Articles + Publications | July 10, 2025

Virginia's Protection of Reproductive Health Information Law – Part Two, Compliance and Implementation

WRITTEN BY

Brent T. Hoard | Brianna L. Dally | David J. Navetta

In Part Two of this FAQ series, we continue to break down Virginia's Senate Bill 754, Consumer Protection Act; prohibited practices, etc., reproductive or sexual health information (Act), which amends the Virginia Consumer Protection Act (VCPA). The law went into effect on July 1, 2025.

In this installment we're asking and answering questions concerning the specific requirements of the Act and operationalizing compliance, including FAQs related to consent, disclosures, and exceptions.

If you missed Part One of our FAQ discussing the scope, applicability, and fines and penalties available to the Virginia attorney general (AG) and private litigants, click here.

WHAT DOES THE ACT MANDATE?

At a high level, the obligations of the Act are straightforward. It prohibits persons from "[o]btaining, disclosing, selling, or disseminating any personally identifiable reproductive or sexual health information without the consent of the consumer." Unfortunately, the Act's lack of caveats, exceptions, and nuance make compliance an involved endeavor.

HOW BROAD ARE THE ACT'S PROHIBITIONS?

The Act does not define "[o]btaining," "disclosing," "selling," or "disseminating" personally identifiable reproductive or sexual health information (RHSI). Nor are these terms defined in the Virginia Consumer Protection Act (VCPA), of which the Act is part. Finally, only the word "sale" is defined under Virginia's Consumer Data Protection Act (VCDPA). Sales under the VCDPA include the exchange of personal data for monetary consideration, which is arguably consistent with the term's plain meaning. Otherwise, the VCDPA utilizes the term "process," which is broader than the Act's operative terms.

Therefore, under Virginia law, these terms must be interpreted according to their "plain meaning" (see this article for more information on the plain meaning and ordinary meaning standards under Virginia law). As such, a good starting point to glean their meaning is Webster's Dictionary: obtain; disclose; and disseminate.

WHAT ARE SOME EXAMPLES OF ORGANIZATIONS AND ACTIVITIES REGULATED BY THE ACT?

Examples of real-world activities that could require consent include:

- An app that collects information about a user's menstrual cycles.
- A retailer that sells purchase history of purchasers of contraceptives or feminine products.
- A manufacturer of pregnancy or ovulation tests that has access to consumer sales data.
- An advertising technology company that tracks online purchases of feminine products to serve targeted ads for similar products.

Our take: Given the broad definitions used in the Act, the law likely regulates organizations that are not traditional health care companies, and goes beyond traditional health information, as demonstrated by the examples above.

UNDER THE VCDPA (AND SIMILAR U.S. STATE PRIVACY LAWS) "PROCESSORS" OF PERSONAL INFORMATION AND "SERVICE PROVIDERS" TYPICALLY ARE NOT REQUIRED TO OBTAIN CONSENT FOR THE COLLECTION OR DISCLOSURE OF PERSONAL DATA. DOES THE ACT LIMIT PROCESSORS' OBLIGATIONS IN A SIMILAR WAY?

No, the Act does not differentiate between "controllers" and "processors," which means that vendors processing RHSI on behalf of other organizations are directly subject to the Act and must get consent if they obtain, disclose, sell, or disseminate RHSI.

Our take: Imposing consent requirements on downstream processors who are only obtaining or disclosing personal data on behalf of their controller customers is a significant departure from existing U.S. privacy laws, which largely shield processors from having to provide notice, obtain consents, and otherwise comply with key components of these laws.

HOW CAN ORGANIZATIONS GET CONSENT FROM CONSUMERS IF THEY OBTAIN RHSI FROM THIRD PARTIES (WITHOUT HAVING A DIRECT RELATIONSHIP OR INTERFACE WITH CONSUMERS)?

It's a good question. B2B2C service providers, data brokers, organizations with video cameras, buyers of data, various entities in the AdTech ecosystem, hosting companies, and similar organizations will need to determine whether and how to obtain consent. While this isn't necessarily a new problem (*e.g.*, the CCPA requires businesses to provide consumers with a privacy notice "at or before the point" of collecting personal information), given the Act's private right of action, downstream RHSI collectors could face much more risk than under current U.S. privacy laws.

However, there may be ways to reduce this risk. The Act does not require a particular entity to get consent from a consumer prior to obtaining their RHSI. Rather, it indicates that a person cannot obtain or disclose RHSI "without consent" — ostensibly a data controller (or other party) with a direct consumer relationship could get consent for downstream parties to obtain and disclose RHSI. Unfortunately, this method requires controllers to act appropriately, and in many cases,fourth, fifth, and other downstream parties will have no knowledge or relationship with the upstream controllers (and no visibility as to whether any consent was obtained).

Assuming they have appropriate contact information, organizations could also get consent by sending an email or

other communication to consumers before obtaining, disclosing, or disseminating their RHSI. In other contexts, organizations have become accustomed to providing notice or obtaining consent after the fact (*e.g.,* after obtaining personal information). However, none of this seems practical or realistic in our current data processing environment.

Our take: Ultimately, employing a strict reading of the consent requirement could effectively make all downstream RHSI collection and disclosure illegal and subject to statutory damages.

WHAT CONSTITUTES VALID CONSENT UNDER THE ACT?

The Act borrows the VCDPA's definition and explanation of "consent":

"Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

There is a lot going on in this definition, so let's break it down.

WHAT KIND OF ACT SATISFIES THE "CLEAR AFFIRMATIVE ACT" REQUIREMENT FOR CONSENT?

Again, the concept affirmative consent (or similar terms) has been used for some time. Not surprisingly, what it means will often depend on the circumstances at hand, how broadly or narrowly an affirmative act is construed, and the risk tolerance of persons subject to the requirement. Ultimately, affirmative consent is on a spectrum. While the Act does not provide examples of affirmative consent, a common method includes requiring a consumers to check boxes or click buttons acknowledging their agreement. On the other end of the spectrum is "consent" obtained by default — regulators would argue that simply linking to a privacy policy indicating that continued use is consent is not "affirmative." For example, the Federal Trade Commission (FTC) takes the position that hovering over, muting, pausing, or closing a given piece of content does not constitute express affirmative consent.

WHAT DOES IT MEAN FOR CONSENT TO BE "FREELY GIVEN"?

For consent to be "freely given," the consent must be voluntary and informed. It must be given without coercion (*e.g.*, service denial without consent), manipulation (*e.g.*, dark patterns), or deception (*e.g.*, misrepresenting data collection and use). In other words, the consent reflects a genuine choice made by the individual.

WHAT IS "SPECIFIC" AND "INFORMED" CONSENT?

These concepts are related when it comes to consent:

- Specific means that the consent relates to a specific action or context. In practice, the consent is narrow in scope to a particular processing activity and is not bundled with other unrelated purposes or tied to vague or overbroad terms.

- Informed means that the individual receives adequate notice that the individual can understand and digest. The

consent indicates the purpose of the processing, the scope of the data to be processed, and the parties involved so the individual is able to determine whether to provide consent.

DOES THE ACT INCLUDE AN EXCEPTION FOR "NECESSARY DISCLOSURES" (*I.E.*, NECESSARY TO PROVIDE THE GOOD OR SERVICE)?

No. Unlike Washington's My Health My Data Act, opt-in consent is required even if the data processing is necessary to deliver the product or service requested by the consumer. Without a "necessary processing" exception, prior consent is required for any disclosure of RHSI. For example, prior consent would be required to disclose customer information to a fulfillment service provider to complete an order for contraceptives.

WHAT OPERATIONAL STEPS SHOULD WE TAKE TO COMPLY WITH THE ACT?

Consider the following six steps to help your organization comply with the Act:

Step 1 – Assess applicability. Review operations and data that you process to determine if you are a "supplier" that is subject to the Act.

Step 2 – Understand your data and data flows. Identify any RHSI you collect and what you receive. Understand how that information is collected, where it is maintained, and how it is processed and disclosed. Consider whether any exceptions apply to the data.

Step 3 – Implement and update consent mechanisms. Develop a form and process to obtain affirmative, informed consent from consumers. Use the data flow analysis in Step 2 to deploy your consent mechanism at relevant collection points.

Step 4 – Update privacy policies and agreements. Update privacy policies with appropriate disclosures about collection, use, and sharing of RHSI. Review contracts with relevant data sources and downstream service providers to update as needed to ensure appropriate contractual obligations and safeguards.

Step 5 – Update SDLC process for relevant data. Update your existing SDLC process to identify technologies that could collect in-scope data.

Step 6 – Train relevant members of the workforce. Ensure that members of the workforce and business are aware of the requirements, restrictions, and processes that apply to processing of RHSI.

CONCLUSION

As you can see from the FAQs above, the Act has a wide application, as it includes entities that are subject to the VCPA and does not require that an entity meet data processing threshold of the VCDPA. Additionally, it may apply to businesses with business practices that are not associated with reproductive or sexual health information. The Act also provides for a right of private action, which allows consumers to sue businesses who violate the Act. As such, organizations should carefully analyze whether and how the law may impact them and implement operational processes and mechanisms to comply with the Act's requirements.

If you have questions about the Act, or if you would like assistance with your approach to compliance, please contact Dave Navetta dave.navetta@troutman.com or Brent Hoard at brent.hoard@troutman.com for more information.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber