Skadden

Privacy & Cybersecurity Update

1 California Regulators Finalize CCPA Regulations That Reflect CPRA Requirements

2 Washington State Becomes First State To Pass Comprehensive Health Data Privacy Law

4 US Appeals Court Finds Coverage Under a Crime Policy for a Fraudulent Wire Transfer Loss

5 HHS Issues a Notice of Proposed Rulemaking To Modify Protections for Reproductive Health Information

6 FDA Issues Guidance to Health Care Industry and Agency Staff on Medical Device Cybersecurity

California Regulators Finalize CCPA Regulations That Reflect CPRA Requirements

The California Office of Administrative Law (OAL) has approved final amendments to California's regulations implementing the California Consumer Privacy Act (CCPA) to adhere to requirements under the California Privacy Rights Act (CPRA).

On March 30, 2023, the OAL gave final approval to various amendments to its CCPA regulations proposed by the California Privacy Protection Agency (CPPA) to reflect the requirements of the CPRA. Previously, in our February 2023 *Privacy & Cybersecurity Update*, we discussed how the first batch of the amended CCPA regulations were expected to take effect in late March or early April at the earliest. In February 2023, the CPPA had approved the final draft of the proposed amended regulations. The finalized regulations do not contain any substantive changes since their initial submission in October 2022 and the text and supporting materials are now available on CPPA's website.

We also described the proposed (and now final) regulations — and certain topics that have yet to be addressed — in our November *2022 Privacy & Cybersecurity Update*.

The regulations are effective immediately. As we previously recommended, any companies that may have been delaying the process of revising their privacy policies, notices, practices and contractual provisions to comply with the CCPA (as amended by the CPRA) until those amendments were finalized, can do so now.

CCPA Regulators Speak on Compliance

Two prominent CCPA enforcement figures, CPPA Executive Director Ashkan Soltani and California Supervising Deputy Attorney General Stacey Schesser, spoke at the IAPP Global Privacy Summit 2023 on April 5, 2023.

While recognizing that the first batch of regulations represent a significant advancement, Mr. Soltani also pointed out that there is still much work to be done. He reminded the attendees (and the public) that the noncompliance notice and 30-day opportunity that were once available under the CCPA of 2018 to cure violations were eliminated by the CPRA amendment. Instead, the CPPA may, at its discretion, issue cure notices to

noncompliant parties. Such cure notices can only be issued by the CPPA, with the attorney general able to act immediately on any violations.

Shedding more light on the different roles of the CPPA and the attorney general in CCPA enforcement, Ms. Schesser mentioned that the CPPA would be handling administrative enforcement, while the attorney general may be focusing on more complex cases because of the office's capability to combine multiple theories of liability that go beyond the purview of the CCPA.

Perhaps reassuring for those under the CCPA's purview was Mr. Soltani's emphasis that the CPPA will stick to the enforcement reprieve, which we also previously discussed in our January 2023 *Privacy & Cybersecurity Update*. The amended regulations provide that the CPPA "may consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good-faith efforts to comply with those requirements," thus giving the agency the flexibility to exercise some discretion in deciding whether and when to take enforcement steps. This discretion offers no guarantee, however, that the CPPA will delay enforcement in any particular instance.

Upcoming Rulemaking Activities

As we've written previously, the CPPA already initiated preliminary rulemaking activities on its next rulemaking package, which will, at the least, address the three outstanding topics — cybersecurity audits, risk assessments and automated decision-making — in February 2023. We will provide periodic updates on such upcoming rulemaking activities.

Key Takeaways

With the approval of the amended CCPA regulations, companies that have been waiting for the final regulation before taking steps to updated their compliance practices can and should accelerate that process now.

The CCPA regulatory process is not yet over. However, with these amendments completed, the CPPA can now devote its resources to developing further amendments and guidance in this area, meaning companies should continue to pay close attention to the agency's activities.

Return to Table of Contents

Washington State Becomes First State To Pass Comprehensive Health Data Privacy Law

Washington state has become the first state to pass a consumer health data privacy law, expanding on the protections offered by HIPAA.

On April 27, 2023, the state of Washington enacted the My Health My Data Act (MHMDA)[1], which seeks to expand the protections applicable to consumer health data by narrowing the gap between the protections that consumers expect to apply to their health data and actual industry practices, through which laws like HIPAA offer only limited protections. Under the MHMDA, many entities not currently subject to laws like HIPAA will become subject to broad obligations involving consumer health data as a result of the legislation.

Broad Applicability of the MHMDA

The MHMDA imposes obligations on regulated entities regarding consumer health data.

- "Consumer health data" is defined to cover "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 incorporates a nonexhaustive list of data that comprises consumer health data, including health conditions, treatment, diseases, procedures, diagnoses, reproductive or sexual health information, gender-affirming care, biometric and genetic information, and medication purchases. Beyond these categories, consumer health data also includes "precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies" and health data that is "derived or extrapolated from nonhealth information."
- "Consumers" comprise natural persons who are either Washington state residents or whose consumer health data is collected in Washington state (in each case, other than individuals acting in an employment context).
- "Regulated entities" subject to the MHMDA comprise any legal entity that conducts business in Washington state (or produces or provides products or services targeted to consumers in the state) and, individually or jointly, "determines the purpose and means of collecting, sharing, or selling consumer health data." Whereas laws like HIPAA only cover health data collected by specified health care entities, the MHMDA's broad definition of regulated entities would supplement HIPAA by

[1] The full text of the MHMDA is available here.

covering entities beyond its scope, including health-related websites and apps. The MHMDA also presents a notable departure from other state privacy laws (like California's CCPA) in that there is no revenue threshold in determining the law's applicability.

Information subject to laws such as the GLBA, the Fair Credit Reporting Act (FCRA), Family Educational Rights and Privacy Act (FERPA) and HIPAA is expressly excluded from the MHMDA. Additionally, the MHMDA is applicable to certain entities, including government agencies, tribal nations and contracted service providers processing consumer health data on behalf of a government agency.

MHMDA Requirements

The MHMDA imposes broadly applicable requirements on regulated entities' ability to collect, share and sell consumer health data, including by requiring such entities to maintain consumer health data privacy policies, obtain separate consents for collection and sharing of consumer health data, receive valid authorization prior to any sale of such data and implement data security practices to restrict access to and use of consumer health data. The MHMDA empowers consumers with certain individual data rights (including rights to confirm whether their health data is being collected, shared or sold; to withdraw consent from collection and sharing; and to request deletion of consumer health data) and would prohibit the use of geofences around facilities that provide health care services.

Consumer Health Data Privacy Policies

A regulated entity must maintain (at a prominent link on its homepage) a consumer health data privacy policy that clearly and conspicuously describes the following:

- categories of consumer health data collected (including the purpose and use associated with such collection);
- categories of sources from which consumer health data is collected;
- categories of consumer health data shared;
- categories of third parties and specific affiliates with which consumer health data is shared; and
- instructions on how a consumer can exercise the data rights provided by the MHMDA (discussed further below).

To the extent a regulated entity wishes to collect, use or share categories of consumer health data not disclosed in the consumer health data privacy policy, or wishes to take such actions for additional purposes not disclosed in the policy, the regulated entity must first disclose such additional categories and purposes, as applicable, and obtain the consumer's affirmative opt-in consent prior to the data's collection, use or sharing.

Consents and Authorizations for Collection, Sharing and Sales of Data

The MHMDA prohibits collecting or sharing consumer health data, except with prior affirmative consent from the consumer for such collection or sharing for a specified purpose (or to the extent required to provide a product or service that the consumer requested). A regulated entity must obtain separate consents for collection and sharing. Any request for consent must clearly and conspicuously describe the categories of consumer health data collected or shared, the purpose for such collection or sharing, the categories of entities with which the consumer health data is shared and instructions on how the consumer can withdraw consent from future collection or sharing of health data.

Similarly, the MHMDA prohibits the sale or offering of the sale of consumer health data without having obtained a valid authorization from the consumer for such sale, which must be distinct from the consents obtained for the collection and sharing of consumer health data. Valid authorizations to sell consumer health data must be written in plain language and contain, among other enumerated items, the name and contact information of the individuals collecting, selling and purchasing the consumer health data, and an expiration date that renders the authorization invalid one year after the date the consumer signs the authorization.

Consumer Data Rights

The MHMDA grants consumers a set of individual rights, including:

- the right to know whether a regulated entity is collecting, sharing or selling the consumer's health data, and the right to access such data (including a list of all third parties and affiliates with which the consumer health data has been shared);
- the right to withdraw consent from collection and sharing of the health data; and
- the right to have the health data deleted by submitting a request for deletion.

Unlawful discrimination against a consumer for exercising any rights included in the MHMDA is expressly prohibited.

Mandated Data Security Practices and Data Processing Agreements

Under the MHMDA, a regulated entity must restrict access to consumer health data by employees, processors and contractors to those with a need to access such information to advance the purposes for which the consumer provided consent, or where required to provide a product or service that the consumer has requested. The MHMDA also requires that a regulated entity establish, implement and maintain administrative, technical and physical data security practices to protect consumer health data that, at a minimum, satisfy a reasonable standard of care within the regulated entity's industry.

Additionally, the MHMDA provides that data processors may process consumer health data only pursuant to a binding contract between the processor and the regulated entity that sets forth the processing instructions and limits the actions the processor may take with respect to consumer health data.

Prohibition on Geofencing

The MHMDA prohibits the implementation of a geofence around any entity that provides in-person health care services. This would apply in cases where the geofence is used to identify or track consumers seeking health care services, collect consumer health data or send notifications, messages or advertisements to consumers related to their consumer health data or health care services.

Timeline and Enforcement

The MHMDA will go into effect gradually, with a March 31, 2024, deadline for most businesses and a June 30, 2024, deadline for small businesses. Any violation of its requirements would constitute a violation of the Washington Consumer Protection Act,[2] which is enforceable by the state attorney general and by a private right of action, which is uncommon in the privacy space outside the context of the Illinois Biometric Information Privacy Act.

Key Takeaways

With the passage of the MHDMA, Washington state has enacted the first state-level comprehensive consumer health privacy law in the United States. We will report on any updated guidance on implementation of the MHMDA's provisions that may be issued.

Return to Table of Contents

[2] The full text of the Washington Consumer Protection Act is available here.

US Appeals Court Finds Coverage Under a Crime Policy for a Fraudulent Wire Transfer Loss

The U.S. Court of Appeals for the Fifth Circuit has affirmed a district court's decision that ruled RLI Insurance Company (RLI) owed coverage under a crime policy issued to its insured, escrow agent Valero Title Inc. (Valero), for a fraudulent transfer that occurred when a malicious actor duped a Valero employee into wiring funds into the malicious actor's account.[3]

The Fraudulent Transfer and RLI's Denial of Coverage

Valero purchased a crime policy from RLI that included a Funds Transfer Fraud endorsement providing that RLI "will pay for loss of funds resulting directly from a fraudulent instruction directing [sic] financial institution to transfer, pay or deliver funds from your transfer account." As relevant here, the endorsement defined "fraudulent instruction" as a "written instruction . . . issued by you, which was forged or altered by someone other than you without your knowledge or consent, or which purports to have been issued by you, but was in fact fraudulently issued without your knowledge or consent."

Shortly after the policy went into effect, a malicious actor posing as an employee of one of Valero's lending banks tricked a company employee into wiring $250,945.31 into an account controlled by the cyber attacker. Valero subsequently submitted a claim to RLI seeking coverage under the policy's Funds Transfer Fraud endorsement. RLI determined that the loss was not covered by the endorsement and therefore denied Valero's claim.

Valero's Coverage Action Against RLI

As a result, Valero sued RLI in the U.S. District Court for the Southern District of Texas seeking coverage for the loss. At issue was the definition of "fraudulent instruction." Valero and RLI agreed that the relevant "fraudulent instruction" definition created two distinct coverage scenarios, which the district court labeled "Clause A" ("written instruction . . . issued by you, which was forged or altered by someone other than you without your knowledge or consent") and "Clause B" ("written instruction . . . which purports to have been issued by you, but was in fact fraudulently issued without your knowledge or consent"). The parties' dispute involved Clause A.

Valero and RLI cross-moved for summary judgment. In its motion, RLI argued that because the wire instructions that Valero sent to the bank were not in fact forged or altered after they were

[3] The decision is *Valero Title Inc. v. RLI Ins. Co.*, No. 22-20155, 2023 WL 1434270 (5th Cir. Feb. 1, 2023).

issued by Valero (rather, Valero's instructions were based on forged or altered instructions from the malicious actor), there was no "fraudulent instruction" to trigger coverage under the Funds Transfer Fraud endorsement. The district court rejected RLI's argument and granted summary judgment in favor of Valero, concluding that Clause A of the "fraudulent instruction" definition should be interpreted to mean any such instruction that is forged or altered by someone other than the insured without the insured's knowledge or consent *prior to* being issued by the insured.

RLI appealed to the Fifth Circuit, asserting that the district court erred in interpreting the Funds Transfer Fraud endorsement. In affirming the district court's decision and rejecting RLI's interpretation of the endorsement, the Fifth Circuit observed that the instruction Valero issued to its bank was identical to the one received from the fraudster posing as the lender — it was not the same as the instruction provided by the lender because it was altered to include different recipient account information. Thus, the Fifth Circuit found that when Valero issued the instruction to its bank, it was a fraudulent instruction that was "forged or altered by someone other than [Valero] without [Valero's] knowledge or consent" and therefore fell within the scope of the Funds Transfer Fraud endorsement.

Key Takeaways

The Fifth Circuit's decision is a reminder of the importance of fastidiously employing multiple safeguards and confirmation systems when wiring money or otherwise transferring funds, even when transacting with known business partners. From an insurance perspective, the decision also is instructive of the need to carefully review an insurance policy's language and ensure that both the insurer and policyholder have a mutual understanding of the scope of coverage.

Return to Table of Contents

HHS Issues a Notice of Proposed Rulemaking To Modify Protections for Reproductive Health Information[4]

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued a Notice of Proposed Rulemaking (NPRM) to modify protections for reproductive health information under HIPAA.[4]

Following the Supreme Court's *Dobbs v. Jackson Women's Health Organization*[5] decision that eliminated constitutional protections for abortion rights, on April 12, 2023, the OCR issued a NPRM on proposed changes to HIPAA regulations to enhance for protected health information (PHI) related to reproductive health. The NPRM follows a July 2022 executive order[6] signed by President Joe Biden that directed HHS to consider taking certain actions to better protect patient-provider confidentiality in this area.

HHS made clear that the NPRM does not provide a "blanket protection" for all reproductive health information, but is intended to be a narrowly tailored "purpose-based prohibition" to address only uses and disclosures for specific prohibited purposes. For example, a covered health care provider could continue to use or disclose PHI for treatment or payment purposes for reproductive health care or other conditions that affect an individual's reproductive health (*e.g.*, routine pregnancy tests before surgery). Additionally, since HIPAA's Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) generally preempts state laws, OCR made clear that the proposed prohibition would only apply where a state "lacks any substantial interest in seeking the disclosure."

Comments to the NPRM are due on or before June 16, 2023.

Prohibition on Certain Uses or Disclosures of PHI

The NPRM proposes to modify the Privacy Rule by prohibiting individuals, covered entities or their business associates (regulated entities) from using or disclosing PHI for either:

- a criminal, civil, or administrative investigation into or proceeding against any person in connection with seeking, obtaining, providing or facilitating reproductive health care that: (i) is provided outside of the state where the investigation or proceeding is authorized and that is lawful in the state in which such health care is provided; (ii) is protected, required or authorized by federal law, regardless of the state in which such health care is provided; or (iii) is provided in the state in which the investigation or proceeding is authorized and that is permitted by the law of that state, and where such health care is lawful under the circumstances in which it is provided; or
- the identification of any person for the purpose of initiating such investigations or proceedings.

Such use and disclosure would be prohibited even with the applicable patient's authorization. Other than in relation to the above proposed prohibitions, regulated entities would still be permitted to use and disclose PHI as permitted by HIPAA. For example, if a regulated entity determines that reproductive health care was provided in a state where it was unlawful to do so and under circumstances in which federal law does not protect the provision of such health care, a regulated entity would be allowed to use or disclose PHI for a criminal, civil or administrative

[4] See Notice of Proposed Rulemaking.

[5] 142 S. Ct. 2228 (2022).

[6] See Executive Order 14076.

investigation against a provider that delivered such care.

Written Attestations

If the proposed changes were implemented as written, prior to any use or disclosure of PHI related to reproductive health care for health oversight activities, judicial and administrative proceedings, law enforcement purposes or to coroners and medical examiners, regulated entities would have to obtain a written and signed attestation from the requestor that the use or disclosure of PHI was not for a prohibited purpose. An attestation would not be required when the person making the request does not seek PHI potentially related to reproductive health care.

HHS is expected to provide a model attestation form for guidance, though regulated entities would not be required to use it so long as the attestation requires the requestor of the disclosure to (i) confirm the types of PHI that they are requesting; (ii) clearly identify the name of the individual whose PHI is being requested, if practicable, or, if not practicable, the class of individuals whose PHI is being requested; and (iii) confirm, in writing, that the use or disclosure is not for a prohibited purpose.

Regulated entities also would need to update their Notices of Privacy Practices to include information on the prohibited uses and disclosures, as well as information related to the attestation requirement.

Proposed and Revised Defined Terms

The NPRM further proposes to add or revise certain key definitions and terms. For example, "reproductive health care" would be added as a subcategory of the existing term "health care" and defined broadly to include, but not be limited to, prenatal care, abortion, infertility treatment, contraception use and treatment for reproductive-related conditions, such as ovarian cancer. Such term would apply broadly to most regulated entities, not just those providing reproductive health care, and over-the-counter medications or supplies purchased in connection with an individual's reproductive health.

Additionally, the NPRM proposes to clarify the definition of the term "person" to align with other definitions of "person" used under federal regulations,[7] such that it expressly includes a "natural person." Such term would not include a fertilized egg, embryo or fetus in its definition.

Key Takeaways

Regulated entities should carefully review these proposed changes, which, if implemented, would impose additional requirements. For example, such entities would have to review requests for disclosure of PHI related to reproductive health and determine whether the reproductive health care was provided under circumstances in which it was lawful to do so. We will monitor for further developments in this area.

Return to Table of Contents

FDA Issues Guidance to Health Care Industry and Agency Staff on Medical Device Cybersecurity

The Food and Drug Administration (FDA) published guidance on a modernized framework for cybersecurity applicable to applicants for certain medical devices.

On March 30, 2023, the FDA released its guidance titled "Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act" to address cybersecurity risks in certain medical devices prior to such devices' approval for use.[8] The guidance is being implemented without prior public comment and applies to applications or submissions submitted to the FDA after March 29, 2023.

Background

On December 29, 2022, the Consolidated Appropriations Act, 2023 (omnibus) was signed into law, which amended the Federal Food, Drug, and Cosmetics Act (FD&C Act) to include Section 524B, "Ensuring Cybersecurity of Devices,"[9] which outlines cybersecurity requirements for certain medical devices, and required the FDA to update its preexisting guidance on the matter to address these new requirements. Per the terms of the omnibus, the amendment went into effect on March 29, 2023. The FDA released its March guidance to clarify its policy on Refuse to Accept (RTA) decisions based on deficient cybersecurity documentation for premarket submissions submitted for cyber devices.

The Details of the Guidance

Scope of Applicability

The guidance is applicable to any medical device that (i) includes software validated, installed or authorized by the sponsor as a device or in a device; (ii) has the ability to connect to the internet; and (iii) contains any technological characteristic validated,

[7] "'Person' … shall include every infant member of the species homo sapiens who is born alive at any stage of development." 1 U.S.C. 8,

[8] The guidance is available here.

[9] The text of the omnibus that addresses the FD&C Act is available here at Section 3305.

installed or authorized by the sponsor that could be vulnerable to cybersecurity threats (cyber device). Sponsors of cyber devices that require premarket submission to the FDA will have to meet the information requirements under the guidance to avoid an RTA decision.

The guidance describes four key requirements to be included with premarket submissions for cyber devices:

- **Monitoring Plan.** Cyber device sponsors must submit to the secretary of the HHS (secretary) a plan to monitor, identify and address post-market cybersecurity vulnerabilities. The guidance does not specify minimum implementation requirements for such monitoring plans.
- **Post-Market Update Process.** Sponsors also must design, develop and maintain processes and procedures to provide a reasonable assurance that the device and related systems are secure. This includes making post-market updates and patches to the device and related systems available to address, (i) on a reasonably justified regular cycle, known unacceptable vulnerabilities; and (ii) as soon as possible (out of cycle), critical vulnerabilities that could cause uncontrolled risks. The guidance does not give a definition for, nor any examples for what qualifies as, known unacceptable vulnerabilities and critical vulnerabilities that could cause uncontrolled risks.
- **Software Bill of Materials.** Sponsors also must submit, as part of the premarket submission, to the secretary, a software bill of materials, including commercial, open-source and off-the-shelf software components.
- **Stay Current on Changing Requirements.** Sponsors also must comply with any other requirements that the secretary may require through regulation.

Timing

Although the guidance applies to applications and submissions submitted after March 29, 2023, the FDA indicated that it does not intend to issue RTA decisions solely based on information required by Section 524B of the FD&C Act for premarket submissions submitted before October 1, 2023. Until then, the FDA intends to collaborate with such sponsors as part of the review process. Beginning October 1, 2023, the FDA expects sponsors of cyber devices will have had sufficient time to prepare such premarket submissions with the required information, and may RTA premarket submissions that contain any such deficiencies.

Key Takeaways

Medical device sponsors whose devices may qualify as cyber devices should review the guidance to understand they types of information they must include with premarket submissions. In addition, such sponsors also should begin to develop the practices described in the required documentation and monitor for any further guidance from the FDA, including any updates to preexisting guidance, regarding best practices or new requirements as issued by the HHS secretary.

Return to Table of Contents

Privacy & Cybersecurity Update

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Avia M. Dunn
Partner / Washington, D.C.
202.371.7174
avia.dunn@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Maya P. Florence
Partner / Boston
617.573.4805
maya.florence@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Nicole L. Grimm
Counsel / Washington, D.C.
202.371.7834
nicole.grimm@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000