The Washington My Health My Data Act

Blog Series by Hintze Law PLLC

Part 1: An Overview of the Act

Provides a high-level overview of the Act.

Part 2: The Scope of "Consumer Health Data"

Discusses in more detail a key element that determines the scope and impact of the Act – the definition of "consumer health data."

Part 3: The Scope of Entities & Consumers Captured by the Act

Delves into other elements of the Act that determine its broad scope and impact: the range of entities and consumers that it captures.

Part 4: Effective Dates

Discusses the effective dates of the Act, including how, at least in part due to a drafting error, some substantive provisions of the Act may come into effect much sooner than expected.

Part 5: Consent Requirements

Discusses the opt-in consent requirements for the collection, use, and disclosure of consumer health data under the Act.

Part 6: Consumer Rights

Discusses the rights consumers have under this Act, including a uniquely broad right of access, a right of deletion with few exceptions, a right to withdraw consent, and a right on non-discrimination.

Part 7: Biometric Data

Discusses the Act's impact on biometric data and technologies.

Part 8: Notice Requirements

Discusses the notice obligations under the Act, which seem to require an entirely separate notice rather than changes to an entity's existing privacy statement or privacy policy.

Part 9: The Attorney General's Guidance

Discusses the highly-anticipated, but non-binding, guidance published by the Washington State Office of the Attorney General.

Part 10: MHMDA vs. HIPAA (coming soon)

Part 1: An Overview

By Mike Hintze • April 10, 2023

This is the first in a series of blog posts about the Washington My Health My Data Act. It provides a high-level overview of the Act.

Last week, the Washington State Senate voted to approve the "Washington My Health My Data Act," a slightly modified version of the bill that was previously approved by the House. By all accounts, the Senate version of the Act will prevail through the reconciliation process and be signed by the Governor.

When signed, the Washington My Health My Data Act will become the most consequential privacy legislation enacted in 2023. And arguably, it will be ***the most consequential privacy legislation enacted since the original California Consumer Privacy Act (CCPA) was adopted in 2018***.

The Act purports to be focused on filling a gap by protecting health data not covered by HIPAA, the federal law that protects the privacy and security health data handled by hospitals, health care providers, and other enumerated "covered entities." But the Act is *very* different from HIPAA, in many ways being broader and having more onerous requirements. Thus, the Act creates enormous disparities between how personal data must be handled between HIPAA covered entities and every other type of entity. As such, it does far more than filling gaps.

The sweeping scope and extreme substantive obligations, combined with vague terms and with a full private right of action, make this Act extraordinarily challenging and risky for entities seeking to comply with its requirements.

Key Elements of the "Washington My Health My Data Act"

- Designed to protect the privacy of health data not covered by HIPAA, but is *much* broader
- Covers a very wide (and ill defined) range of personal data, entities, and consumers
- Opt-in consent for any collection, use, disclosure, or other processing of data beyond what is necessary to provide a consumer-requested product or service
- Extremely onerous authorization requirement for data "sales" which creates, in effect, a prohibition on any activity that could constitute a "sale" including 3rd-party targeted ads
- Data subject rights that go further than any other existing law in any jurisdiction, including a deletion right with virtually no exceptions

- Unique notice requirements that seem to require separate and redundant privacy statements
- A prohibition on geofencing around any facility that provides any services that meet a very broadly defined set of health care services
- A private right of action, with presumptions benefiting plaintiffs, in addition to Attorney General enforcement
- Comes into effect 31 March 2024 (for small businesses, 30 June 2024), or maybe sooner…

The Scope of the Act is Sweeping

The Act has a definition of "consumer health data" that could potentially capture virtually any type or category of personal data. The scope could encompass any data that could arguably be related to health, wellness, nutrition, fitness, or related topics. And because it includes data that could be used to infer such information, it may be hard to safely conclude that any personal data is out of scope.

There are a few narrow exceptions, primarily for data used for certain approved peer-reviewed research in the public interest, deidentified data (if all the requirements for deidentification are met), and certain publicly available data. There are also exceptions for data that is subject to certain enumerated privacy laws, most notably HIPAA, GLBA, FCRA, and FERPA.

The Act also captures a wide range of entities and consumers. It includes any entity doing business in Washington or that provides products or services that are "targeted" to consumers in Washington. Because "targeted" is undefined, it is an open question whether merely allowing consumers to access a website or online services that does not otherwise have any Washington-specific content or features will be enough. But it is likely that the scope will be interpreted broadly, capturing entities with little or no actual connection to Washington.

Likewise, with consumers, because of some odd and non-obvious definitions, the Act captures data about consumers who have no connection to Washington at all. The only connection need be that the data about them is merely processed in Washington. It is worth noting that some of the largest global cloud service providers are headquartered in Washington, with significant data center footprints in Washington. Thus, a huge amount of data about consumers outside of Washington is potentially processed in Washington.

Because of these provisions, this Act will have applicability that reaches far and wide beyond Washington State.

The Substantive Obligations of the Act are Extreme

The Act requires ***opt-in, GDPR-level consent for any collection, use, disclosure, or other processing of consumer health data beyond what is necessary to provide a consumer-requested product or service***. There is also a requirement for a separate opt-in consent for any "sharing" of consumer health data beyond what is required for a consumer-requested product or service – including any sharing with corporate affiliates. Such consents cannot be inferred, bundled with other consents, obtained as part of a terms of use or other agreement, or obtained via deceptive design.

There is an even more onerous authorization requirement for data "sales." "Sale" is defined in the way it is defined under the CCPA, which has been interpreted to include a wide range of data transfers that would not normally be thought of as a data "sale" given the usual meaning of that word – including nearly all third-party online targeted advertising. There is no reason to think that it will be interpreted any more narrowly here. The authorization requirement is so onerous (and includes a provision that sets up a near certainty of non-compliance) that it creates, in effect, ***a prohibition on any activity that could constitute a "sale" including nearly all third-party targeted advertising***.

Data subject rights include a right to know / right of access similar to that in CCPA and other laws. And there is a right of non-discrimination for consumers who request to exercise their rights.

But the deletion right is sweeping and goes well beyond what is required by any other privacy law on the planet. Specifically, ***the deletion right has virtually no exceptions***. It lacks the common exceptions found in every other law with a deletion right. There is not even an exception for situations where retention of the data is required for compliance with law. This will put companies in an impossible position of determining which law they must violate when a consumer makes a deletion request.

The deletion right also includes a passthrough requirement to send a notification of the consumer's request to all processors, affiliates, and third parties with which the consumer health data has been shared. And those ***processors, affiliates, and third parties have an absolute obligation to also delete the data***. This is the case even if one or more third parties are providing a service to the consumer that the consumer wishes to continue and the deletion would be contrary to the consumer's wishes and interests.

The Act includes a notice obligation which requires the posting of a "Consumer Health Data Privacy Policy." This notice must contain a list of enumerated disclosures, most of which will be redundant of the organization's general privacy statement. And there is nothing in the Act that suggests it can be combined with the organization's general statement, creating a ***requirement of duplicate and redundant privacy notices***. And with the requirement to include a link to the

Consumer Health Data Privacy Policy on the company's website homepage, that homepage will be getting awfully crowded with this link added to the multiple privacy links required by other privacy laws.

The Act includes a geofencing prohibition around any facility that provides in person health care services where the geofence is used 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. As already noted, the definition of "consumer health data" is broad such that it potentially includes virtually any personal data. Likewise, the definition of "health care services" is broad and includes any services "to assess, measure, improve, or learn about a person's mental or physical health."

As such, ***the prohibition on geofencing could apply to a very wide range of businesses and common business activities***. For example, given such a broad definition, a grocery store that offers nutrition tips could be providing "health care services" and that store's loyalty club app that offers coupons when entering the store could, therefore, be seen as violating this prohibition. And remember, this is an absolute prohibition – there is no provision allowing the business to obtain consent from the consumer for such activity.

The Act also includes fairly standard requirements for reasonable data security measures. The most noteworthy provision related to that is ***a very strict internal access control provision***. Regulated entities must restrict access to consumer health data by employees, processors, and contractors to that which is necessary to provide the consumer-requested product or service or for the purposes for which the consumer provided consent.

Finally, the Act includes a number of provisions related to contracts between regulated entities and processors. The required terms do not seem incompatible with what is typically in data processor / service provider contracts today – terms designed to meet the requirements of GDPR, CCPA, and other privacy laws. But it ***may warrant another look, and possibly some modest updates, to processor agreements*** to make sure those contracts are sufficient for the purposes of this Act.

Private Right of Action

The Act includes a ***full private right or action, with presumptions benefiting plaintiffs***, in addition to Attorney General enforcement. These enforcement provisions, combined with the vague and opened-ended language and near-impossible compliance standards, will inevitability result in a wave of "gotcha" lawsuits that will be enormously costly and disruptive. Companies will have to take this risk into account in determining their compliance strategies to mitigate the risk of litigation and nuisance claims.

Effective Date

The Act purports to come into effect on ***31 March 2024*** for most regulated entities, and three months later, on 30 June 2024, for small businesses. However, due to what may be drafting errors in the version of the Act passed by the Senate, the Act could be read such that ***a number of the substantive provisions might come into effect much sooner***. Unless fixed, there is a risk that these provisions – including the prohibition on geofencing, the right to delete, the opt-in consent for sharing, and others – will come into effect 90 days after the end of the current legislative session. Given the session is scheduled to end on 23 April 2023, this would mean these provisions could come into effect 22 July 2023. That conclusion is contrary to the stated legislative intent, but it is foreseeable that aggressive plaintiffs' lawyers will not hesitate to test and exploit it.

Part 2: The Scope of "Consumer Health Data"

By Mike Hintze • April 12, 2023

This is the second in a series of blog posts about the Washington My Health My Data Act. This part discusses in more detail a key element that determines the scope and impact of the Act – the definition of "consumer health data."

The substantive requirements of the Washington My Health My Data Act apply to collection, use, and disclosure of "consumer health data." Because the definition of that term is so key to the Act's broad scope and impact, no other aspect of the bill was as actively discussed and debated as it made its way through the legislative process.

What Data is Excluded?

Before describing what *is* included in the definition of "consumer health data," I'll first note what is not included.

First, there are ***exceptions for data subject to certain enumerated privacy laws, most notably HIPAA, GLBA, FCRA, FERPA,*** and several existing Washington state laws related to health care and insurance. The HIPAA exception is particularly important here, as this covers nearly all health information processed by a HIPAA covered entity (hospitals, clinics, pharmacies, other health care providers, health insurance providers, etc.) or a "business associate" processing the data on behalf of a covered entity. The Act even excludes data that may not be covered by HIPAA, but that originates from and is maintained by a covered entity or business associate which it intermingles with HIPAA-covered data. This exclusion aligns with the stated intent of the Act to protect data that is not protected by HIPAA. But as noted in Part 1 of this blog series, this Act is very different from HIPAA, in many ways being broader and having more onerous requirements. Thus, the Act creates enormous disparities between how personal data must be handled between HIPAA covered entities and every other type of entity.

Second, because "consumer health data" is data about "consumers," and the definition of "consumer" does not include individuals acting in an employment context, ***employee and B2B data should be considered out of scope***.

Third, within the definition of "consumer health data" itself, there is a ***narrow exception for data used for certain approved peer-reviewed research*** in the public interest.

Finally, by virtue of "consumer health data" being limited to "personal information" ***the exclusions of "deidentified data" and "publicly available" information from the definition of "personal information" also excludes them from "consumer health data."*** For data to be considered "deidentified" under the Act, it must meet the following definition:

> "Deidentified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable consumer, or a device linked to such

> consumer, if the regulated entity or the small business that possesses such data (a) takes reasonable measures to ensure that such data cannot be associated with a consumer; (b) publicly commits to process such data only in a deidentified fashion and not attempt to reidentify such data; and (c) contractually obligates any recipients of such data to satisfy the criteria set forth in this [definition].

For data to be considered "publicly available information" under the Act, it must meet the following definition:

> "Publicly available information" means information that (a) is lawfully made available through federal, state, or municipal government records or widely distributed media, and (b) a regulated entity or a small business has a reasonable basis to believe a consumer has lawfully made available to the general public.

The way the "publicly available information" definition is drafted creates some confusion and ambiguity. Normally, the "and" between parts (a) and (b) of the definition would suggest that both (a) and (b) must be satisfied. But that results in a nonsensical reading that would capture little or no actual data. For instance, when information is "is lawfully made available through … government records" it is the government making the data available, not the consumer. So, part (a) is met, but not part (b). If the "and" was intended to require that both prongs be met, the definition would have simply said that the regulated entity must have a reasonable basis to believe that a consumer has lawfully made the information available to the general public though government records or widely distributed media. But it did not, which suggests that the "and" is best interpreted as an "or." Of course, given the private right of action under this Act, relying on sensible interpretations of ambiguous terms is risky.

Thus, as a result of the additional requirements necessary to consider data to be deidentified (public commitments and contractual restrictions) and the ambiguities around what constitutes publicly available data, these exceptions may in practice be quite narrow as well.

What Data is Included?

As included in the latest version of the Act, passed by the Senate last week, ***the definition of "consumer health data" is extremely broad and open-ended***. It begins with a general definition, as any personal information "that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."

The definition goes on to enumerate a list of data types that are included within "physical or mental health status." Although the list is non-exclusive (being preceded by "includes, but is not limited to"), it is critical to helping to understand just how broad this definition is, and so it is worth quoting it in its entirety:

> (b) For the purposes of this definition, physical or mental health status includes, but is not limited to:

(i) Individual health conditions, treatment, diseases, or diagnosis;
(ii) Social, psychological, behavioral, and medical interventions;
(iii) Health-related surgeries or procedures;
(iv) Use or purchase of prescribed medication;
(v) Bodily functions, vital signs, symptoms, or measurements of the information described in this subsection (8)(b);
(vi) Diagnoses or diagnostic testing, treatment, or medication;
(vii) *Gender-affirming care information*;
(viii) *Reproductive or sexual health information*;
(ix) *Biometric data*;
(x) *Genetic data*;
(xi) *Precise location information* that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies;
(xii) Data that identifies a consumer seeking *health care services*; or
(xiii) Any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the data described in (b)(i) through (xii) of this subsection that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).

Italics and underlining is added in the above to indicate other defined terms within this definition.

Some of the individual items listed in the above-quoted portion of the definition are subject to extremely broad interpretations. "Social … interventions" in undefined but could cover a wide range of everyday social interactions among people. "Bodily functions" certainly includes functions such as digestion, and so could be read expansively to include information about eating a meal at a restaurant.

But perhaps the broadest item is "data that identifies a consumer seeking health care services." "Health care services" is a defined term and means:

> "any service provided to a person to assess, measure, improve, or learn about a person's mental or physical health."

A search engine is a service that a person could use to "learn about" their health. Similarly, any online or offline research about topics relating to health, wellness, nutrition, or fitness could fall into such a sweeping definition. A gym membership is almost certainly a "service provided to a person to … improve [their] … physical health" Likewise, a store selling running shoes could be seen as offering a service that allows a "person to … improve [their] … physical health."

In light of these expansive elements of the relevant definitions, it's clear that the plaintiffs' bar will have the ammunition to at least put forth arguments that nearly any purchase, nearly any use of media, nearly any activity could identify a consumer's "health status" and therefore information about any of that could be "consumer health data."

This conclusion is reinforced by the fact that proponents of the Act repeatedly cited the decade-old incident in which Target inferred a likelihood of pregnancy based on the purchase of items that are not directly related to pregnancy (unscented lotions, cotton balls, vitamins, large handbags, etc.). This focus on inferences is reflected in part (xiii) of the above-quoted definition, which, while confusingly drafted, could be argued that it opens up the definition to even more types of data.

Of course, there are a range of counterarguments that this and other aspects of the definition should be read more narrowly and reasonably. But the private right of action creates the incentives for plaintiffs' attorneys to make the case for expansive readings.

The stunning breath of certain parts of the "consumer health data" definition, the references to inferences and derived data, and the open-ended nature of the enumerated data types ("includes, but is not limited to"), combined with the creativity (and financial incentives) of trial lawyers, means ***that it will be difficult to safely conclude that any category of personal data is out of scope of the Act***.

As a result, it is inaccurate to refer to the Washington My Health My Data Act as a "health data privacy law." On the contrary, it is, in effect, a generally-applicable privacy law.

A Final (Personal) Note on The Definition of Consumer Health Data

It is important to acknowledge that two particular categories of health care are specifically called out in the definition of "consumer health data" – "reproductive and sexual health" and "gender-affirming care." It's no secret that these are two classes of health care that are under political and legal threat in the United States, in large part flowing from last year's Supreme Court decision in *Dobbs v. Jackson Women's Health Organization* overturning the constitutional right to abortion. Other protections related to reproduction, sexuality, and gender have been called into question based in the reasoning in *Dobbs* and have been undermined or threatened in many U.S. states. This context was clearly and explicitly called out by supporters of this Act as a motivation behind it and was a key factor in propelling it forward.

Let me say unequivocally and without hesitation, ***I strongly support the right of all people to access these services and the importance of protecting the privacy of those seeking such care****. These involve some of the most private decisions that can be made and go to the very core of human dignity and autonomy. To the extent that my analyses of this legislation may be viewed as a critique, that should not be taken in any way as a lack of support for such legislative intent or objectives.* On the contrary, my analyses are focused solely on the challenges faced by those entities seeking to comply with its requirements. Those challenges would have been significantly lessened, and much of the business opposition to the legislation surely would have diminished, had the bill been more clearly and squarely focused on the sensitive information related to those types of services. But as described in this post and elsewhere, it is much, much broader than that.

As noted above, in the coming days we will discuss other aspects of the Act and the issues it raises. In the next post, we will look at another element that determines the broad scope and impact the Act: the scope of entities and consumers that it captures.

Part 3: The Scope of Entities and Consumers Captured by the Act

By Mike Hintze • April 17, 2023

This is the third in a series of blog posts about the Washington My Health My Data Act. This part delves into other elements of the Act that determine its broad scope and impact: the range of entities and consumers that it captures.

The Washington My Health My Data Act applies to "regulated entities" that collect or process "consumer health information" from "consumers." Part two of this series addressed the definition of "consumer health data" and how that definition results in a scope of applicability that is far beyond what we might typically think of as sensitive health data. But the other two above-quoted defined terms – "regulated entity" and "consumer" also result in a very broad (and in some ways surprising) scope and impact.

What "Regulated Entities" are Covered by the Act?

The Act applies to "regulated entities" as defined in the Act. It is a sufficiently broad definition that ***most non-governmental entities may find themselves subject to the Act***. The definition is as follows

> "Regulated entity" means any legal entity that:
>
> (a) Conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington; and
>
> (b) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data.

The definition goes on to specify that a regulated entity does not include "government agencies, tribal nations, or contracted service providers when processing consumer health data on behalf of the government agency."

Small Businesses

The Act also defines the term "small business" as another type of entity subject to the Act. However, the term "small business" is a subset of the term "regulated entity" and all obligations under the Act apply equally to small businesses and other regulated entities. The only difference in the Act is that ***for some provisions, there is a different effective date for small businesses***. So, while the statute unnecessarily and redundantly refers to "regulated entities and small businesses" throughout, I will refer only to regulated entities in this discussion, which should be read as including small businesses.

Some Nexus to Washington State

The first prong of the regulated entity definition requires some nexus to Washington. But it is likely that this requirement will be interpreted broadly. Certainly, having a physical retail storefront in Washington will be enough. Shipping goods to Washington, engaging in a financial transaction with a consumer in Washington, having sales personnel or other employees located in Washington, and other activities with a nexus to Washington will also likely subject the entity to the Act. For online services, it ***may be debatable whether merely allowing users to access a website or online service that does not otherwise have any Washington-specific content or features will be enough***. But that is an open question that will certainly be tested in the courts.

It is also noteworthy that the first prong of the definition applies to any entity that "produces" products or services targeted to Washington consumers – so it ***could apply to developers, OEMs, manufacturers, etc. if they process consumer health data*** – even if they are not the entities *offering* or *providing* the services directly to Washington consumers.

A Possibility of Geo-Blocking Washington Consumers?

It will be interesting to see if certain online services choose to begin geo-blocking online visitors from Washington or taking other steps to ***exclude Washington residents*** as a strategy to minimize the likelihood of being subject class action claims under the Act – in much the same way some companies have blocked Illinois users from certain services (or at least the biometric features of their services) to avoid the litigation risk under Illinois' Biometric Information Privacy Act (BIPA) because of that law's private right of action.

Controllers and Processors

Although the Act does not use the term "data controllers," the second prong of the regulated entity definition uses GDPR-like data controller language to limit the definition to an entity that "alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data."

This "data controller" part of the definition is important. ***All the obligations of the Act apply to regulated entities (controllers)***. But compared to most other modern privacy laws, the Act imposes ***relatively few obligations directly on processors*** (a term that *is* used in this Act).

A "processor" is defined as "a person that processes consumer health data on behalf of a regulated entity or a small business." Processors are required to assist regulated entities in meeting their obligations. And processors' use of consumer health data must be limited by the regulated entity's instructions as set out in a contract. But the Act leaves quite a bit of wiggle room about how broad or narrow those instructions may be.

Large processors that use standard, non-negotiable contracts will likely impose "instructions" on their controller customers that give themselves sufficiently broad data use permissions. As a result, such processors may face significantly less impact (and risk) under this Act than those that act as

"regulated entities." However, ***processors should still pay close attention to the risks created by the Act***.

Section 8 of the Act provides that if a processor exceeds the regulated entity's instructions "or processes consumer health data in a manner that is outside the scope of the processor's contract with the regulated entity," the processor will become a regulated entity subject to all the obligations of the Act with respect to that data. Relatedly, because the Act borrows GDPR-like controller / processor language, it is possible that courts will look to GDPR interpretations as guidance. And, increasingly, there is a recognition in Europe that there is no such thing as an entity that operates purely as a data processor because even where a processor is mainly processing data on behalf of another entity, the processor inevitably uses such data for its own purposes, including meeting its own legal obligations – thereby making it a controller with respect to such activities. If such an interpretation is adopted under this Act, even those entities that mainly meet the "processor" definition and have broad contractual "instructions" may find themselves considered a regulated entity for at least some uses of consumer health data.

Entities Covered By Certain Other Privacy Laws

There are a number of exclusions in Section 12 of the Act, primarily for data covered by other enumerated privacy laws, including HIPAA, GLBA, and FERPA (and certain existing Washington state laws related to health care and insurance). And, as explained in part two of this series, while these are data-level exclusions rather than entity-level exclusions, certain types of entities regulated by these sector-specific laws (health care providers, financial services, and schools, for example) will find some or all of their data processing outside the scope of the Act.

What "Consumers" are Covered by the Act?

The second post in this series described the broad range of data types included, or potentially included, within the scope of "consumer health data". Inherent in that term and its definition is that it is limited to personal information data about a "consumer."

Consumer is defined by Act, as follows:

> "Consumer" means (a) a natural person who is a Washington resident; or (b) a natural person whose consumer health data is collected in Washington. "Consumer" means a natural person who acts only in an individual or household context, however identified, including by any unique identifier. "Consumer" does not include an individual acting in an employment context.

Employee Data and B2B Data Excluded

The last two sentences of this definition seem to ***exclude employees and B2B data***. So, unlike the scope of "consumers" covered by the California Consumer Privacy Act, in this Act "consumer" actually means consumers as that term is typically understood, and not employees or business contacts.

Mere Processing in Washington is Enough

But unfortunately, not all terms in this definition are what they seem. In particular, the first sentence, which sets geographic boundaries on the scope of consumers covered, seems straightforward and unsurprising; but ***the scope of individuals this definition captures is much broader than it appears on its face***.

The second prong of that first sentence captures any person "whose consumer health data is collected in Washington" (emphasis added). The non-obvious scope of the "consumer" definition is due to the Act confusingly ***defining "collect" as including any data "processing."***

> "Collect" means to buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any manner.

Thus, ***personal data of individuals with no connection to Washington could be captured by this law if that data in some way is processed in Washington***. In other words, it is possible that if a resident of Florida makes a purchase at a store in New York owned by a company based in Texas, the information related to that purchase would be subject to the Act if that data is processed in a cloud server located in Washington.

Data Localization Implications?

It is noteworthy that some of the largest global cloud service providers are headquartered in Washington, with significant data center footprints in Washington. Does this mean that customers of cloud service providers need to start worrying about data location and transfers of data across state lines *within* the United States, with an aim of limiting the scope of potential liability by avoiding data processing in Washington? Such ***data localization measures may be advisable as a way to limit potential legal exposure under this Act***. Will cloud service providers respond by offering an option to process data in data centers outside Washington state? Such actions results are certainly foreseeable and may be one of the stranger outcomes of this Act.

Likewise, will companies avoid hiring vendors, contractors, or remote employees in Washington state in order to avoid personal data processing in Washington that might not otherwise occur? That would be unfortunate, but again, is a foreseeable outcome of the risks and costs created by this Act.

As noted above, in the coming days we will discuss other aspects of the Act and the issues it raises. In upcoming posts, we will look at consumer consent and authorization requirements, data subject rights, notice obligations, geofencing restrictions, and other topics raised by the Act.

Part 4: Effective Dates

By Mike Hintze • April 18, 2023

This is Part 4 in a series of blog posts about the Washington My Health My Data Act. This part discusses the effective dates of the Act. ***Spoiler alert****: due to what one can only conclude is, at least in part, a drafting error, some of the substantive provisions of the Act may come into effect much sooner than expected.*

Yesterday the amended Senate version of the Washington My Health My Data Act was approved by the Washington State House, completing the legislative process and sending the Act to the Governor for signature (which is widely expected to happen). Now that it is a near certainty the Act will become law in its current form, entities subject to the Act need to start preparing to comply. The key factor in determining deadlines for having compliance measures in place is the effective date of the Act.

In a rational universe, this would be a straightforward question, the answer to which would be simply stated in the legislation and easily determined by the reader. But that is, unfortunately, not the case here. In fact, although the Act ***purports to come into effect on March 31, 2024*** (and for small businesses, three months later on June 30, 2024) ***many provisions could come into effect in July 2023***.

In Washington, if legislation does not specify an effective date, the requirements of that legislation come into effect 90 days after the end of the session. The current legislative session is scheduled to end in just a few days – on 23 April 2023. As a result, if the session ends on time, in the absence of a specified effective date, the requirements of the Act would come into effect on July 22, 2023.

The original House bill did not specify effective dates. The Senate striker amendment stated an intent to add "an effective date of March 31, 2024, for regulated entities and an effective date of June 30, 2024, for small businesses." That quoted language is taken directly from the summary of the effect of the amendment, which is found at the bottom of the amendment document. However, the way those effective dates were added is problematic.

In particular, the effective dates were added on a section-by-section basis, rather than as a separate section that applies to the entire bill. Specifically, effective date language was added to sections 4 through 9.

Notably, effective date language was not added to Section 10 – the geofencing prohibition. That means that ***the geofencing prohibition takes effect 90 days after the session***, contrary to the stated intent of the amendment. It appears that this result, however, may have been deliberate.

Further, even in those sections where effective dates were added, the way dates were added in most sections makes the March 31, 2024 date seemingly apply to only the first paragraph of each section. For example, Section 5(1) is illustrative of how the effective dates were added:

(a) Except as provided in subsection (2) of this section, beginning March 31, 2024, a regulated entity or a small business may not collect any consumer health data except:

(i) With consent from the consumer for such collection for a specified purpose; or

(ii) To the extent necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity or small business.

(b) A regulated entity or a small business may not share any consumer health data except:

(i) With consent from the consumer for such sharing that is separate and distinct from the consent obtained to collect consumer health data; or

(ii) To the extent necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity or small business.

(c) Consent required under this section must be obtained prior to the collection or sharing, as applicable, of any consumer health data, and the request for consent must clearly and conspicuously disclose:

(i) The categories of consumer health data collected or shared;

(ii) the purpose of the collection or sharing of the consumer health data, including the specific ways in which it will be used;

(iii) the categories of entities with whom the consumer health data is shared; and

(iv) how the consumer can withdraw consent from future collection or sharing of the consumer's health data.

(d) A regulated entity or a small business may not unlawfully discriminate against a consumer for exercising any rights included in this chapter.

Because the effective date language is part of subsection (a) and forms part of the sentence that sets out the substantive requirement of (a), if read literally, that effective date applies only to subsection (a) and does not apply to subsections (b), (c), or (d). That means that ***the requirement of Section 5(1)(a) to obtain consent for "collection" comes into effect March 31, 2024; but the requirement of Section 5(1)(b) to obtain consent for "sharing" may come into effect late July 2023***. Again, this is contrary to the stated intent of the amendment that added the effective dates, but it is what a literal reading of the section seems to require.

It is worth noting that after setting out parts (a)-(d) of subsection 5(1), subsection 5(2) then states: "A small business must comply with this section beginning June 30, 2024." By placing the effective date

for small businesses at the end, it is clear that this effective date does apply to the entire section. Thus, the discrepancy noted above affect only regulated entities that do not meet the definition of a "small business."

Section 6, which creates consumer rights, also has the same discrepancy. As drafted, the right to access consumer health data does not come into effect until March 31, 2024. But it appears that the extremely onerous right to delete that data could be read as coming into effect much sooner – in late July 2023.

And there is a comparable problem in Section 4 (notice requirements) that creates an even more nonsensical result. The effective date language is similarly part of subsection 4(1)(a) – the section that requires regulated entities to have a "consumer health data privacy policy." Thus, the requirement to have such a document does not come into effect until March 31, 2024. But subsection 4(1)(b), which requires regulated entities to post a link to the consumer health data privacy policy on the entity's homepage, does not have an effective date and therefore seemingly comes into effect in late July 2023. Thus, between July 2023 and March 31, 2024, the Act appears to require regulated entities to post a homepage link to a document that need not yet exist. That creates an absurd result that seems to clearly indicate a drafting oversight.

Perhaps in an effort to be compliant, companies will add a homepage link which will take users to a page that says "coming soon." Or, perhaps courts will interpret subsection (b) to require that the link go to the actual policy, thereby nullifying the effective date set out in subsection (a) and requiring that all of Section 4 come into effect in July 2023. Or, perhaps courts will recognize this as a drafting error and defer to the stated legislative intent, concluding that all of Section 4 comes into effect in March 2024. Of course, this uncertainty puts regulated entities in a very difficult situation of guessing how these discrepancies will be interpreted and gauging risks associated with the different possibilities.

There are similar drafting issues in Sections 8 and 9. Only Section 7 has added the effective date in a way that makes it clear that it applies to each subsection.

The following chart sets out the key substantive requirements of the Act and the effective dates that seem to apply to them.

Substantive Requirement	**Effective Date for Most Regulated Entities**	**Effective Date for Small Businesses**
§4(1)(a) Obligation to maintain a "consumer health data privacy policy"	March 31, 2024	June 30, 2024
§4(1)(b) Obligations to publish a homepage link to the consumer health data privacy policy	Late July 2023	June 30, 2024

§4(1)(c) Consent for collection, use, or sharing *categories* of data not disclosed in consumer health data privacy policy	Late July 2023	June 30, 2024
§4(1)(d) Consent for collection, use, or sharing for *purposes* not disclosed in consumer health data privacy policy	Late July 2023	June 30, 2024
§4(1)(e) Prohibition on contracting with a processor to process in manner inconsistent with consumer health data privacy policy	Late July 2023	June 30, 2024
§5(1)(a) Consent for *collection* of consumer health data for a secondary purpose	March 31, 2024	June 30, 2024
§5(1)(b) Consent for *sharing* consumer health data for a secondary purpose	Late July 2023	June 30, 2024
§5(1)(d) Prohibition on unlawful discrimination	Late July 2023	June 30, 2024
§6(1)(a) Right to know / right of access	March 31, 2024	June 30, 2024
§6(1)(b) Right to withdraw consent	Late July 2023	June 30, 2024
§6(1)(c) Right of deletion	Late July 2023	June 30, 2024
§6(1)(d)-(h) Procedural requirements related to consumer requests to exercise rights	Late July 2023	June 30, 2024
§7 Data Security	March 31, 2024	June 30, 2024
§8(1)(a)(i) Requirement for processor contract	March 31, 2024	June 30, 2024
§8(1)(a)(ii) Processor limit to processing consistent with contractual instructions	Late July 2023	June 30, 2024
§8(1)(b) Processor obligation to assist regulated entity in meeting its obligations	Late July 2023	June 30, 2024
§9 Consumer Authorization for Data "Sale"	March 31, 2024	June 30, 2024
§10 Geofencing Prohibition	Late July 2023	Late July 2023

It would have been far cleaner and clearer if there were a separate section that simply stated that the effective dates of March 31, 2024 (for regulated entities) and June 30, 2024 (for small businesses) apply to each of the substantive sections of the Act (i.e., sections 4-10). Further, even if there had been an unstated legislative intent to have some sections come into effect sooner than others, the effective dates could have been added on a section-by-section basis in a much more straightforward way. For example, the last subsection of each section could have simply stated: "A regulated entity must comply with this section beginning March 31, 2024, except that small business must comply with this section beginning June 30, 2024."

Unfortunately, the drafters instead added the dates in a way that seemingly creates a patchwork of effective dates that is contrary to the stated legislative intent and in some cases creates absurd results.

Further, because of Washington's limited legislative schedule, there is no longer time in this session introduce a new "clean up" bill to correct these (and other) drafting problems, leaving few avenues for a fix. And the next legislative session will not begin until January 2024 – too late to fix these issues with the effective dates.

This unfortunate approach to drafting leaves companies seeking to comply with the Act scrambling to comply with several highly onerous and costly obligations on a very short timeframe. The only alternative is to hope that they can fend off aggressive plaintiffs' lawyers seeking to exploit this drafting issue and that the courts will ultimately conclude that the stated legislative intent should prevail. But that could prove to be a risky and costly gamble.

Update: Subsequent to the post, the Act was signed by the Governor with the effective date problems discussed here remaining. However, on June 30, the Office of the Attorney General (OAG) published important (albeit non-binding) guidance addressing the effective date issue. As expected, the OAG takes the position that only the geofencing prohibition takes effect in late July 2023, whereas all the other substantive requirements take effect on March 31, 2024 (except for small businesses which must comply beginning June 30, 2024). Part 9 of this blog series discusses this guidance and its likely impact.

In the coming days we will discuss other aspects of the Act and the issues it raises. In upcoming posts, we will look at consumer consent and authorization requirements, data subject rights, notice obligations, geofencing restrictions, and other topics raised by the Act.

Part 5: Consent Requirements

By Mike Hintze • April 19, 2023

This is Part 5 in a series of blog posts about the Washington My Health My Data Act. This part discusses the opt-in consent requirements for the collection, use, and disclosure of consumer health data under the Act.

When it comes into effect, the Washington My Health My Data Act will impose ***strict consent requirements on a wide range of common data collection and processing activities***. In essence, the Act requires affirmative (opt-in) consent for any collection, use, disclosure, or other processing of consumer health data beyond what is necessary to provide a consumer-requested product or service.

The consent requirements of the Act are primarily set out in Section 5, but there are consent requirements also in Section 4 (Notice) and Section 9 (Authorization for Data "Sales").

GDPR-Level (or Higher) Consent

The definition of "consent" establishes a requirement for ***GDPR-level consent***:

> "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.

That definition goes on to further require that for consent to be valid, it cannot be obtained by a consumer (i) accepting a general terms of use or similar agreement, (ii) hovering over, muting, pausing, or closing a piece of content, or (iii) agreeing where such agreement was obtained though deceptive design. This language mirrors that found in other state privacy laws, with a welcome difference being the use of the term "deceptive design" rather than the more ambiguous and problematic "dark patterns."

As discussed below, ***an even higher level of consent (or "authorization") is required for any disclosure of data that would be considered a "sale"*** of consumer health data under the Act.

It is worth noting that the consent requirements of the Act are opt-in requirements, unlike the opt-out requirements found in many privacy laws (such as the CCPA). And unlike other privacy laws that do have opt-in consent requirements for certain data uses, this Act has opt-in requirements that apply to any uses beyond what is necessary to provide a consumer-requested product or services (discussed in detail below). Further, unlike other privacy laws that have consent requirements, this Act does not have exceptions or alternatives to consent for common, expected, or benign data uses. There *is* a limited security-related exception discussed below, but that does not cover a number of common, and in some cases essential, data uses. As a result, ***it is likely that consumers will be faced with a growing number of disruptive consent requests for common and expected data uses***.

Note also that the Act also gives consumers the ***right to withdraw consent***. Thus, any processing that relies on consumer consent could be halted by the consumer at any time.

Consent for "Collection"

Section 5 requires an entity to get consent to "collect" consumer health data unless the collection is "necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from" that entity.

This requirement is ***much broader than it appears on its face because of the odd and unexpected way "collect" is defined***. As noted in Part 3 of this series, "collect" is much broader than its plain English meaning. In this Act, "collect" means: "to buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any manner" (emphasis added). So, "collect" includes any "processing."

In turn, "process" means: "any operation or set of operations performed on consumer health data." So, performing analytics on data is "collecting" that data. Sharing data is "collecting" that data. Deidentifying data is "collecting" that data. Disposing of data is "collecting" that data.

Editorial Note: As an aside, it is beyond frustrating when legislative drafters choose to use and define words in ways that are divorced from their usual meaning. It makes legislation needlessly opaque and puts those making good faith efforts to comply at increased risk of inadvertent mistakes. English is a rich language with plenty of perfectly precise and descriptive words avaialble to choose from that will foster transparency and understanding rather than the opposite. Please, legislative drafters, use them.

Given these definitions, this consent requirements should be thought of as ***consent for any "processing" of consumer health data beyond what is necessary to provide a consumer-requested product or service***. Although the Act doesn't use the term "secondary purpose," this may be a useful shorthand for that processing which requires consent.

The unusual way "collect" is defined, combined with these strict opt-in consent requirements, can also lead to some harmful or absurd results. For example, because "collect" includes any "processing," and "processing" includes any "operation" performed on consumer health data, as noted above, the act of deleting or disposing of data is an "operation" on that data and therefore a "collection." So, unless deleting data is necessary to provide a consumer-requested service, it cannot be done without consumer consent. A specific request to delete data would constitute consent. But ***absent a specific consumer request to delete, this Act would seem to require regulated entities to retain consumer health data forever***, even if they no longer have any use for it. A regulated entity *might* be able to argue that proactive deletion of data falls within the "security exception" (discussed below), but the burden is on the entity to justify that interpretation, so the safer course might just be to keep the data indefinitely. Of course, this result is contrary to privacy-protective principles such as data minimization and retention limitation. But it's what a strict reading of the Act seems to require.

Finally, how narrowly or broadly the term "necessary" is interpreted will have an enormous impact on the scope of processing that may be permitted without affirmative, opt-in consent (i.e., what is considered a secondary purpose). The Act does not say "strictly necessary," so there may be some leeway for reasonableness here. But that will surely be tested through litigation, and many regulated entities may not want to take that risk. At the very least, regulated entities will need to carefully consider their justification for any processing for which they do not obtain affirmative opt-in consent.

Separate Consent for Sharing

Section 5 of the Act goes on to require a separate consent for any "sharing" of consumer health data beyond what beyond what is necessary to provide a consumer-requested product or service.

Although, given the odd definition of "collect" described above, sharing is actually a subset of collection. Nevertheless, the Act specifies that consent for "sharing" must be "separate and distinct from the consent obtained to collect consumer health data." So, ***if a regulated entity is sharing data for a secondary purpose, there may be a need for two separate consent experiences*** – one for collection / processing and one for sharing.

To understand the scope and applicability of this separate consent for sharing, it is important to note the definition of "share." Under the Act, "share" means to:

> release, disclose, disseminate, divulge, make available, provide access to, license, or otherwise communicate orally, in writing, or by electronic or other means, consumer health data by a regulated entity or a small business to a third party or affiliate.

There are several elements of this definition that make the scope of "sharing" very broad. For example, it includes "make available." So, for example, ***allowing third-party cookies or pixels on a website could constitute sharing, requiring opt-in consent***. Note also that if such access could constitute a data "sale," an even higher level of consent may be required, as discussed below.

The definition of "share" also includes disclosures to affiliates. So, within a large corporation that includes a number of distinct legal entities, ***access to common data systems or other routine data operations that involve sharing data among different subsidiaries could potentially require the opt-in consent of the consumer***.

The definition of "share" does include some notable exceptions, such that disclosures to "processors" acting on behalf of the regulated entity is not sharing, nor are certain disclosures in the context of a merger, acquisition, bankruptcy, or similar corporate transaction. There is also a narrow exception for disclosures to third parties with which the consumer has a direct relationship where the disclosure is for the purpose of providing a consumer-requested product or service; but the narrowness of this exception along with certain other requirements make it unlikely to particularly useful.

There is also a general exception in the Act for security and related purposes, noted below, that may allow for certain data disclosures without consumer consent.

Consent for Collection or Processing Beyond What is Described in the Notice

Section 4 of the Act sets out requirements for a notice, referred to as the "Consumer Health Data Privacy Policy." Among the requirements of that section are that a regulated entity must get consumer consent for any:

- collection, use, or sharing additional categories of data not disclosed in the notice, and
- collection, use, or sharing of data for additional purposes not disclosed in the notice.

Given that these consent requirements are tied to what is disclosed in the notice, regulated entities can mitigate the risk by making sure that their notices are sufficiently broad up front. And given the breadth of the consent requirements in section 5, it is unlikely in practice that these Section 4 consent requirements would trigger consent obligations beyond what would be required in any event.

Heightened Consent for "Sale" of Consumer Health Data

Finally, Section 9 of the Act requires an ***extreme level of opt-in consent for any "sale" of consumer health data***. As with the consent to "share," the consent to "sell" must also be separate from any other consents. Also, this consent requirement applies to any "person" and not just to "regulated entities," which means it could potentially apply to an even broader range of companies, organizations, and even individuals.

"Sell" is defined under the Act in a way similar to CCPA definition of that term. The Act defines "sell" as "the exchange of consumer health data for monetary or other valuable consideration." Note that under CCPA, the "other valuable consideration" phrase ***has been interpreted broadly so as to cover many activities not traditionally thought of as a sale of data*** – including nearly all third-party online targeted advertising. There is no reason to think that it will be interpreted any more narrowly here.

Any activity that could constitute a "sale" of consumer health data requires an "authorization" by the consumer. An authorization is a lengthy document that contains a long list of enumerated information and statements that must be signed and dated by the consumer. And such authorizations expire after one year. The written authorization must contain:

- The specific consumer health data to be sold
- The name and contact information of the seller
- The name and contact information of the buyer
- The purpose of sale
- How the data will be gathered

- How the data will be used by the buyer
- Statements that:
    - The provision of goods or services may not be conditioned on data sale authorization
    - The consumer has right to revoke the authorization at any time
    - The data sold may be subject to redisclosure and may no longer be protected by the Act
- How the consumer may submit a revocation
- The date of signing
- An expiration data that is 1 year from the date of signing.
- The signature of consumer

A copy of the signed authorization must be provided to the consumer and both the seller and the buyer of the data must retain a copy of the authorization for 6 years.

Obviously, ***such a consent requirement is incredibly onerous – to such an extent that it is unlikely business would regularly seek such authorizations***.

There is also a conflict within the Act that makes it even less likely any business would or should seek an authorization to sell consumer health data. Specifically, note that the authorization document must contain "*the specific consumer health data concerning the consumer that the person intends to sell.*" Thus, the authorization document will contain consumer health data. Further, the Act requires both the seller and purchaser of consumer health data to retain a copy of the authorization for 6 years.

However, Section 6 of the Act includes a consumer right to delete consumer health data which, as discussed in Part 1 of this series, does not have the common exceptions that deletion rights have in other privacy laws. In particular, there is no exception for where retention of the data is required by law. So, if a consumer, after signing the authorization, makes a deletion request, the business would be required to delete all consumer health data, which would include the authorization since it necessarily includes the relevant consumer health data. So, does the company violate section 6 by refusing to delete the authorization, or does it violate section 9 by failing to retain the authorization? ***It is impossible to comply with both***.

For a plaintiffs' lawyer, this would be an easy trap to spring – simply find a company that seeks authorization to sell consumer health data, provide such an authorization, then a few days later, make a deletion request … then just wait to see which provision of the Act the company violates.

For these reasons – both the burden of seeking such an onerous authorization and the litigation trap it creates – ***this authorization requirement is, in effect, a prohibition on data sales***.

Further, given the breadth of what constitutes a "sale" (and taking into account the influence of CCPA precedent interpreting the similarly-defined term) ***this may, in effect, be a prohibition on***

targeted advertising using any data that could arguably constitute "consumer health data" – which as described in Part 2 of this series, is potentially a very, very broad range of data.

General Exception for Security-Related Purposes

The Act includes a relatively broad exception for any processing for certain security-related activities. Specifically, Section 12(3) provides that nothing in the Act restricts a regulated entity's ability to:

> collection, use, or disclosure of consumer health data to prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any activity that is illegal under Washington state law or federal law; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action that is illegal under Washington state law or federal law.

This exemption presumably means that ***even if some data processing activity would otherwise require consent under the Act, a regulated entity can collect, use, or disclose that data without consent if it falls into one of these security-related purposes***. However, this section goes on to state that if a regulated entity is relying on this exemption, "such entity bears the burden of demonstrating that such processing qualifies for the exemption…"

As a result of this and the other provisions addressing consent under the Act, ***regulated entities should carefully evaluate their justifications for any processing not relying on consumer consent***.

As noted above, future posts will discuss other aspects of the Act and the issues it raises, including data subject rights and notice obligations.

Part 6: Data Subject Rights

By Mike Hintze • April 24, 2023

This is Part 6 in a series of blog posts about the Washington My Health My Data Act. This part discusses the rights consumers have under this Act including a uniquely broad right of access, a right of deletion with few exceptions, a right to withdraw consent, and a right on non-discrimination.

The Washington My Health My Data Act provides consumers with several rights, including a right of access, a right to delete, a right to withdraw consent, and a right to not be discriminated against for exercising their rights. While each of these rights can be found in other privacy laws and so, at a high level, do not seem particularly surprising here, the ways they are included in this Act are unique, create uncertainty, and in some cases go well beyond what exists in any other privacy law. As a result, ***regulated entities seeking to comply with them will face difficult, costly, and disruptive implementation challenges*** (and with respect to the deletion right, the potential for catch-22 situations where full legal compliance may be impossible). These challenges, along with the Act's private right of action, set up a significant risk of expensive legal claims and litigation.

For each of these consumer rights, regulated entities must keep in mind just how broadly they will apply in light of the broad scope of "consumer health data" as discussed in Part 2 of this series and the broad scope of consumers covered by the Act as discussed in Part 3. Also, as described in Part 4, some of these rights and obligations may come into effect much sooner than intended - as soon as late July of this year.

Right of Access / Right to Know

Like many privacy laws, this Act includes a right of access. Specifically, it gives consumers a right to confirm whether a regulated entity is collecting, sharing, or selling consumer health data about them. And it gives consumers a right to access such consumer health data in possession of the regulated entity.

But this right of access goes further, by also giving consumers ***a right to receive "a list of all third parties and affiliates*** with whom the regulated entity … has shared or sold the consumer health data and an active email address or other online mechanism that the consumer may use to contact these third parties."

Because this additional element of the right, and corresponding obligation, is novel and goes beyond what other privacy laws require under a right of access or right to know, it will require regulated entities to ***develop and put in place new processes and tools to track data transfers in a way that such a list can be generated and provided to consumers who request it***.

It is noteworthy that this requirement to provide a list and contact information includes affiliates as well as third parties. So, where a corporation consists of multiple legal entities that share common data systems, it is likely that the list to be provided to consumers will have to include the names and contact details of all such affiliates – even if those entities are not normally consumer facing (e.g.,

those established solely for purpose of internal operations, taxation, etc.) and do not normally provide a way for consumers to contact them.

Right to Delete

A right to delete is also a common element found in many privacy laws. And this Act gives consumers a right to have the consumer health data held by a regulated entity deleted upon request. But this ***deletion right goes well beyond what is found in any other privacy law, and as a result will create serious challenges and risks for regulated entities***.

First, it is noteworthy that the federal HIPAA privacy rules do not include a right to delete, and this Act carves out data subject to HIPAA. So, health data held by hospitals, clinics, doctors' offices, pharmacies, and other HIPAA covered entities does not need to be deleted when requested by a consumer. By contrast, subject to few exceptions, health data subject to this Act must be deleted upon request.

Further, the deletion right in this Act is unprecedented in two important ways.

First, it lacks the common sense exceptions found in virtually every other privacy law. There is a limited exception in Section 12(3) for data necessary for certain security-related purposes. But ***the Act does not include other common exceptions, including where the data may be required to defend against legal claims, to enforce agreements, or to comply with legal obligations***.

The fact that there is no exception where retention is necessary to defend against claims means that a consumer wishing to make a legal claim against a regulated entity can first use the access right to circumvent normal discovery procedures and gather the relevant data. Then, once the consumer obtains that data, they can use the deletion right to force the regulated entity to delete it and thereby deprive the entity of the information it needs to defend itself.

The lack of an exception for where data retention is required to meet legal obligations will ***put regulated entities in catch-22 situations in which meeting all its legal obligations is impossible.*** A deletion request may require regulated entities to choose whether they violate a legal retention obligation or violate this Act's deletion requirement. Consumer health data may appear in records that must be retained for tax purposes, accounting and auditing purposes, or other required recordkeeping purposes. As noted in Part 5 of this series, even this Act itself has a data retention obligation that can come into conflict with its own deletion right / obligation.

The second way in which the deletion right goes well beyond other privacy laws and will create major challenges for regulated entities is that it includes a "passthrough" obligation whereby ***when a consumer makes a deletion request, the regulated entity must notify "all affiliates, processors, contractors, and other third parties with whom the regulated entity … has shared consumer health data."*** And the recipient of such notification must delete such data.

This passthrough obligation will obviously require regulated entities to put in place new procedures and mechanisms to be able to send such notifications of a deletion request. And entities that receive consumer health data will likewise ***need to develop and implement new policies, procedures and tools*** that will allow them to receive and validate such notifications; to track the sources of data to be able to identify which data is subject to the deletion request; and to be able to purge such data from their systems.

Beyond the operational challenges, this passthrough deletion requirement ***may result in deletion of data that the consumer neither intended nor desired, and/or that is contrary to the interests of the consumer***. Imagine that a consumer affirmatively asks Company A (a regulated entity) to transfer consumer health data to another service, operated by Company B (an independent third party) with which the consumer has a direct relationship. The consumer may later decide that it no longer wants Company A to retain the consumer health data, but it does want to continue to use Company B's service which depends on having the consumer health data. When the consumer sends a deletion request to Company A, Company A has no option but to send a notification to Company B, and Company B has no option but to delete the data. Depending on the circumstances, this result could range from annoying to even dangerous and harmful for the consumer.

Finally, the deletion requirement under the Act ***also applies to data archives and backups***. However, there is a longer deadline of 6 months to complete such a request.

Right to Withdraw Consent

The Act gives consumers the right to withdraw consent for the "collection and sharing" of consumer health data. But this right is broader than it appears on its face because, as described in Part 5 of this series, the term "collect" is defined to include any "processing." Thus, the right to withdraw consent also applies to any use or other processing of consumer health data for which consent was provided.

As also discussed in Part 5 of this series, the Act requires consent for any collection, sharing, or other processing of consumer health data beyond what is necessary to provide a consumer-requested product or service. As a result, many routine and benign data processing purposes may be based on consumer consent. Given the wide range of data processing that is potentially subject to consent, ***regulated entities will have to develop and put in place new mechanisms to receive and respond to such requests with respect to types of data processing that are not subject to such a right under other privacy laws***. Thus, complaince with this obligation is likely to be costly and enormously disruptive to the operations of a regulated entity.

The right to withdraw consent also raises a number of questions that are unanswered in the text of the statute. Typically, a right to withdraw consent of forward looking, and does not apply to processing that occurred prior to the withdrawal. So, for example, if consent for sharing is withdrawn, the regulated entity should not share the data any further, but it does not affect previously-shared data. That would seem the be the most sensible interpretation, but the private right of action may incentivize plaintiffs' lawyers to argue otherwise.

Further, if consent for collection is withdrawn, does that require the regulated entity to delete the data – or just stop using it for non-exempted purposes? Certainly, if the data is still needed to provide a consumer-requested product or service, a withdrawal of consent for other processing would not require deletion. But if it is no longer necessary, must a regulated entity delete the data? If so, it would seem to render the deletion right redundant and superfluous since these two rights would have precisely the same effect. And courts often will gravitate towards interpretations that avoid determining that a provision of a law is superfluous.

So, there is significant uncertainty about the impact of this right. The full consequence of a right to withdraw consent is likely to be a question addressed in future litigation.

Right of Non-Discrimination

The Act also provides for a right of non-discrimination by specifying that regulated entities "***may not unlawfully discriminate against a consumer for exercising any rights***" under the Act. Curiously, this provision is in Section 5, which otherwise deals with consent requirements, rather than in Section 6 which sets out the consumer rights and how consumers can exercise them.

Unlike the CCPA non-discrimination right, however, this provision does not specify any details about what kind of discriminatory practices are prohibited. For example, under the CCPA, a business cannot deny goods or services, charge a different price, offer different discounts, or provide a different level of service in response to a consumer exercising rights such as opt-out or data deletion rights. Those examples caused a great deal of debate about whether the CCPA non-discrimination provisions would prohibit loyalty programs, club cards, etc. which necessarily involve different pricing or discounts. CCPA was amended to clarify that such programs, including financial incentive programs, are permitted subject to certain requirements. With this Act, there is no such specification of the kinds of differential treatment that may be prohibited.

Importantly, this provision prohibits regulated entities from "unlawfully" discriminating. Arguably, the inclusion of that word makes this provision superfluous given that "unlawful discrimination" is already, well … unlawful.

However, there is a risk that courts may be inclined to avoid interpretations that give a provision of an Act no effect, and therefore may seek to give this provision some impact beyond prohibiting discriminatory contact that is already unlawful. Will courts look to CCPA or other laws as a guide for the scope of this Act's non-discrimination provision? Will they come up with something new? Or will they conclude that the inclusion of "unlawfully" really does mean that this provision has no substantive effect?

Procedural Requirements For Consumer Rights

Finally, the Act also sets out several procedural requirements that regulated entities must follow in receiving and responding to consumer requests to exercise their rights. Most are borrowed from other privacy laws and are not particularly noteworthy. These provisions address the need for a secure and

reliable means for consumers to submit requests, the need to authenticate the consumer making the request, a prohibition on charging a fee for up to two requests annually, a 45-day deadline to comply with requests (which may be extended for up to another 45 days if reasonably necessary), and an appeal process for consumers whose request was denied. Regulated entities will need to ensure that their processes for receiving and responding to consumer requests to exercise their rights complies with each of these requirements.

As noted above, future posts will discuss other aspects of the Act and the issues it raises, including biometric data, notice obligations, and geofencing restrictions.

Part 7: Biometric Data

By Mike Hintze & Jevan Hutson • April 27, 2023

This is Part 7 in a series of blog posts about the Washington My Health My Data Act. This part discusses the Act's impact on biometric data and technologies.

Biometric data is among the broad range of "consumer health data" regulated by the Washington My Health My Data Act (MHMDA). Under MHMDA biometric data is defined expansively, broader than the scope of biometrics covered by the previously-existing Washington biometric privacy law (RCW 19.375). MHMDA's substantive provisions overlap with, but differ from those of RCW 193.75, many of which raise the bar on substantive obligations or add new requirements applicable to biometric data (and a wide range of other data). Finally, MHMDA includes a private right of action, like Illinois' Biometric Information Privacy Act (BIPA) and unlike RCW 19.375, thereby subjecting the processing of biometric data to a significant risk of litigation under Washington law.

Definitions of Biometric Data

As described in Part 2 of this series, MHMDA regulates a broad range of "consumer health data" which is defined as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status." The definition goes on to specify that "physical or mental health status" includes, among many other things, "[b]iometric data."

The Act defines biometric data as:

> data that is generated from the measurement or technological processing of an individual's physiological, biological, or behavioral characteristics and that identifies a consumer, whether individually or in combination with other data. Biometric data includes but is not limited to:
>
> (a) Imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted; or
>
> (b) Keystroke patterns or rhythms and gait patterns or rhythms that contain identifying information.

This is an expansive definition of biometric data, which in several ways is broader than the scope of biometric data covered by the previously-existing RCW 19.375.

RCW 19.375 defines "biometric identifier" as:

> data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual.

That definition goes on to exclude any "physical or digital photograph, video or audio recording or data generated therefrom."

Thus, the first way that the MHMDA definition is broader than that of RCW 19.375 is that the later definition is dependent on the data actually being "used to identify a specific individual." The mere potential to identify a person is not enough. By contrast, the MHMDA definition captures any data about an "an individual's physiological, biological, or behavioral characteristics" that are identifying or would be identifying when combined with any other type of data.

The second way in which the MHMDA definition is broader is that under RCW 19.375, "biometric identifier" does not include "a physical or digital photograph, video or audio recording or data generated therefrom." But, under the MHMDA, biometric data does include "[i]magery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted." So, a mere photograph of a person's face may be enough to be considered "biometric data" under MHMDA.

Additionally, RCW 19.375 is limited to persons who "enroll" biometric identifiers. And "enroll" is defined as the "means to capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual." This, in effect, limits the scope of RCW 19.375 to certain types of practices commonly used in biometric identification systems. There is no such limitation in MHMDA. As a result, MHMDA's broad scope of regulated entities (as further detailed in Part 3), along with its broad definitions of "consumer health data" and "biometric data," mark a considerable expansion of the scope of biometric privacy requirements under Washington law.

Lastly, there is one way in which the MHMDA definition is narrower than that of the previously-existing RCW 19.375. As noted in Part 1 and Part 3 of this series, "consumer health data" is data about "consumers," and the definition of "consumer" does not include individuals acting in an employment context. Thus, unlike under RCW 19.375 (and under Illinois BIPA) ***biometric data collected from employees and B2B contacts should be considered out of scope of MHMDA***.

Overlapping Obligations & New Challenges

Because of the overlapping, but differing, definitions and scope of MHMDA compared to RCW 19.375, some biometric data will be subject to just one of the laws and not the other, but ***a great deal of biometric data will be subject to both Washington laws***. Thus, entities subject to these laws will need to reconcile and develop compliance measures to comply with the overlapping obligations. This challenge is made more difficult by the fact that the ***MHMDA introduces new requirements and raises the bar on substantive obligations applicable to biometric data*** (and a wide range of other data)

Consent

MHMDA and RCW 19.375 both have consent requirements that apply to the collection, use, and disclosure of biometric data. But they are quite different from each other.

As outlined in Part 5 of this series, ***MHMDA requires consent for collection, processing, or sharing consumer health data (including biometric data) for any purpose other than that which is necessary to provide a consumer-requested product or service*** (i.e. only for secondary purposes).

By contrast, the range of biometric data processing that requires consent under RCW 19.375 is different. "Enrolling" a biometric identifier in a database for a commercial purpose requires consent whether or not the enrollment is necessary to provide a consumer requested product or service. In other words, "enrollment" requires consent for both primary and secondary purposes. But for the *sharing* of a biometric identifier under RCW 19.375, like MHMDA, consent is required only for a secondary purpose. Specifically, consent for sharing is not required under RCW 19.375 if the disclosure is "necessary to provide a product or service subscribed to, requested, or expressly authorized by the individual."

Illinois' BIPA is different still, with collection requiring consent in all cases, sharing requiring consent unless necessary to complete a financial transaction, and selling being prohibited.

The level and type of consent required also differs between MHMDA and RCW 19.375. ***MHMDA specifies a GDPR-level of consent***, meaning it must be "freely given, specific, informed, opt-in, voluntary, and unambiguous." MHMDA requires an even higher level of consent (or "authorization") for any disclosure of consumer health data that would be considered a "sale." By contrast under RCW 19.375, the type of consent required seems to be more flexible. That statute notes that "the exact notice and type of consent required...is context dependent."

The high level of consent required under MHMDA may negatively impact many common and beneficial uses of data. As an example, the creation and improvement of biometric technologies heavily depends on using data for training and development. In this context, much or most of the useful data could be classified as biometric data or consumer health data. And the use of artificial intelligence and machine learning technologies in the development or improvement of biometric technology may exceed what is considered necessary to offer a consumer-requested product or service. Such use could therefore be subject to the Act's strict opt-in consent requirements, which would, in turn, severely limit the data sets available. This limitation could create significant obstacles for the development of biometric technologies and other uses of AI/ML.

Data Subject Rights

As discussed in Part 6 of this series, MHMDA creates data subject rights – including ***rights of access and deletion that go well beyond what exists in other laws***. This is in striking contrast to both RCW 19.375 and BIPA, which do not grant rights of access and deletion. Thus, regulated entities processing biometric data will need to be able to comply with such data subject requests with respect to that biometric data.

Such obligations may require companies to develop new means to provide access to and/or delete biometric data upon request. These rights also create obligations, which if companies fail to meet, are likely to lead to class action claims that go beyond the types of claims that have been (or can be) made under BIPA.

Data Retention

Notably, both RCW 19.375 and BIPA include retention limitations applicable to biometric data. Specifically, RCW 19-375 states that a biometric identifier may be retained "no longer than is reasonably necessary to:

1. Comply with a court order, statute, or public records retention schedule specified under federal, state, or local law;
2. Protect against or prevent actual or potential fraud, criminal activity, claims, security threats, or liability; and
3. Provide the services for which the biometric identifier was enrolled.

MHMDA, by contrast, does not have a data retention limitation. In fact, as noted in Part 5 of this series, the consent requirements of MHMDA, which apply to any "processing" of data that is not necessary to provide a consumer-requested product or service, could be interpreted to mean that in the absence of specific consumer consent, a regulated entity cannot delete data because deletion according to a retention schedule is a type of processing that not necessary to provide the product or service. If that interpretation prevails, it would effectively nullify the retention limitation of RCW 19.375 since, as quoted above, that law's retention limitation does not apply where retention is required to "comply with … a statute."

Important Exceptions

There are several important exceptions under MHMDA that limit the applicability of the strict substantive obligations.

First, MHMDA, similar to both RCW 19.375 and BIPA, has an exclusion for data that is subject to HIPAA and the Gramm-Leach-Bliley Act. MHMDA also has additional exclusions for data that is subject to other federal and Washington state regulations related to health and insurance.

Second, as noted above, ***MHMDA excludes employee and B2B data***, unlike either RCW 19.375 or BIPA.

Third, ***both MHMDA and RCW 19.375 have exclusions that apply to security-related uses of biometric data*** (unlike BIPA, which does not). Specifically, RCW 19.375.020(7) provides:

> Nothing in this section requires an entity to provide notice and obtain consent to collect, capture, or enroll a biometric identifier and store it in a biometric system, or otherwise, in furtherance of a security purpose.

MHMDA has a more detailed articulation of security-related purposes that are excluded from the Act's strict substantive requirements that is arguably even broader. Specifically, the exclusion applies to the

> collection, use, or disclosure of consumer health data to prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any activity that is illegal under Washington state law or federal law; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action that is illegal under Washington state law or federal law."

The employee and security-related exemptions mean that ***many uses of biometric data that are most common (and which have been the subject of a large portion of the litigation under BIPA) will be exempt from MHMDA's substantive compliance requirements*** and will likely avoid the risk of litigation under the Act's private right of action. Consider the following scenarios, for example:

- **Scenario 1**: *Use of facial recognition in retail store security cameras for security purposes*. Assuming the retailer does not use the biometric data for any other (non-security related) purposes, this scenario would fall within the MHMDA security exception.
- **Scenario 2**: *Use of a biometric identity verification service to prevent identity theft or fraud in financial transactions*. This scenario would fall within the MHMDA security / fraud exception.
- **Scenario 3**: *Use of biometric access control and timekeeping for employees*. The Act's definition of "consumer" does not include an individual acting in an employment context, so this scenario would fall into the employee data exception. Further, if the biometric access control and timekeeping for employees are for security and fraud-prevention purposes, this scenario would also likely fall within the MHMDA security / fraud exception.

Enforcement

As noted above, ***MHMDA may be enforced through a private right of action***, in addition to enforcement by the Washington Attorney General. By contrast, RCW 19.375 may be enforced solely by the Attorney General. Notably, the Washington Attorney General has not brought a single action enforcing RCW 19.375.

Thus, Washington will join Illinois as the second jurisdiction in the U.S. that allows for a private right of action for violations of privacy rules applicable to biometric data***. If the enormous volumes of costly litigation under Illinois' BIPA is any indication, Washington courts are likely to see a high volume of claims under MHMDA***.

This is likely the case even though the scope of biometric use cases subject to MHMDA is narrower in some respects than those subject to BIPA — due to the employee and security exceptions and the consent requirement applying only to secondary purposes under MHMDA. On the other hand, the scope of biometric data (and the larger superset of consumer health data) under MHMDA is much broader than under BIPA. Further MHMDA adds additional obligations, such those connected to the access and deletion rights, that do not exist under BIPA. So, compared to BIPA, the targets for class action litigation related to biometric data are narrower in some respects and broader in others.

Summary and Conclusion

The key differences in the treatment of biometric data between the new Washington MHMDA, the existing Washington biometric privacy law (RCW 19.375), and Illinois' BIPA are summarized in the following table.

	Washington MHMDA	**Washington RCW 19.375**	**Illinois BIPA**
Definition could include a mere photo	Yes	No	No
Definition includes data not "used" to identify	Yes	No	Yes
Employee and B2B biometric data included	No	Yes	Yes
Consent required for "primary purpose" collection	No	Yes	Yes
GDPR-level consent for secondary purposes	Yes	Not Specified	Not Specified
Consumer access & deletion rights	Yes	No	No
Retention limitation	No	Yes	Yes
Private right of action	Yes	No	Yes

MHMDA, given its broad definition of biometric data, GDPR-level consent requirements, new obligations, and private right of action ***dramatically changes and complicates the regulation of biometric data in Washington*** state and is poised to become the ***most disruptive change in U.S. biometric privacy law since Illinois' BIPA***.

As noted above, in the coming days we will discuss other aspects of the Act and the issues it raises. In upcoming posts, we will look at notice obligations, geofencing restrictions, and other topics raised by the Act.

Part 8: Notice Obligations

By Mike Hintze • May 13, 2023

This is Part 8 in a series of blog posts about the Washington My Health My Data Act. This part discusses the notice obligations under the Act, which seem to require an entirely separate notice rather than changes to an entity's existing privacy statement or privacy policy.

When it comes into effect, the Washington My Health My Data Act (MHMDA or the Act) will impose new privacy notice obligations on regulated entities. The Act requires specific privacy disclosures relating to data that meets the very broad definition of "consumer health data." It appears to require regulated entities to draft, post, link to, and maintain a separate "Consumer Health Data Privacy Policy" that will be largely, but not entirely, redundant of their existing privacy statement(s).

Because the Consumer Health Data Privacy Policy will be publicly available and easily scrutinized by plaintiffs' lawyers and the Washington Attorney General, mistakes implementing this obligation are likely to be a key source of costly and disruptive litigation. Regulated entities will therefore need to take great care in meeting the Act's notice requirements which are, in some respects, unusual and unexpected.

Required Disclosures

The Act requires regulated entities to develop and publicly post a "Consumer Health Data Privacy Policy." This document must contain the following elements:

1. The *categories of consumer health data* collected;
2. The categories of *sources* from which consumer health data is collected;
3. The *purposes* for which consumer health data is collected and used;
4. The categories of consumer health data that is *shared*;
5. A list of the *categories of third parties* with which consumer health data is shared;
6. A list of the *specific affiliates* with which consumer health data is shared; and
7. A description of how a consumer can *exercise the rights* of access, deletion, and withdrawal of consent (as provided in section 6 of the Act).

As practitioners who have drafted or reviewed privacy statements (also referred to as privacy policies or privacy notices) required under *other* privacy laws will readily recognize, nearly everything on this list is commonly found in most organizations' existing privacy statements.

For example, the CCPA requires that a business have a "privacy policy" that includes, among other things, disclosures that are substantively equivalent to every item on the above list, except #6. Likewise, the EU GDPR requires that data controllers provide notice that contains nearly all of the above elements. Moreover, those laws (and others) specifically categorize health data as a special

category of sensitive data such that such data is typically specifically called out in the privacy statements of organizations that process such data.

The result is that because most organizations are subject to a number of privacy laws across jurisdictions that require privacy notices, nearly every organization already must have a comprehensive, general privacy statement that describes nearly everything that must also be in a MHMDA Consumer Health Data Privacy Policy.

A List of Specific Affiliates

The one outlier in the MHMDA list of required disclosures is the list of "specific affiliates" with which consumer health data is shared. The scope of the requirement turns on the definition of "affiliate", which is, in relevant part, "a legal entity that shares common branding with another legal entity and controls, is controlled by, or is under common control with another legal entity." Thus, ***while every other type of third party with which data may be shared should be listed at the category level, those entities that meet the "affiliate" definition must be specifically listed***.

This one is just weird. It's counterintuitive and counterproductive, imposing a more burdensome requirement and putting a heightened focus on sharing with the one category of third parties that is likely to raise the fewest privacy issues. There is good reason why it does not appear in other privacy laws.

First, in light of the definition of "affiliate," the requirement applies only to those affiliated entities that share common branding. From a transparency perspective, this gets it exactly backwards. The common branding already signals to consumers that these entities are closely related and that data sharing among them is likely. It's the affiliates that lack common branding where consumers might not understand the relationship between them and where heightened transparency may therefore be warranted. But that's not required here.

Second, the "common control" element of the definition also suggests that data sharing with such affiliates present fewer privacy concerns than sharing with third parties where such control does not exist. Such entities often share common backend data systems and so "sharing" is indistinguishable from routine internal processing within a corporation. Often, such affiliates effectively operate as a single entity, under common policies and complaince programs. The fact that a corporation consists of multiple legal entities rather a single legal entity typically does not affect how data is processed and protected. The common control enables a level of assurance with respect to data protection that just does not and cannot exist when data is shared with other types of third parties.

Again, the requirements to hold this type of sharing to a higher transparency standard makes no sense and distracts from consumer disclosures that are more meaningful. Still, it is a requirement that regulated entities must now add to their notice obligations.

Categories of Consumer Health Data

One other required element of a Consumer Health Data Privacy Policy that potentially goes beyond what is currently required and common in privacy statements is the inclusion of "the categories of consumer health data collected."

Other privacy laws require that privacy notices include the categories of "personal data" collected and processed, and organizations might list "health data" as one of those categories. However, given the very broad definition of "consumer health data" under the MHMDA, along with the implicit requirement that this broad category should be broken down into different subcategories in a Consumer Health Data Privacy Policy, regulated entities may have to rethink how they categorize the broad range of personal data that may qualify as consumer health data under the Act. At a minimum, they will likely ***need to describe health data both more broadly and more granularly*** than they currently do.

Fortunately, ***MHMDA seems to allow regulated entities significant flexibility in how they categorize and describe consumer health data***. This flexibility is in contrast to California's CCPA, which suggests that the categories of data listed should align with the statutory definition of "personal information" – constraining flexibility and leading to some very awkward descriptions. Nevertheless, while the MHMDA does not provide any similar direction on how consumer health data should be broken down into different categories, it may still be prudent to look to the definition of consumer health data for guidance. But regulated entities should be free to formulate and describe data categories in a sensible way that aligns with how it processes data and that will be understandable and meaningful to consumers.

A Separate Notice Document

Given that most organizations already have a privacy statement that contains most of what is required in this new Consumer Health Data Privacy Policy, can they just add the list of affiliates to their privacy statements, expand on the categories of health data, and then call it good? That approach would be the simplest for regulated entities, and likely best for consumers as well, but unfortunately, it is risky.

While not explicitly stated, ***the clear implication of the statutory language is that the Consumer Health Data Privacy Policy is a separate document from the regulated entity's general privacy statement***. Thus, it appears that the notice requirements of MHMDA cannot be met by simply incorporating the required elements into the entity's existing privacy statement.

As a result, consumers are likely to be confronted with multiple, overlapping privacy notice documents when dealing with regulated entities. In addition to the Consumer Health Data Privacy Policy required by MHMDA, there will be a general privacy statement as s required by multiple other privacy laws. There may also be a "notice at collection" as required by CCPA (although this *can* be incorporated into the general privacy statement). If the entity has some part of its operations covered by HIPAA, there will likely be a separate HIPAA privacy notice. The addition of the Consumer Health Data Privacy Policy creates or contributes to a confusing web of notice documents

for the consumer to navigate. Those consumers who want the "full picture" will have to read through two or more privacy notice documents that are largely, but not entirely, redundant. The practical impact will be to frustrate consumers and make it more difficult to find the information that is most relevant to them. This approach of a separate notice is more likely to undermine transparency rather than enhance it.

Companies that are committed to doing the right thing for consumers may have to get creative in how they meet these new requirements without burdening and confusing consumers. Unfortunately, with the private right of action under MHMDA, creativity and doing anything other than the literal requirements carries risk.

Link on the Homepage (and every other page)

The Act requires that there be a prominent link to the Consumer Health Data Privacy Policy on a regulated entity's homepage. But "homepage" doesn't just mean the main landing page of the regulated entity's website. Like so many other terms in the Act, it is defined in a way that is much broader than its commonly understood meaning.

A "homepage" under the MHMDA is "the introductory page of an internet website *and any internet webpage where personal information is collected*" (emphasis added). Note that this definition says any page where "personal information" is collected – not just where consumer health data is collected. "Personal information," in turn, is defined broadly to include, among other things, an IP address. Because an IP address is necessarily collected on each and every webpage (that whole "that's how the Internet works" thing), under MHMDA, "homepage" means "every page." Thus, ***the link to the Consumer Health Data Privacy Policy must appear on <u>every</u> page of a regulated entity's website(s)*** – whether or not those pages have anything to do with the collection of consumer health data.

Further, the definition of "homepage" further specifies that for apps, the link must be on the application's "platform page or download page" and within the app itself.

While this requirement is not as technically difficult to implement as many of the other requirements under the Act, it will contribute to an increasingly cluttered list of privacy links that will be unnecessarily confusing for consumers. As discussed above, ***the growing number of privacy laws that require their own special privacy notices and links will create more consumer confusion and frustration***, ultimately undermining the goals of transparency and consumer empowerment.

There may be some alternative approaches that regulated entities might want to consider, which may assume some risk by relying on the fact that the statutory language does not explicitly say that it must link "directly" to the privacy policy. Regulated entities must evaluate the operational and consumer benefits of such alternatives against the risk if not taking the safest route of a dedicated, direct link to a consumer health data privacy policy.

Go Broad and Future Proof

The Act includes other requirements that are tied to, and dependent upon, the content of the Consumer Health Data Privacy Policy.

Specifically, the Act requires regulated entities to obtain opt-in consent for any collection, use, or sharing of additional categories of consumer health data not disclosed in the policy and for any collection, use, or sharing of consumer health data for additional purposes not disclosed in the policy. Further, regulated entities cannot contract with a processor for any processing of consumer health data inconsistent with the Consumer Health Data Privacy Policy.

The implication of these two provisions is that ***regulated entities should make sure that the Consumer Health Data Privacy Policy is thorough, accurate, and broad enough to cover all current and anticipated data collection, use, and disclosure***. Describing the data categories and purposes in broad, general terms, in addition to providing specific examples and details, may be one useful approach to help ensure that regulated entities are not later facing the need to get new consents and/or limit their use of processors.

Timing

As discussed in Part 4 of this series, the way effective dates were incorporated into the Act has created confusion and uncertainty. In particular, for certain sections of the Act, including Section 4, which sets out these notice requirements, the effective date of March 31, 2024, was added to only the first subsection of the section. The subsequent substantive subsections are silent as to effective dates. And under Washington law, when legislation is silent on effective dates, the requirements come into effect 90 days after the end of the legislative session. In this case, that would be late July 2023.

Thus, when read literally, it appears that the first subsection will come into effect March 31, 2024, but the subsequent substantive subsections will come into effect late July 2023. But for the notice requirements of Section 4, such a literal reading leads to absurd results. For example, the requirement to have a consumer health data privacy notice is in the first subsection, with an effective date. Thus, the Act states that ***regulated entities need not publish a Consumer Health Data Privacy Policy until March 31, 2024***. However, other requirements in that section, including the requirement to have a homepage link to the Consumer Health Data Privacy Policy are silent on effective dates, and therefore could come into effect in late July 2023.

Does this mean that companies should post a link that goes to a page that says "coming soon"? Well, that might be the safest approach. But I suspect few companies will. The result of the literal reading of effective dates in this section is so ridiculous that it is likely courts confronting this issue would adopt a more sensible reading that is more aligned with what is the clear legislative intent to have the notice obligation – *and those requirements that flow from it* – come into effect next year. Further, plaintiffs would have a very hard time demonstrating any harm resulting from not having a link to nowhere.

Similarly, the other obligations under Section 4 are closely tied to the requirement to post the Consumer Health Data Privacy Policy, and it would be equally absurd to interpret those as coming into effect before the requirement to post the policy is in effect.

That's not to say that plaintiffs' counsel won't try to argue an earlier effective date applies to some aspects of the Section 4 notice requirements. But in terms of risk-based compliance planning and prioritization, regulated entities may conclude that in light of the many other challenges with this law, rushing to get notice requirements implemented by July of this year need not be the top priority. Nevertheless, regulated entities should begin this and other compliance tasks as soon as possible because even a March 31, 2024, effective date does not provide a lot of time.

As noted above, future posts will discuss other aspects of the Act and the issues it raises.

Part 9: The Attorney General's Guidance

By Mike Hintze • July 5, 2023

This part discusses the highly-anticipated, but non-binding, guidance published by the Washington State Office of the Attorney General.

On Friday, June 30, the Washington State Office of the Attorney General (OAG) published its expected guidance on the Washington My Health My Data Act (MHMDA or the Act) in the form of seven "frequently asked questions." Given the many ambiguities in the Act, this guidance has been eagerly awaited in the hope that it would provide some much-needed clarity. And while it addresses one of the biggest areas of ambiguity and concern (the effective dates) and provides some useful insights into a handful of others, it, unfortunately, left many questions unanswered.

Further, to understand the impact of this guidance, it is important to note that the Act does not give the Attorney General formal rulemaking authority. Nor is this guidance a formal Attorney General opinion. In fact, the text at the end of the guidance reinforces its informal and nonbinding nature:

> This FAQ may be periodically updated and is provided as a resource for general educational purposes and is not provided for the purpose of giving legal advice of any kind. Readers should not rely on information in this guide regarding specific applications of the law and instead should seek private legal counsel.

Thus, it is clear that this guidance does not have the force of law. And judges may feel free to ignore it if they determine the language of the statute leads to a different interpretation.

Nevertheless, particularly because the Act originated with an Attorney General requested bill, and the OAG played a key role in the formulation of the legislation, the views of that office are likely to be taken as persuasive. Therefore, this guidance may give organizations seeking to comply with the law greater comfort that a particular interpretation may prevail. As such, these FAQs should be carefully considered by those seeking to develop MHMDA compliance plans.

Effective Dates

One of the most troublesome and concerning aspects of the Act is the way the effective dates were added to the statute. As discussed in Part 4 of this blog series, in several instances, effective dates were added to only the first subsection of a section in a way which, if read literally, would seem to apply to only that first subsection and not the subsequent parts of that section. Because those subsequent subsections were silent on effective dates, under Washington law, where an effective date is not stated in legislation, the relevant provisions come into effect 90 days after the end of the legislative session. In this case, that would be late July of this year. That literal interpretation, however, would lead to several absurd results.

The legislative history, as well as statements made by key players in the legislative process, suggest this problem was a drafting oversight and that the effective dates were intended to apply to the

entirety of each section in which they appear. FAQ 1 of the new guidance, as expected, reflects that interpretation.

It states that for most of the substantive sections of the Act (i.e., sections 4-9), the requirements will come into effect March 31, 2024, with a delay until June 30, 2024, for those regulated entities that meet the definition of a "small business." Only the prohibition on geofencing in section 10 of the Act, which is entirely silent on affected dates, will come into effect in late July of this year.

This guidance should give some comfort to companies that have been working on compliance but have realized that meeting many of the substantive obligations requires work that could not possibly be completed by late July of this year. Of course, because this guidance is not binding law, it is still possible that plaintiffs' lawyers will seek to test this issue by claiming that the plain, literal reading of the statute results in a much earlier effective date for many of its substantive obligations. If aggressive plaintiffs seek to pursue such claims, this guidance should strengthen defensive arguments that such an overly-literal interpretation is contrary to legislative history and intent and, therefore, should be rejected.

The Scope of Consumer Health Data

As discussed in Part 2 of this blog series, the definition of "consumer health data" is extraordinarily broad and raises a number of questions about just how expansively it can be construed. FAQs 5 and 6 attempt to shed some light on the scope of consumer health data. But they focus on only two areas and leave a large number of much more significant ambiguities unresolved.

FAQ 5 addresses the question of whether information about the purchase of toiletries (deodorant, mouthwash, toilet paper, etc.) constitute consumer health data because they relate to "bodily functions." The OAG states that "ordinarily, information limited to the purchase of toiletry products would not be considered consumer health data." By way of example, it states that "information about the purchase of toilet paper or deodorant is not consumer health data, an app that tracks someone's digestion or perspiration is collecting consumer health data."

Unfortunately, this guidance does little to provide much clarity or to constrain the potential sweeping scope of consumer health data.

First, the general statement quoted above is qualified by "ordinarily" – suggesting that there are exceptions. What are those exceptions? How many are there? Could the exceptions swallow the rule?

Second, the examples offered for what falls outside the scope reflect only an extreme benign end of the range of common product purchase information that could constitute consumer health data. Virtually every person purchases and/or uses toilet paper and deodorant, and the purchase of such products does not reveal anything about a person's health. And even if it did, from a risk perspective, it is highly unlikely that the OAG would pursue a case involving such benign data or that a plaintiffs' counsel could demonstrate any injury supporting a recovery in litigation.

But what about the other types of purchase information connected to health, wellness, fitness, or nutrition which, though various elements of the "consumer health data" definition, are arguably covered? What about purchases of running shoes, low-calorie or high-fiber foods, exercise equipment, vitamins, meditation recordings, or gym memberships? These are examples that have been raised in this this blog series and elsewhere but, unfortunately, they are not addressed in the FAQs and the questions being raised about them remain unanswered.

Third, the examples provided for what *is* covered, if anything, ***reinforce the extremely broad nature of consumer health data***. We already knew that those involved in the drafting of the bill were focused on certain data collected by applications. The clearest example, which was raised several times by bill supporters in testimony and elsewhere, is menstruation tracking apps that could reveal pregnancy. Here, the FAQ states that apps that track "digestion or perspiration" are also covered. Unlike menstruation, digestion and perspiration is something that every person does virtually every day. And perhaps with some exceptions at the extremes, such information, by itself, is not likely reveal any particular health status or condition. These examples thereby suggest that ***the "bodily function" aspect of the definition will be interpreted very expansively by the OAG***.

FAQ 6 addresses inferences. It was already reasonably clear that ***inferred health data is in scope***. Supporters' testimony and other statements made thorough the legislative process repeatedly cited the 2012 example were Target used purchase data related to a range of products to predict the likelihood that a consumer is pregnant. And this FAQ repeats that example and reiterates that such an inference is consumer health data. FAQ 6 notes that even health-related inferences made from the purchase of toiletries, tying back to the examples of non-health data cited in FAQ 5, would be consumer health data.

Interestingly, FAQ 6 concludes with the following: "In contrast, nonhealth data that a regulated entity collects but does not process to identify or associate a consumer with a physical or mental health status is not consumer health data." Clearly, the inference of a physical or mental health status itself is consumer health data. But if non-health data is used to draw that inference, does that underlying data thereby become consumer health data? The above-quoted statement suggests it might.

If non-health data is *not* processed to infer a health status (thereby identifying or associating the consumer with that status), then it is *not* consumer health data. The converse of that suggests that if it is so processed, then ***that underlying (previously non-health) data might be transformed into consumer health data by virtue of it being used to infer health status***. Thus, would a consumer have the right to request the regulated entity to delete not only the inference but also the underlying purchase data used to create that inference? While not squarely addressed by this FAQ, the implication is that it would.

Together, FAQs 5 and 6 provide some insight into the views of OAG on the definition of consumer health data – reinforcing that it is, indeed, very broad. But there are many, many other ambiguities inherent in the definition of consumer health data that are not addressed in the FAQs. Hopefully,

future updates to the OAG guidance will provide additional insights, but many gray areas will inevitably remain. Organizations will still need to make reasonable, risk-based classifications of the data they collect (and derive or infer) to guide their compliance approaches under the Act.

Resolving the Conflict Between Retention and Deletion Obligations

As described in Part 6 of this blog series, MHMDA gives consumers broad rights. And the right to have consumer health data deleted upon the consumer's request lacks common exceptions found in virtually every other privacy law – including an absence of an exception for situations in which retention of the data is required by law. Part 5 of this blog series notes that such a retention requirement exists in the Act itself, setting up an internal contradiction and a potential litigation trap.

Specifically, the onerous "authorization" requirements for any transfer of consumer health data that could constitute a "sale" include the requirements that the authorization documentation contain the consumer health data to be sold and that both the seller and the buyer of the data retain that authorization document for six years. Thus, if the consumer who provided the authorization thereafter requests that either the buyer or the seller delete their consumer health data, the entity would be in a catch-22 position of having to violate either the deletion obligation or the obligation to retain the authorization containing that data.

FAQ 7 resolves that conflict by clarifying that ***in response to such a deletion request, the entity can and should redact the consumer health data from the authorization*** while continuing to retain the redacted document for the required period. Given the nature of the conflict, this is a sensible resolution. Those companies that seek authorizations to sell consumer health data will surely find some comfort in this guidance. The practical impact, however, is likely to be minimal because the requirements for obtaining a valid authorization remain so onerous that few companies will regularly seek to obtain them.

Privacy Policy Links

FAQ 4 addresses the requirement from Section 4(b) of the Act that a regulated entity must post a link to the required Consumer Health Data Privacy Policy on its homepage. As discussed extensively in Part 8 of this blog series, this seemingly simple requirement includes more than is apparent on its face and raises a number of challenging issues. Unfortunately, this FAQ takes on none of those issues and merely quotes the statutory language on the one, narrow issue it addresses, adding no new insight or information.

It would have been helpful, for example, if the FAQ addressed whether the link must be direct. In other words, is a "privacy" link to the entity's general privacy statement, which in turn links to a more specific Consumer Health Data Privacy Policy, sufficient to meet this obligation? Relatedly, can the Consumer Health Data Privacy Policy be incorporated into the general privacy statement, or does it absolutely have to be a stand-alone document, even if redundant of information that is already in the general privacy statement? Or it could have addressed any of the other genuinely difficult questions that the Act's notice obligations raise. Instead, it addressed a question the answer to which

was already apparent from the statutory language, as evidenced by the fact that the FAQ did nothing other than repeat that language.

Scope of Regulated Entities, Extraterritorial Impact, and Data Storage Location

FAQ 3 poses the following question: "**How will a business located outside of the state of Washington but that stores its data in Washington be impacted**?"

The formulation of the question suggests that it would address one of the more opaque but hugely impactful issues raised by the Act – the extraterritorial range of "consumers" whose data is within the scope of the Act (created by the odd definition of "collect" – as described below). But it did not. Instead, it mainly focused the scope of regulated entities covered by the Act. Both of these issues are separately discussed in Part 3 of this blog series, but it appears as if the OAG's FAQ 3 conflates them.

Here too, the FAQ reiterates the statutory language to answer the question it poses:

> Subject to some exceptions, a regulated entity is a legal entity that (a) conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington and (b) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data.

Clearly, to be a regulated entity, an organization must meet both of those two prongs from the statutory definition. If it does, it is a regulated entity subject to the Act. If it does not, it is not a regulated entity. So, the next statement in the FAQ should come as no surprise: "An entity that only stores data in Washington is not a regulated entity." Of course, it isn't – unless it meets the two prongs of the statutory definition. Whether or not an organization stores data in Washington is irrelevant to the question of whether the organization is a regulated entity that is subject to the Act. And nobody who has carefully read the statute has ever suggested otherwise.

But location of data storage *is* relevant to the definition of "consumer." That is because a consumer is defined as "(a) a natural person who is a Washington resident; or (b) a natural person whose consumer health data is *collected* in Washington" (emphasis added). "Collect" in turn, is defined as "to buy, rent, access, retain, receive, acquire, infer, derive, or *otherwise process* consumer health data in any manner" (emphasis added). And finally, "process" means "any operation or set of operations performed on consumer health data." The breadth of these cascading definitions suggests that consumer health data from an individual with no connection to Washington could be subject to the Act if the data is stored in Washington. That is, if the data is stored in Washington, it would be "processed" in Washington and, therefore, "collected" in Washington, making that individual a "consumer" for purposes of the Act.

So why is data location important? Not because it impacts whether an organization is a regulated entity subject to the Act, as the question posed in this FAQ suggests. But rather, because it impacts the entirely separate question of how many individuals' data would be subject to the Act. This is an

important question because it can dramatically impact the volume of data that a regulated entity must treat as subject to the Act's requirements. And, in light of the Act's private right of action, it can dramatically impact the size of a potential class of plaintiffs. If the scope of "consumers" and, therefore, the potential class were limited to only residents of Washington and others whose data was actually collected (in the normal sense of the word) in Washington, that could be a quite small percentage of an organization's global customer base. But if it includes all individuals whose data in some way touches Washington state, that could be the organization's entire global customer base. For plaintiffs' counsel, this significantly increases their financial incentives to bring claims and litigate.

Unfortunately, FAQ 3 did not address this much more interesting and impactful question about data location.

It did, however, shed some light on one question raised by the definition of regulated entity. Recall that the first prong of the definition is that the entity "conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington." There is some question about what it means to "target" consumers in Washington. And when the FAQ states that in general, all entities that "conduct business in Washington (or provide services or products to Washington)" may be subject to the Act, it suggests a broad reading of "targeted" – equating targeting with providing. Part 3 of this series suggested that it was likely enough that the company makes its online services or websites avaialble to or accessible by consumers located in Washington, and this language in the FAQ supports that broader reading.

Interestingly, FAQ 3 also points out that two sections – Section 9, which sets out the "authorization" requirement for data "sales," and Section 10, which prohibits certain uses of geofencing – apply to all "persons" and not just regulated entities and that the scope of "persons" is not limited by geography. This means that these provisions apply to individual natural persons – and not just businesses and other organizations. And, importantly, they apply to both individuals and organizations located anywhere in the world without regard to whether they conduct business in Washington or provide services or products to Washington. Whether the more extreme examples of potential extraterritorial application will have meaningful, real-world impact remains to be seen. But the potential this creates is quite stunning and fascinating.

Finally, FAQ 3 states that processors located out of state who are processing data on behalf of regulated entities are subject to the Act. But that was not really in doubt.

Enforcement

FAQ 2 is perhaps the most obvious and, therefore, least interesting of those contained the OAG's guidance. It asks: "**What is the Attorney General's role in enforcing the My Health My Data Act?**" And it answers with what we stated in Part 1 of this blog series and which anyone who has followed this Act already knows – that a violation of the MHMDA is deemed to be a violation of Washington Consumer Protection Act, which can be ***enforced by the Attorney General and/or through a private right of action***. Here too, there are a number of interesting issues related to

enforcement, which the FAQ does not address. Those issues may be a topic for a further blog post in this series.

Future posts will discuss other aspects of the Act and the issues it raises.