technology for HIPAA-covered entities which is covered later in this paper.

Consent for Collection / Processing / Sharing

The MHMDA permits regulated entities and small businesses to collect and process consumer health data only to the extent necessary to provide a product or service specifically requested by the consumer or with consent from the consumer.

Per MHMDA, "consent" means "a clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and unambiguous agreement, which may include written consent provided by electronic means."

Consent for Sale

In addition, the law requires a written consent—i.e., a "valid authorization"—before a regulated entity may sell or offer to sell consumer health data. The valid authorization must be written in plain language and contain such information as (i) the name and contact information of the seller and the purchaser of the consumer health data, and (ii) a description of the purpose for the sale, including how the consumer health data will be gathered and used. Further, any written consent/valid authorization obtained to sell consumer health data is valid only for one year.

[3] Worth noting, the term "health services or supplies" is not defined by MHMDA. " Under the current definition, "health services or supplies" would likely broadly relate to all of those provided at a local drug store.

Consumer Rights

MHMDA grants consumers rights to know, access, delete, and withdraw consent from the collection, sharing, or selling of consumer health data. If a regulated entity receives an access request, they must provide the consumer with a list of all third parties and affiliates with which the consumer health data was shared or sold and an active email address or other online mechanisms that the consumer may use to contact these parties. Deletion requests must be processed within 45 days of receipt of the deletion request.

Unlike other state privacy laws, the MHMDA does not include exemptions to consumer rights (i.e., regulated entities do not have a right to reject a deletion request if another conflicting law requires a regulated entity to maintain the data). This may be at odds with existing laws and/or generally create confusion for regulated entities as to when data may be retained for valid reasons.

Geofencing

The MHMDA disallows any person from instituting a geofence around an entity that provides in-person health care services in order to (1) identify or track consumers seeking health care services; (2) collect consumer health data; or (3) send notifications, messages, or advertisements to consumers related to their consumer health data or health care services. Under the MHMDA, a "geofence" means a virtual boundary that is 2,000 feet or less from the perimeter of the physical location of the company.

Health Data Privacy Policies

The MHMDA mandates that entities maintain consumer health data privacy policies, which must clearly and conspicuously disclose (1) the categories of consumer health data collected, the purpose for collection, and how the data will be used; (2) the categories of sources from which the consumer health data is collected; (3) the categories of consumer health data shared; (4) a list of the categories of third parties and names of specific affiliates with whom consumer health data will be shared; and (5) how consumers can exercise their MHMDA rights. A link to this health data privacy policy must be exhibited prominently on the homepage.

Access Controls and Security

Entities subject to MHMDA are required to restrict access to consumer health data to only those employees, processors, and contractors for which access is necessary to (1) provide the product or service requested by the consumer, or (2) further the purposes for which the consumer provided consent.[4] The law also mandates the establishment, implementation, and maintenance of administrative, technical, and physical data security practices that meet the "reasonable standard of care" for the regulated entity's industry appropriate to the amount and nature of the consumer health data retained.

[4] In cases where a system is collecting the data and then making it available for targeting, that data could be shared with an alias which would be accessible by multiple people. It is a practice that is not any industry best practice, but it will be even more problematic under MHMDA for consumer health data.

Data Minimization and Purpose Limitation

MHMDA places data minimization and purpose limitation obligations on the collection, sharing, and sale of consumer health data by data controllers, processors, and third parties. To that end, MHMDA includes "data minimization" requirements where regulated entities are required to limit the use and disclosure of data. Under MHMDA, data minimization entails limiting access to what is necessary to further the purpose for which the consumer provided consent, or where necessary, to provide a product or service that the consumer requested.

Contractual Obligations

In the MHMDA, data processors are only allowed to process consumer health data if there is a binding, data processing contract with the regulated entity. The contract must include processing instructions and limit the scope of actions a processor may take with respect to consumer health data. If there is a failure to adhere to those contractual obligations, a data processor would be considered a regulated entity for the sake of liability purposes.

Effective Dates

The MHMDA requires covered entities to comply with its obligations effective March 31, 2024. Small businesses must comply by June 2024. The only exception to these operational dates is the provision banning geofencing, which does not include an effective date, thereby defaulting to Washington's standard enforcement time frame of 90 days, or July 23, 2023.

MHMDA Enforcement - A Private Right of Action

MHMDA includes a private right of action (PRA) under Washington's Consumer Protection Act for consumers to sue companies for violations of the law. The MHMDA can also be enforced by the Washington Attorney General's office. The state attorney general's office can impose civil penalties up to $7,500 per violation. A PRA enables individuals to sue companies directly for violations of MHMDA, either for technical errors, damages, or injunctions.

Other Resources

An official FAQ from the Washington State Attorney General's Office on implementation of the MHMDA is available **here**. The MHMDA does not grant the Washington Attorney General formal rulemaking authority (which means that the FAQs here are informal and non-binding); however, the FAQs provide an important perspective on how the Attorney General will interpret the law.

B. Other States With Standalone Health Data Privacy Laws

While Washington's MHMDA is the trendsetter in terms of standalone health data privacy laws, other U.S. states have passed similar laws in 2023 that take aim at health data collection, processing, and sale. The pace with which these laws were enacted in 2023 is reflective of a growing interest by state legislators in strengthening protections for consumer health data.

Nevada

In June 2023, the Nevada legislature passed **Senate Bill 370**, Nevada's Consumer Health Data Privacy Law (NCHDPL), which is effective March 31, 2024. It is very similar to MHMDA, with a few notable exceptions.

Importantly, unlike the MHMDA which applies to consumer health data "that identifies the consumer's past, present, or future physical or mental health status," NCHDPL is more narrowly defined to include consumer health data "*that a regulated entity uses* to identify the past, present or future health status of the consumer."[5]

Both NCHDPL and MHMDA include additional exceptions for PHI deidentified in accordance with HIPAA; however, MHMDA leaves open the chance that a HIPAA-covered entity, or its business associate, may be subject to MHMDA requirements in its processing of consumer health data that is not PHI or de-identified PHI.

Similar to MHMDA, NCHDPL also generally bans the collection and sharing of consumer health data without a consumer's affirmative, voluntary consent (with separate consents required for collection and sharing, respectively), and would similarly prohibit the sale of consumer health data without the consumer's written authorization. It requires specific contracts between processors and covered entities, access control and security, geofencing requirements, consumer rights, etc.

Most notably, however, unlike the MHMDA, NCHDPL does not contain PRA enforcement. Instead, enforcement is solely vested with the state's attorney general.

---

[5] In addition, under NCHDPL, "consumer health data" specifically includes "information relating to:

- Any health condition or status, disease, or diagnosis.
- Social, psychological, behavioral, or medical interventions.
- Surgeries or other health-related procedures.
- The use or acquisition of medication.
- Bodily functions, vital signs, or symptoms.
- Reproductive or sexual health care.
- Gender-affirming care.
- Biometric data or genetic data related to information described above.
- Information related to the precise geolocation information of a consumer that a Regulated Entity uses to indicate an attempt by a consumer to receive health care services or products"

Any information described above that is derived or extrapolated from information that is not consumer health data, including proxy, derivative, inferred, or emergent data derived through an algorithm, machine learning, or any other means.

Connecticut

Connecticut SB 3 - Adding Consumer Health Data Protections

In June 2023, Connecticut became the first state to amend its existing comprehensive data privacy law, the Connecticut Data Privacy Act (CTDPA), to include new provisions that strengthen protections for consumer health data.

Through **SB 3**, Connecticut amended its existing comprehensive data privacy law, **Connecticut Data Privacy Act (CTDPA)**,[6] to bolster protections for the commercial use of consumer health data.

In addition to new protections for children's online safety, **SB 3**'s provisions on consumer health data will, among other things, prevent covered entities from selling or processing consumer health data without first obtaining consumer consent. Like MHMDA, it requires affirmative, freely given, opt-in consent before any person can sell or offer to sell consumer health data.

In CTDPA, protections for consumer health data result from both its classification as sensitive data and stand-alone provisions enacted via SB 3 that are directly applicable to consumer health data. Specifically, SB 3 added "consumer health data" to the CTDPA's definition of "sensitive data." Sensitive data in most state privacy laws requires clear, express consent before processing. In the revised CTDPA, consumer health data is defined as "any personal data *that a controller uses to identify* a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive sexual health data." This definition is more narrow than in MHMDA (see above).

Similar to MHMDA, although narrower, SB 3 has a geofencing provision that prevents anyone from establishing a virtual boundary that is within 1,750 feet of any mental health facility or reproductive or sexual health facility for the purpose of identifying, tracking, collecting data from, or sending any notification to a consumer regarding the consumer's consumer health data.

Similar to the access controls in MHMDA and NCHDPL, CTDPA also puts obligations on controllers to ensure their personnel and employees are properly handling consumer health data. CTDPA covered entities are prohibited from allowing any employee or personnel to access consumer health data without first requiring said employee or personnel to sign a confidentiality agreement (or ensuring they are subject to a statutory duty of confidentiality).

The newly-enacted health data privacy and children's online safety amendments in CTDPA take effect on October 1, 2024 (and not the earlier effective date of July 1, 2023, otherwise applicable to the CTDPA).

[6] Connecticut General Statutes Sec. 42-515 et. seq.

The Connecticut Attorney General **released FAQ guidance** on the new privacy rights that the CTDPA creates for Connecticut consumers, potentially indicating that the agency will be paying close attention to compliance efforts.

New York

New York's 2023 consumer health data privacy law is significantly more limited in scope than those passed in Washington, Connecticut, and Nevada. Passed as a **provision included in the SFY 2023-24 budget**, the NY law prohibits any person, corporation, partnership, or association from creating a geofence, or similar virtual boundary around any health care facility, other than its own health care facility, in New York state to deliver a digital advertisement to a user, or for the purposes of building consumer profiles, or inferring the health status, medical condition, or medical treatment of any person. The ban, which became effective on July 2, 2023, is intended to protect individuals who enter healthcare facilities from being targeted by third-party organizations with digital ads on their mobile phones or other connected devices.

As written, the New York law strictly prohibits the establishment of a geofence within 1,850 feet around any "health care facility," defined to include entities offering medical care services in addition to *any structure where such entities are located,* for the purpose of delivering any digital advertisements to a user. The law also makes it unlawful to deliver any digital advertisement to a user at or within such a healthcare facility or the structure where such a facility is located through the use of geofencing, even if the digital advertisement has no relation to health, a health condition, or health-related information.

Geofencing Prohibitions in Health Data Privacy Laws

New health data privacy laws have added specific provisions that explicitly prohibit geofencing or creating a virtual boundary around healthcare facilities for the purposes of healthcare-related advertising. This includes prohibiting identifying, tracking, and collecting data within a defined radius of a healthcare facility. Washington's law sets its geofencing prohibitions at 2,000 feet or less from the perimeter of the physical location, while New York's is 1,850 feet, and Nevada's and Connecticut's are 1,750 feet.

Also worth noting, the New York law's broad geofencing provisions makes it unlawful to deliver any digital advertisement to a user at or within such a healthcare facility or the structure where such a facility is located through the use of geofencing, even if the digital advertisement has no relation to health, a health condition, or health-related information.

C. Comparing Standalone Health Data Privacy Laws to Existing Comprehensive State Data Privacy Laws

State privacy laws are comprehensive, omnibus-style laws. As such, they do not narrowly regulate consumer health data or any single industry but extend across the entire private sector. As of February 2024, there are 15 comprehensive data privacy laws in CA, CO, CT, DE, FL, IA, IN, MT, NH, NJ, OR, TN, TX, UT, and VA.[7] In addition, states including California, Colorado, New Hampshire, and New Jersey have or will have implementing regulations issued for their respective laws.

4A's Exclusive State Privacy Law Guidance Document

To assist agencies in their state privacy law compliance efforts, the 4A's partnered with Venable LLP to offer an **exclusive guidance document** to help agencies compare and contrast U.S. state privacy laws taking effect in 2023, understand the laws' consumer data rights and requirements, and consider practical tips and next steps for developing policies, procedures, and contracts to comply with these laws. The document focuses on the obligations these laws may impose upon agencies related to the personal information agencies collect and process, both on behalf of clients and for their own purposes.

Definition of Sensitive Information

U.S. state privacy laws recognize certain kinds of information collected from consumers as sensitive and deserving of heightened protection. However, each state privacy law's definition of what constitutes sensitive data is slightly different. The definition of sensitive data in the Indiana, Tennessee, Montana, Florida, Texas, Oregon, and Delaware privacy laws remains relatively uniform.

Notice and Consent for Collection, Processing, and/or Sale of Sensitive Information

In addition to variances in how sensitive data is defined within each law, state privacy laws impose different requirements related to sensitive data collection and use. There are also variances in state privacy laws concerning whether consumer opt-in consent is required for the processing of sensitive information.

[7] Worth noting, Nevada also has its own data privacy law, which is not as robust and comprehensive as those in other states, as it only covers opt-out of sale rights for Nevada consumers' personal information from website operators. Traditional consumer rights such as access, correction, deletion, portability, etc. found in other bills are not present in Nevada privacy law. The concept of sensitive data, and any special considerations for it, are also not present in the law. As such, it is excluded from the analysis in this section.

State privacy laws in Colorado, Connecticut, Virginia, Texas, Florida, Oregon, Indiana, Montana, Tennessee, New Hampshire, New Jersey and Delaware all define sensitive data to include certain health data and require express, opt-in consent from a consumer before the processing of sensitive information. In addition, Florida requires all for-profit entities to obtain express consumer consent for the sale of sensitive data.

Conversely, the California, Iowa, and Utah privacy laws require companies to provide consumers with notice of sensitive data processing and the choice to opt out of the processing of most types of sensitive data.

Consumer Rights Requests

In addition to requiring opt-in consent for the processing of sensitive information, most state privacy laws also require opt-out rights for the sale of personal information, targeted advertising and profiling (the latter in some states only). There are specific requirements in state privacy laws as it relates to responding to opt-out requests including timelines, verification, etc.

Similarly, because a consumer's health data is collected as part of the buckets of what is considered "sensitive information" or "personal information", the consumer health data would be subject to the various consumer rights found in U.S. state privacy laws (i.e. right to access, right to delete, right to portability, right to know, right to correction, right to appeal, etc.). These rights are governed by specific controller procedures found in state privacy laws.

Notable Exemptions - HIPAA, Non-profits, and Government Entities

State privacy laws to date have routinely provided for certain exemptions. The most significant exemptions are tied to four federal laws: the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Act (GLBA), Family Educational Rights and Privacy Act (FERPA), and the Fair Credit Reporting Act (FCRA). Employment data and business-to-business (B2B) data have also traditionally been exempted, except in California's privacy law. State privacy laws also commonly exempt state and local government agencies,[8] nonprofit organizations, and institutions of higher education, except in a few cases for the latter two.

To date, all the state privacy laws have some kind of HIPAA-related exemption established, as outlined in the chart on the following page.

[8] Most states that have exemptions for state agencies or political subdivisions of the state but do not explicitly exempt the business partners of those agencies/subdivisions. Some states do, however. Utah and Indiana, for example, exempt "a governmental entity or a third party under contract with a governmental entity when the third party is acting on behalf of the governmental entity."

HIPAA Exemptions in State Data Privacy Laws	
California	Exempts (1) "medical information" governed by the CA Confidentiality of Medical Information Act (CMIA); (2) "protected health information" under HIPAA; (3) "providers of healthcare" (CMIA) and HIPAA-covered entities to the extent they protect patient data as required by the CMIA and HIPAA, respectively; and (4) certain clinical trial data and biomedical research. It also exempts HIPAA de-identified information derived from PHI except in places contracting restrictions on sale or license of HIPAA de-identified information, which applies to non-profits.
Virginia	Data-level and entity-level exemptions. Exempts covered entities and business associates, as those terms are defined by HIPAA. Exempts PHI, as defined under HIPAA. Health records, such as those held by local health departments and utilities. Patient identifying information (PII) already subject to confidentiality requirements under 42 U.S. Code § 290dd–2. Identifiable private information for the protection of human subjects under 45 CFR Part 46. information originating from, and intermingled to be indistinguishable with, PHI or certain other exempt information that is maintained by a healthcare facility or healthcare provider or by a program or qualified service organization under Part 2 of the Confidentiality of Substance Use Disorder Patient Records regulations. Healthcare-related information that is deidentified (pursuant to the deidentification requirements of HIPAA). Information used only for public health activities and purposes as authorized by HIPAA.
Colorado	Data-level exemptions. Exempts PHI, as defined under HIPAA. Exempts information and documents created by a covered entity for the purposes of complying with HIPAA. Exempts HIPAA de-identified information derived from PHI, and certain other types of health-related information.
Connecticut	Data level and entity level exemptions. Exemption largely tracks Virginia law.
Utah	Data level and entity level exemptions. Exemption largely tracks Virginia law.
Iowa	Data level and entity level exemptions. Exemption largely tracks Virginia law.
Indiana	Data level exemptions. Exempts PHI, as defined under HIPAA; Exempts information processed by HIPAA-covered entities or their business associates. Exempts data that is intermingled with and indistinguishable from HIPAA-covered PHI. Exempts HIPAA de-identified information derived from PHI. Exempts various other data uses related to health and medical research. Information used for public health activities and purposes as authorized by HIPAA.
Tennessee	Data level and entity level exemptions. Exemption largely tracks Virginia law. Provides specific entity-level carve-out for insurance companies, entirely exempting all insurance companies licensed under Tennessee law.
Montana	Data level and entity level exemptions. Exemption largely tracks Virginia law
Texas	Data level and entity level exemptions. Exemption largely tracks Virginia law
Florida	Data level and entity level exemptions. Exemption largely tracks Virginia law
Oregon	Data level exemptions. Exempts PHI, as defined under HIPAA; Exempts information processed by HIPAA-covered entities or their business associates. Exempts data that is intermingled with and indistinguishable from HIPAA-covered PHI. Exempts HIPAA de-identified information derived from PHI. Exempts various other data uses related to health and medical research. Information used for public health activities and purposes as authorized by HIPAA.
Delaware	Data level exemptions. Exempts PHI, as defined under HIPAA; Exempts information processed by HIPAA-covered entities or business associates. Exempts data that is intermingled with and indistinguishable from HIPAA-covered PHI. Exempts HIPAA de-identified information derived from PHI. Exempts various other data uses related to health and medical research. Information to the extent it is used for public health, community health, or population health activities and purposes, as authorized by HIPAA, when provided by or to a Covered Entity or when provided by or to a Business Associate pursuant to a Business Associate Agreement with a Covered Entity.
Washington	Data level exemptions. The Act provides several data-level exemptions including, but not limited to, exemptions for protected health information as defined under HIPAA, publicly available information (which is excluded from the definition of "personal information"), certain personal information used for research in the public interest as well as identifiable private information for purposes of the federal policy for the protection of human research subjects (among other research-related data-level exemptions).the Act also includes a separate and more fulsome carve-out for data that is deidentified to the standard set forth in HIPAA. It also includes a couple of special circumstances exemptions, focused on information used for public health activities as well as on data that is part of a HIPAA limited data set (which may be used or disclosed for research, public health, or health care operations purposes if certain conditions are met). Includes exemptions for certain information maintained by HIPAA covered entities or business associates, or by health care facilities or health care providers as defined under Washington law. It also provides data-level exemptions for personal information subject to the Washington Health Benefit Exchange.
Nevada	Data level and entity level exemptions. Exempts entities subject to HIPAA. Exempts data related to the Health Care Quality Improvement Act. Additionally, there are exemptions for specific data collected for clinical research, deidentified data, and PHI governed by HIPAA.
New Jersey	Data level exemptions. Exempts PHI collected by HIPAA-covered entities or their business associates.
New Hampshire	Data level and entity level exemptions. Exemption largely tracks Virginia law.

While most state privacy laws blanket exempt personal health information (PHI) as defined by HIPAA, healthcare providers (or their business agents) may still have obligations under these laws with respect to other personal information, such as employee information or website data.

Data Protection Assessments

Consumer privacy laws in Colorado, Connecticut, Virginia, Montana, Indiana, Tennessee, Texas, Florida, Oregon, Delaware, New Jersey, and New Hampshire each require data protection assessments (DPA)[9] for any information processing practices that may create a risk of harm to a consumer.

Several state data privacy statutes mandate that a DPA be conducted if an organization intends to sell personal data or use it for targeted advertising, although the specific requirements for what triggers a DPA varies by law.

Some states also require DPAs when processing personal information for profiling with a reasonably foreseeable risk of (a) unfair or deceptive treatment; (b) unlawful disparate impact on consumers; (c) financial physical or reputational injury; (d) physical or other form of intrusion on solitude or seclusion in which the intrusion would be offensive to a reasonable person; or (e) other substantial injury. DPAs are also required when a controller processes sensitive information which can contain consumer health data per the "sensitive data" definition. The amended Connecticut bill explicitly includes a requirement for DPAs when processing "consumer health data."

Most state privacy laws require a company's DPAs to be available to a state's attorney general upon request, although the CPPA is considering annual DPA submissions to CPPA as part of its proposed rulemaking process.

D. Best Practices For Agencies

The recommendations below may or may not be relevant depending on an agency's role as a controller, third party, or service provider as defined in statute. See the 4A's 2023 state privacy guidance **here** for recommendations on how to determine a company's entity status under existing state privacy laws.

- Identify whether the organization is collecting consumer health data. Because the term "consumer health data" is expansive, many businesses that are not traditionally healthcare-focused or considered healthcare companies may be collecting covered data.
- Evaluate where current disclosures, consent mechanisms, or other compliance efforts may already address certain requirements of each state privacy law and/or whether they can be updated for the purposes of compliance with both comprehensive state privacy laws and healthcare-specific data privacy laws.

[9] An alternative term for DPAs defined in some state laws is "data protection impact assessment" (DPIA).

- Limit internal and external access to sensitive or consumer health data to only those individuals that really need it.
- Consider requiring two-factor authentication to improve data access security. This should include client-side websites, databases, and marketing platforms.
- Review client master services agreements and data processing contracts for indemnification clauses to better understand legal liability associated with breaches of data protection obligations.
    - Review related agreements with any third-party that may be collecting, processing, or sharing client data.
    - Consult with the legal team in the event of breaches, or as necessary, to review data contracts and agreements for potential breach liability.
- Consider purchasing or bolstering data breach insurance and cyber liability coverage to be added to the agency's business insurance policy. Contact **4A's Benefits** for guidance and more information on available policies in the marketplace.
- Begin building required notices, consents, and authorizations for consumer health data and sensitive data collection, processing, sale, etc.
    - Review proscribed website and notice language and procedures for filing consumer complaints spelled out in state laws.
- Design a consumer health data privacy policy (which will likely require companies to undergo some data mapping in advance).
    - Consumer health data privacy policies will likely require frequent review with evolving consumer health data processing uses and changes in affiliates.
- Review and potentially eliminate uses of cookies, pixels, and web beacons on sites or ads that may be collecting "consumer health data."
- Obtain consent from consumers prior to the collection, processing, sale, or sharing of any consumer health data.
- Develop and implement a secure and reliable mechanism for receiving and processing consumer health data rights requests.
- Establish deletion and consent revocation flow-down procedures with affiliates, business partners, etc. and mechanisms to delete consumer health data from backup systems and archives.
- Prior to processing, perform a data protection impact assessment for activities that involve processing consumer health data or sensitive information.
- Cease operations of any geotargeting in and around healthcare facilities within all states' law-defined radii.

III. Federal Regulatory Landscape

While Congress has recently considered comprehensive privacy legislation, no proposal has advanced to date. Given the high level of bipartisanship on children's online safety and health data privacy, these are the two most likely policy areas under the data privacy reform umbrella that could advance in the years ahead without a larger data privacy package.

While Congress decides its next move on data privacy, the Biden Administration has taken up the banner to establish a stronger federal regulatory paradigm by way of new regulations, enforcement actions, and reinterpretation of current policies via advisory opinions. If President Biden wins a second term in 2024, experts expect these new actions to ramp up. The Biden Administration views health data privacy as an imperative following the *Dobbs* decision.

To that end, the Biden-era FTC has recently been taking a larger role in regulating the use of consumer health data and has been using the tools at its disposal – namely, the Health Breach Notification Rule (HBNR) and the Federal Trade Commission Act (FTC Act) – to enforce against businesses that misuse or share consumer health information without individuals' authorization.

At A Glance - Federal Regulatory Landscape

In the absence of action by Congress to enact a federal, preemptive privacy law, the FTC and HHS OCR have taken aggressive steps to regulate the commercial use of consumer health information. A December 2022 HHS OCR Bulletin on Online Tracking Technologies instituted a new ban on the use of cookies, pixels, web beacons, etc. by HIPAA-regulated entities when they would result in impermissible disclosures of PHI. Ongoing utilization of data tracking technologies on websites and mobile applications operated by healthcare organizations and other HIPAA-regulated entities has triggered investigations by federal regulators and the media into potential HIPAA violations.

The FTC Act's protections for consumer health information apply to HIPAA-covered entities and business associates, as well as to companies that collect, use, or share health information that are not HIPAA-covered. The new Health Breach Notification rule expands what is considered a "breach" to include unauthorized sharing or acquisition of covered health information by non-HIPAA covered entities such as health apps or connected devices

Recent enforcement actions against BetterHelp, GoodRx, and Premom, the FTC has put healthcare companies on notice that they must keep watch on health data flows to third parties that use tracking technologies integrated into websites and apps. Privacy notices, privacy attestations, as well as establishing formal processes to obtain affirmative, express consent for any collection and selling of covered health information should be a key area of compliance focus for agencies.

[10] Executive Order No. 14076, Protecting Access to Reproductive Healthcare Services. (2022, July 8). The White House. https://www.federalregister.gov/documents/2022/07/13/2022-15138/protecting-access-to-reproductive-healthcare-services

A. HHS OCR Bulletin on Online Tracking Technologies

In December 2022, HHS OCR issued a **new guidance bulletin** regarding the use of online tracking technologies (i.e. cookies, web beacons, and pixels) by covered entities and business associates under the HIPAA **Privacy**, **Security**, and **Breach Notification Rules**. Under 45 CFR 160.103 of HIPAA, a "covered entity" is defined as a health plan, a health care provider, or a health care clearinghouse.

The guidance bulletin was issued amid a flurry of class action lawsuits, state and federal regulatory inquiries, and media investigations regarding the utilization of data tracking technologies on websites and mobile applications operated by healthcare organizations and other HIPAA-regulated entities.

The guidance has far-reaching implications for HIPAA-regulated entities that utilize online platforms, and as a result, many organizations are required to update their use of tracking technologies in order to maintain compliance with HIPAA. This guidance represents a novel interpretation of a longstanding HIPAA statute.

What's Covered Under the New Guidance

The guidance analyzes how the HIPAA rules apply to user-authenticated web pages (i.e., when user login is necessary before the user can access the webpage), unauthenticated webpages (i.e., publicly-available websites that do not require a user login to access the webpage) and mobile apps; it also makes it clear that "[HIPAA] regulated entities are not allowed to use tracking technologies in a way that would result in impermissible disclosures of PHI, or any other violations of the HIPAA rules."

The guidance details the circumstances in which data collected by online tracking technologies is considered PHI, indicating it will be contingent upon the website or mobile app (and, in some instances, the page or screen within that website or mobile app) through which the data was collected and the overall context.

Personal Health Information

The HHS OCR reiterates throughout the guidance bulletin that HIPAA applies when covered entities collect user data that includes PHI via tracking technologies and also if such data is then shared with technology vendors. Per the guidance bulletin, PHI would include "individually identifiable health information" (IIHI), such as an individual's medical record number, home address, email address, or appointment dates, as well as an individual's IP address or geolocation, medical device ID, or any unique online or mobile identifying code. IIHI collected on a regulated entity's website or mobile app generally is PHI even if the user does not have an existing relationship with the covered entity and even if the IIHI does not include specific treatment or billing information (e.g., appointment dates or type of healthcare services).[11]

[11] All PHI is IIHI, but not all IIHI is PHI. This is because HIPAA does not protect all individually identifiable health information. The IIHI has to be transmitted or maintained in some form to be protected, qualifying it as PHI. IHII is health information that can be linked to a specific person, or if it would be reasonable to believe that an individual could be identified from the information.

User-Authenticated Web Pages

Per the guidance bulletin, a covered entity must configure any user-authenticated webpages (i.e. those that utilize user logins) that include tracking technologies to allow such technologies to only use and disclose (and secure) PHI in compliance with HIPAA.

Important for agencies, tracking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (i.e. health care operations) or to provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI.

Unauthenticated Webpages

This category includes publicly available pages that allow anyone to access the content and typically only contain basic information about a covered entity. Per the guidance bulletin, tracking on these types of web pages is generally not regulated under HIPAA. In some cases, the guidance states tracking technologies on such unauthenticated webpages may have access to user PHI and may disclose such data to outside vendors, thus triggering the HIPAA Rules.

Mobile Apps and Tracking

The guidance bulletin states that information typed in by a user, as well as device-level data (e.g., network location, geolocation, device ID, advertising ID, etc.) collected by a covered entity must comply with HIPAA for any PHI the mobile app uses or discloses. The guidance bulletin states that HIPAA applies to "any PHI collected by a covered health clinic through the clinic's mobile app used by patients to track health-related variables associated with pregnancy....", a clear nod to the recent Supreme Court *Dobbs* Decision.

Compliance Obligations

The guidance bulletin reiterates that regulated entities are mandated to comply with the HIPAA Rules when using tracking technologies and reminds covered entities to make sure that "all disclosures of PHI to tracking technology vendors are specifically permitted by the Privacy Rule and that, unless an exception applies, only the minimum necessary PHI to achieve the intended purpose is disclosed."

HHS OCR urges covered entities to " evaluate [their] relationship with [] tracking technology vendor[s] to determine whether such vendor[s] meets the definition of a business associate and ensure that the disclosures made to such vendor[s] are permitted by the Privacy Rule." The HHS OCR ends the guidance bulletin with some additional compliance reminders for regulated entities that use tracking technologies.

HHS OCR / FTC Joint Letter Notice To Companies of Risks of Tracking Technologies

In July 2023, the FTC and HHS OCR sent a **joint letter** to approximately 130 hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities.

In their letter, both agencies reiterated the risks posed by the unauthorized disclosure of an individual's personal health information to third parties. For example, the disclosure of such information could reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, and where an individual seeks medical treatment. The two agencies cautioned that online tracking technologies may continue to gather identifiable information about users even after the users navigate away from the original website to other websites and that they can gather identifiable information about users without their knowledge and in ways that are difficult for users to avoid.

The agencies reaffirmed that companies not covered by HIPAA still have a responsibility to protect against the unauthorized disclosure of consumer health information—even when a third party developed their website or mobile app.

More details **here**.

Resources for HIPAA Guidance:

- **HIPAA and Google Analytics**
- **Health Apps**
- **Privacy Rule**
- **Security Rule**
- **Business Associate Contracts**
- **FTC Technology Blog: Hidden Impacts of Pixel Tracking (March 2023)**

B. FTC Health Breach Notification Rule

The FTC's recent interpretation of the Health Breach Notification Rule (HBNR) is a novel reading of the decade-old regulation and one that has big ramifications for any company found to be in violation. Companies that fail to comply with the HBNR could be subject to monetary penalties of up to about $43,792 per violation per day. When multiplied by millions of affected users, companies may face substantial financial harm for any companies violating the law.

2021 Policy Statement on Health Breach Notification Rule

In September 2021, the FTC issued a Policy Statement that was intended to clarify the scope of the FTC's HBNR. The purpose of HBNR, finalized in 2009, was to hold non-HIPAA entities accountable in cases of health data breaches by requiring them to notify relevant stakeholders, such as U.S. consumers and the FTC. The 2021 Policy Statement was intended to extend HBNR's applicability to a large number of technology companies and activities, including health apps.

This Policy Statement did not change the HBNR's existing definitions; however, it hinted that the FTC intended to expand enforcement under the HBNR, and it interprets the following elements more broadly: (1) covered entities, (2) covered health information, and (3) breach of security.

New Proposed Rulemaking on the Health Breach Notification Rule

On May 18, 2023, the FTC **announced** a **proposed rule to amend HBNR**. The proposed changes are primarily intended to clarify the scope of entities subject to the HBNR and what constitutes a breach that triggers the rule's notification requirements. The HBNR requires covered companies to give notice of a "breach of security" to affected individuals, the FTC, and, in some cases, the media. From a tactical perspective, the proposed rule attempts to align the FTC's expansive HBNR interpretation with recent FTC enforcement actions concerning consumer health data.

The NPRM is just the latest move in the FTC's efforts to regulate this space and ensure that businesses not regulated by HIPAA do not use and share health information in contravention of consumers' wishes and expectations. With the FTC's renewed interest in enforcing the HBNR, the NPRM should pique the interest of many businesses in the healthcare space.

A final HBNR is expected from the FTC in 2024.



Health Breach Breach Notification Rule- Important Applications for Agencies

Agencies assisting clients in the healthcare wearables and app space need to understand revised security breach definitions and consumer consent requirements in order to prevent what regulators may perceive as breaches.

C. FTC Enforcement Actions Concerning Health Data Privacy

Since 2021, the FTC has signaled its eagerness to enforce the HBNR and other perceived violations of consumer privacy under the FTC Act such as the sharing of consumers' sensitive location data and personal health information.

While not covered in this paper, we also recommend healthcare marketers review recent FTC enforcement actions concerning **Premom** and **Flo Health**, reproductive healthcare app companies who both allegedly shared fertility and reproductive health data with third parties for advertising purposes without first obtaining users' consent.

FTC Lawsuit Against Data Broker Kochava (Precise Location Data)

The FTC **filed a lawsuit against data broker Kochava Inc.** in August 2022 for selling the geolocation data of hundreds of millions of mobile devices that can be used to trace the movements of individuals to and from sensitive locations. Kochava's data allegedly could reveal people's visits to reproductive health clinics, places of worship, homeless and domestic violence shelters, and addiction recovery facilities. The FTC alleges that by selling data tracking people, Kochava was enabling others to identify individuals and exposing them to threats of stigma, stalking, discrimination, job loss, and even physical violence. The FTC's lawsuit seeks to halt Kochava's sale of sensitive geolocation data and require the company to delete the sensitive geolocation information it has collected.

In May 2023, an Idaho federal judge ruled that the FTC needs stronger assertions of consumer harm in order for its data privacy suit against Kochava Inc. to proceed. The judge sided with Kochava's argument that the agency had not adequately supported its claim that the company's sales of geolocation data constituted unfair conduct under Section 5 of the FTC Act, finding no allegations that the practices "created a 'significant risk' of concrete harm." The court simultaneously found no basis for Kochava's suit to block the FTC's enforcement action. The FTC **refiled its amended lawsuit** in June 2023. The outcome of that amended suit is still TBD as of the publishing date of this paper. More details on the legal case are available **here**.

> **Takeway:** This enforcement action seems to indicate that the FTC is adopting an assertive stance on commercial use of sensitive personal data (especially sensitive location data), while looking to widen the net of its authority over unfair practices. This case will set the tone for enforcement towards the data broker business model. Data brokers, and any businesses dealing in sensitive personal data from consumers (such as precise geolocation data and consumer health data) should examine their data collection, use, and disclosure practices, and review their technical, administrative, and physical controls.

FTC Enforcement Action Against GoodRx

In February 2023, the FTC **announced an enforcement action** for the first time under its HBNR against the telehealth and prescription drug discount provider GoodRx Holdings Inc. The agency began investigating GoodRx after Consumer Reports published **an article** in February 2020 about the company's data sharing practices. The publication used sophisticated traffic monitoring software to examine how the company utilized its app to collect, disclose, and sell its customers' data, including data generated from searches for antidepressants, fertility treatments, and other sensitive medication.

According to the **FTC complaint**, GoodRx, which the FTC considers a "**vendor of personal health records**" under HIPAA, failed to notify consumers and the media of its unauthorized disclosures of consumers' personal health information to Facebook,[12] Google, Criteo, and other advertising companies—in direct contradiction of its privacy promises—and as required by the HBNR. Under the HBNR, following the discovery of a breach of security of unsecured PHR identifiable information, vendors shall notify each individual whose unsecured personal health records (PHR) were acquired. Since GoodRx had not collected affirmative, express consent from its users to authorize the sharing of their PHR data with third parties, the sharing — even for somewhat limited purposes — was a "breach" in violation of the HBNR.

Over a period of four years, GoodRx repeatedly disclosed users' sensitive personal health information about chronic physical or mental health conditions, medical treatments and treatment choices, life expectancy, disability status, information relating to parental status, substance addiction, sexual and reproductive health, sexual orientation, and other highly sensitive and personal information without their consent.

Per the action, GoodRx was assessed a $1.5 million civil penalty for violating the rule.

[12] In early 2020, Facebook found GoodRx had violated its platform policies for advertisers, which prohibit ad content that asserts or implies personal attributes including physical or mental health conditions. Despite this, the FTC complaint alleges, GoodRx continued to share information with third parties until November 2020.

> **Takeway:** This case signals a shift in the FTC's use of its unfairness authority in privacy cases, with some important takeaways for privacy programs that handle health-related data. It asserts a novel application of the HBNR against digital health services, which often fall outside the scope of HIPAA.

FTC Enforcement Action Against BetterHelp

In July 2023, the FTC **finalized an order** banning online counseling service BetterHelp, Inc. from sharing consumers' health data, including sensitive information about mental health challenges, for advertising purposes. Per the order, which covers the company's advertising practices that were in effect between 2017 to 2020, BetterHelp agreed to pay $7.8 million to consumers to settle charges that it revealed consumers' sensitive data to third parties despite promising consumers that it would only use or disclose personal health data for limited purposes.

According to the **FTC's complaint**, repeatedly throughout the signup process, BetterHelp promised consumers that it would not use or disclose their personal health data except for limited purposes, such as to provide counseling services.

Despite those attestations, BetterHelp used and revealed consumers' email addresses, IP addresses, and health questionnaire information to Facebook, Snapchat, Criteo, and Pinterest for advertising purposes. The FTC found BetterHelp's disclosures to be deceptive because statements in the sign up process and BetterHelp's privacy policy created the impression that information would not be shared. Various forms of disclosures, in particular about cookies, were said to be misleading.

The complaint also alleges that BetterHelp actively shared details regarding certain individuals with Facebook and requested that Facebook use its "look-alike" tool to profile the individuals and market to those with similar characteristics.

The FTC found that the company did not properly train its employees regarding using information for advertising and failed to properly supervise its staff's use of the data. The FTC complaint alleges that BetterHelp agreed to the stock wording of third-party contracts and failed to negotiate for special protection for health data.

BetterHelp displayed HIPAA seals on numerous web pages. Its sales representatives told consumers that the company was "HIPAA certified." According to the order, no third party reviewed the company's information practices to determine whether they complied with HIPAA. Additionally, the FTC observed that many of the company's therapists are not subject to HIPAA and that the company does not know which data is protected by HIPAA and which is not. As such, the FTC complaint determined that displaying a seal implying compliance with the Health Insurance Portability and Accountability Act (HIPAA) was deceptive.

> **Takeway:** This FTC enforcement action reinforces the federal government's position that an email or an IP address by themselves can disclose private information about consumers based on the entity sharing the data. Healthcare companies and their agencies should make sure they keep whatever privacy promises have been made to consumers regarding their data sharing and use.

D. Best Practices For Agencies

Breach Notification, Privacy Programs, Data Sharing, and Consent Framework

- Agencies and their clients should determine whether the HBNR applies to their organization and if necessary, update incident response and breach response policies and procedures;
- If applicable, companies should perform data mapping to understand the data collected from consumers and identify the purposes for which it is used and shared, taking into account what identifiable health information can be inferred by the data collected using tracking technologies and other marketing services;
- Consider the risks of making public representations regarding HIPAA compliance and other privacy and security measures before making them, and update any existing statements that are misleading or inaccurate;
- Monitor and audit third party disclosures of IIHI for compliance with applicable laws; and
- Review current and prospective contracts with third parties to ensure applicable data sharing provisions are in compliance with applicable laws, the company's information privacy and security policies, and procedures, and public representations. Contract language to limit processing scope is key.

Online Tracking Technologies

- Perform an analytics audit to find any tracking issues that could be exposing an organization to a HIPAA violation, including legacy pixels. This should be done in collaboration with an advertiser's IT team.
- Re-evaluate data sharing practices with tracking technology vendors or the use of tracking technology itself for compliance. Contextual advertising, cookieless targeting, article-based context, page-level Metadata, and modeled script segments exist as possible alternatives.
- Create a formal process for implementation of any new tracking on the advertisers site. This should require internal review, review with the IT team, and reviews with the legal team.
    - If online tracking technologies must be used, identify pages on the site that do not relate to the provision of health care services. Unauthenticated pages that are related to the provision of health care services, including as described in the HHS bulletin, are more likely to be HIPAA-covered, and marketers should not set analytics tags on HIPAA-covered pages.
- Set up a clean room approach with data partners to build modeled, probabilistic audiences for advertisers; this prevents a marketer from ever targeting the actual patients whose data was used for modeling.

E. HHS/FTC Resources Available To Companies

- FTC Health Privacy Page
- HHS OCR Bulletin on Online Tracking Technologies
- FTC Blog for Businesses: FTC-HHS Joint Letter Gets to the Heart of the Risks Tracking Technologies Pose to Personal Health Information
- FTC Blog for Businesses: First FTC Health Breach Notification Rule Case Addresses GoodRx's Not-So-Good Privacy Practices
- Business Guidance: Complying with the FTC's Breach Notification Rule
- Health Breach Notification Rule: The Basics for Business
- FTC Blog for Businesses: Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data
- FTC Blog for Businesses: FTC Says Data Broker Sold Consumers' Precise Geolocation, Including Presence at Sensitive Healthcare Facilities
- FTC Guidance Health Mobile Apps
- FTC Blog for Businesses: Health AppDevelopers: Updated Interactive Tool Can Help You Get Started on Compliance
- FTC Blog for Businesses: Protecting the Privacy of Health Information: A Baker's Dozen Takeaways from FTC cases

IV. Putting Agency HIPAA Compliance into Practice

As healthcare marketing agencies grow their reach through online avenues and serve more personalized experiences through targeted advertisements, the need for understanding HIPAA regulations grows as well. As noted earlier, the fines for HIPAA incompliance can be harsh. As of December 2023, there have been a recorded **348,887 HIPAA violations**.

HHS OCR recently delivered two reports to Congress in early 2023 regarding HIPAA compliance and breaches of unsecured health information; the report **revealed** that between 2017 and 2021, complaints about violations of HIPAA increased 39% and large breaches reported increased by 58%. HHS OCR **received** 609 notifications of events affecting 500 or more individuals that reached approximately 37.2 million individuals in total. Breaches affecting less than 500 individuals reported only affected a total of 319,215 individuals.

Implementing compliance processes into your business and screening other vendors for HIPAA compliance may seem daunting. By implementing an internal agency HIPAA compliance management process, exerting external vendor due diligence, and signing specific BAAs, an agency can reduce its liability and risk.

At A Glance - HIPAA Compliance Software Vendors and Certification

Comprehensive compliance software solutions can help agencies navigate the nuances of HIPAA, the HITECH Act breach notification requirements, and evolving state privacy laws.

Compliance software helps an agency demonstrate to regulators that they have taken good faith steps to meet the legal requirements of HIPAA and federal and state privacy laws by establishing necessary recordkeeping and documentation of compliance activities. Moreover, to simplify compliance management, some HIPAA compliance software solutions allow their customers the ability to send self-reported audit requests to business associates, track the results of those audits, and record business associate agreements.

HIPAA compliance certification can help agencies provide assurances to their clients that policies and procedures have been introduced in line with HIPAA, showcase that an agency is fully aware of its responsibilities under HIPAA including the necessary training for its employees, and confirm that software meets or exceeds the minimum standards for privacy and security under the law. HIPAA compliance certification should improve an agency's marketability to prospective healthcare clients, substantiate an agency's security conveyances, and head off costly data breaches.

A. The Role Of HIPAA Compliance Software

HIPAA compliance software solutions help companies navigate the nuances of HIPAA and ensure all applicable provisions of the HIPAA **Privacy**, **Security**, and **HBNR** are satisfied. The software also proves a company has made a good faith effort to comply with HIPAA and state privacy laws by maintaining full documentation of compliance activities.

One of the most important elements of the HIPAA Security Rule is the risk analysis or risk assessment. The purpose of the risk assessment is to identify all risks to the confidentiality, integrity, and availability of PHI. If the risk assessment is not performed, covered-entity healthcare organizations and their business associate advertising agencies cannot be sure that all risks have been identified; this means it will not be possible to reduce those risks to a reasonable and acceptable level through the HIPAA risk management process.

Even though the risk assessment is the foundational element of HIPAA compliance, it is one of the provisions of HIPAA that causes healthcare advertising agencies the most problems. The failure to conduct an organization-wide, HIPAA-compliant risk assessment is the single most common HIPAA violation penalized by HHS OCR in its enforcement actions.

The use of HIPAA risk assessment software helps to ensure that the risk assessment is completed to the standard demanded by HIPAA, by guiding agencies through the whole process and ensuring all identified risks are tracked along with the efforts made by the company to remediate those risks.

B. Avoid Taking Shortcuts with HIPAA Compliance

Be cautious of compliance solutions that only address specific elements of HIPAA compliance, such as the risk assessment. While HIPAA risk assessment software is a great place to start, it only covers one required provision of the **HIPAA Security Rule**.

Software that only covers specific aspects of HIPAA compliance will not help healthcare clients and your agency assess and demonstrate that they are fully compliant. Even if the healthcare client and your agency are confident about their compliance programs, it is best to use a comprehensive software solution that covers all the required and addressable implementation specifications of HIPAA, the HITECH Act breach notification requirements, and evolving state privacy laws.

Comprehensive compliance software solutions have greater upfront costs. However, the efficient guiding of business associate advertising agencies through the full compliance process can reduce overall compliance costs, identify and address gaps in legal compliance, and minimize the risk of regulatory fines for noncompliance.

C. What HIPAA Compliance Software Should Do

HIPAA compliance software vendors that offer a comprehensive compliance solution will walk an advertising agency with healthcare clients through setting up, implementing, and maintaining HIPAA policies and procedures. They help to supervise staff training, and ensure all appropriate safeguards are implemented to meet HIPAA **Privacy** and **Security Rule** requirements, all the while facilitating the customization of specific BAAs.

Many HIPAA compliance software solutions offer templates for policies and HIPAA documents. While these are certainly useful and can save time, please note that HIPAA requires all policies and procedures to be specific and relevant to each organization. More comprehensive HIPAA compliance software solutions should also assist with the development of specific BAA agreements, as well as be supported by knowledgeable and available compliance staff or external expert consultants. HIPAA compliance software solutions should make it easier for policies, procedures, and HIPAA documentation to be customized to cover the specific ways that the organization creates, receives, uses, stores, and transmits PHI.

Agencies who are business associates for healthcare clients can be fined directly for HIPAA violations. A HIPAA breach at a business associate advertising agency will not only have negative implications for the agency, but also for a covered-entity healthcare client who also has a responsibility to ensure vendors are fully compliant.

Some HIPAA compliance software solutions allow covered entities the ability to send self-reported audit requests to business associates, monitor the results of those audits, and track and maintain BAAs.

HIPAA compliance software solutions should allow a business associate advertising agency to track employee HIPAA and security awareness training, ensuring that every member of the workforce has received and – where required – has attested to receiving training.

Finally, it should be noted that the use of HIPAA compliance software will not absolve companies of liability in every circumstance (i.e., in the event of an employee violating HIPAA, such as an employee stealing PHI for personal gain); however, regulators do take a covered entity's or business associate's good faith efforts to comply with HIPAA into account when deciding whether a financial penalty or other sanction is appropriate. HIPAA compliance software solutions are not guaranteed to resolve all HIPAA compliance issues.

D. What is HIPAA Compliance Certification

There is currently no officially recognized HIPAA compliance certification software, as any certification from a HIPAA compliance software vendor only confirms that a business associate agency has incorporated all of the required safeguards to meet the requirements of HIPAA Rules.

HIPAA Compliance Certification: Not a True Safe Harbor

The Children's Online Privacy Protection Act Rule (COPPA) includes a safe harbor provision that allows industry groups and others to seek FTC approval for self-regulatory guidelines that implement protections that are "the same or greater" than the COPPA Rule.

The HIPAA rule does not include a specified safe harbor for HIPAA compliance certification. However, while HIPAA compliance certifications may not be officially recognized by federal regulators, it can help a company signal that it is committed to HIPAA standards, including that it adheres to HIPAA training for its employees.

That said, many training and software companies issue HIPAA compliance certification to users that have demonstrated compliance through the use of the software. These HIPAA compliance certifications may not be officially recognized by HHS OCR and state attorneys general, but they do serve an important purpose. They provide assurances that policies and procedures have been introduced in line with HIPAA, demonstrate a company is fully aware of its responsibilities under HIPAA including the necessary training for its employees, and confirm that software meets or exceeds the minimum standards for privacy and security demanded by HIPAA.

Perhaps more importantly, agencies looking to continue making pitches to prospective healthcare clients or wanting to break into the healthcare market will need to demonstrate that they are aware of their responsibilities with respect to HIPAA and provide "reasonable assurances" to a covered entity healthcare business that they are compliant. HIPAA compliance software and any accompanying HIPAA compliance certification will help to differentiate an agency's products and services to stand out from the competition.

It can be time-consuming finding an appropriate HIPAA compliance software vendor with a product to match the agency's specific needs. There is no "one-size-fits-all" solution to HIPAA compliance, but the effort an agency puts into identifying and addressing HIPAA compliance shortfalls is likely to pay dividends in the long run.

Ensuring all aspects of HIPAA are satisfied should improve an agency's marketability to prospective healthcare clients, enhance an agency's security posture, and help prevent costly data breaches. HIPAA compliance software will ensure that no provision of HIPAA is overlooked, reporting processes are in good working order, and employee education in a rapidly evolving state privacy legislative and federal regulatory environment is a routine occurrence, thus helping an advertising agency or their clients avoid regulatory fines for noncompliance.

Agency Checklist of Nine HIPAA Compliance Recommendations

- [ ] 1. Make HIPAA Compliance a Condition for Doing Business
- [ ] 2. Adopt a HIPAA Compliance Management Process
- [ ] 3. Conduct Periodic HIPAA Risk Assessments
- [ ] 4. Incorporate Data Backup and Disaster Recovery Protocols
- [ ] 5. Create Remediation Plans to Address Deficiencies
- [ ] 6. Establish New Employee & Routine Workforce Compliance Training
- [ ] 7. Document HIPAA Compliance Efforts and Keep Records
- [ ] 8. Complete Routine Self-Audits
- [ ] 9. Quickly Report Incidents & Data Breaches to Clients And Maybe Regulators

Contact Us

Have questions about health data privacy laws and compliance? Please contact Alison Pepper, 4A's Executive Vice President of Government Relations & Sustainability, at appepper@4as.org, Amanda Anderson, 4A's Vice President of Government Relations, at aanderson@4as.org, or Jim Potter, CHC Executive Director at jpotter@cohealthcom.org.