Thomson Reuters™

Geofencing Laws: Protecting Reproductive Health Data in a Shifting Landscape

by Andrea Frey, Stephen Phillips, and Sheryl Xavier, Hooper, Lundy & Bookman, P.C., with Practical Law Data Privacy & Cybersecurity

Status: **Law stated as of 14 May 2025** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **content.next.westlaw.com/w-045-6594**
Request a free trial and demonstration at: **tr.com/practicallaw-home**

An Article that examines the evolving legal landscape surrounding geofencing technology and its implications for consumer health data privacy in the post-*Dobbs* era as states have enacted varying laws affecting reproductive health care access and data protection. This Article explores geofencing technology's ability to track individuals' locations and its use by third parties and law enforcement. It discusses geofencing warrants that law enforcement use to gather location data from devices within specific areas and the constitutional challenges they pose under the Fourth Amendment. It also reviews state efforts to regulate the use of geofencing warrants and geofencing technology and protect consumer health data, including reproductive health information. The Article underscores the tension between states limiting abortion access and those safeguarding it, and potential federal-state conflicts over reproductive health data privacy. As geofencing technology continues to impact privacy rights, legal professionals and stakeholders must stay informed on emerging laws and judicial interpretations.

In the aftermath of the Supreme Court's 2022 decision in *Dobbs v. Jackson Women's Health Organization*, 142 S. Ct. 2228 (2022), which overturned *Roe v. Wade*, 410 U.S. 113 (1973) and *Planned Parenthood of Southeastern Pennsylvania v. Casey*, 505 U.S. 833 (1992), certain states have limited individuals' access to abortion, contraceptive methods, and gender-affirming care, while over a dozen others have strengthened or expanded individual reproductive health care rights. Although many of these laws focus on access to abortion and gender-affirming care services, others more broadly safeguard individually identifiable health data, including reproductive health data, from use by law enforcement or third-party companies.

In 2024, to address growing concerns over the safety of health data, the U.S. Department of Health and Human Services expanded the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule to prohibit covered entities from using or disclosing protected health information related to reproductive health care if the information is sought to incriminate or impose liability on a person seeking or providing lawful reproductive health care (89 Fed. Reg. 32976 (Apr. 26, 2024) (HIPAA Reproductive Health Rule); see US Dept. of Health and Human Services: HIPAA and Reproductive Health and Practice Note, HIPAA Privacy Rule: Reproductive Health Care).

Even with the previous administration's attempts to safeguard protected health information, new state laws aimed at curbing the use, sale, or other disclosure of individually identifiable health data reflect growing concerns that existing federal privacy regulations fail to adequately protect this data, particularly reproductive health data, from third-party access and criminal investigation.

A notable area of concern is the use of data obtained through geofencing, which enables enforcement agencies and third parties to track individuals' precise

physical locations. This Article explores how third parties and law enforcement can use geolocation data to access an individual's health data, particularly reproductive health data, to target patients and providers, and state actions responding to the increased use of this technology.

Geofencing Technology

Geofencing uses technologies like global positioning systems (GPS), WiFi, cellular data, and radio frequency identification (RFID) to create virtual perimeters around geographic locations. Individuals who enter the perimeter have their location registered within the perimeter and stored as data. Although geolocation data is often linked to a unique advertising ID rather than a person's name (pseudonymized), data brokers can purchase this location data in bulk and use or disclose it to law enforcement agencies, political groups, and advertising companies. These third-party recipients may be able to use location data or combine it with other data they access to identify and disclose individuals' locations without their knowledge or consent.

Geofencing has a wide range of practical applications. Retailers can leverage geofencing technology to track movement around their physical stores, so they can better understand their customer's behavior or deliver location-based advertisements. Combining geofencing with cross-device tracking also allows companies to:

- Deliver behavioral advertising as people move around a store or to a specific location.
- Assess a specific advertising channel's likelihood of success, such as an electronic message, by tracking a recipient's actual purchase behavior.

Law enforcement can also use data collected through geofencing to investigate and prosecute alleged criminal activity by determining individuals' locations at specific times, among other purposes (see Geofencing Warrants).

Impact on Consumer Health Data

Generally, HIPAA prohibits covered entities and business associates from using or disclosing protected health information, defined as individually identifiable health information created, received, or disclosed by covered entities and business associates, without either a permitted purpose, such as treatment or payment, or individual consent. HIPAA protections, however, do not extend to individually identifiable health information created, received, or disclosed by non-HIPAA regulated entities, such as mobile apps or software vendors receiving this information directly from individuals. Some examples include:

- Fitness trackers and wearable devices like Apple Watches, Fitbits, and Garmin trackers that collect data on physical activity, sleep patterns, heart rate, menstrual cycles, and other health metrics. This data can be synced with mobile apps that share it with third parties.
- Mobile health apps like MyFitnessPal and Headspace that collect data on diet, exercise, and mental health and use it to provide recommendations, track progress, and offer other services.
- Social media and online forums on sites like Facebook and Reddit that collect data on user discussions, health concerns, and personal experiences to identify trends and offer targeted advertising.
- Wearable sensors and devices like smart scales, blood pressure monitors, and blood sugar trackers that collect data on vital signs and health metrics.

Many of these apps use precise location data to function, and despite the sensitivity of the personal data that many of these apps collect, many states do not prohibit businesses from freely using, sharing, and selling consumer health and location data. On a federal level, the Federal Trade Commission (FTC) has provided guidance for mobile health app developers (see FTC: Mobile Health App Developers: FTC Best Practices and Mobile Health App Interactive Tool) and brought enforcement actions alleging unfair and deceptive trade practices against companies collecting, using, selling, and sharing sensitive geolocation data without consumer consent (see Practice Note, Tracking Technologies: Privacy and Data Security Issues: Sensitive Geolocation and Web Browsing Data).

Geofencing data can expose individuals to targeted advertisements, harassment, and criminal prosecution in states where abortion or gender-affirming care is illegal. For example, the Massachusetts Attorney General's office opened an investigation against digital advertising company Copley Advertising, alleging it violated Massachusetts' Consumer

Protection Act by using geofencing technology to tag the smartphones of women entering reproductive health clinics without their consent, and then sending anti-abortion advertisements to the tagged devices for its anti-abortion activist client. The Massachusetts AG was concerned that the practice unfairly interfered with a consumer's right to privacy in their medical decisions and conditions and may result in the collection or disclosure of individually identifiable health information without the consumer's knowledge or consent.

Copley settled the allegations in April 2017 by agreeing not to use geofencing technology at or near any Massachusetts health care facility to draw inferences about an individual's health state, medical condition, or medical treatment. For more on Copley's settlement, see Massachusetts Office of the Attorney General: AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities and Legal Update, Massachusetts AG Settles Geofencing Case with Copley Advertising.

Geofencing Warrants

Geofencing warrants enable law enforcement to collect location data from devices present in a specific geographic area during a particular timeframe. Law enforcement can use this data, for example, to:

- Identify devices present at a location where a crime occurred to find potential suspects and witnesses.
- Connect multiple crime scenes by finding common devices present at each location.
- Determine devices present during large events, riots, or public disturbances.
- Fact-check suspect and witness statements.
- Investigate missing persons cases.
- Enforce restraining orders.

Geofence warrants typically request a technology company, such as Google or Apple, to search their location history database, disclose anonymized information about devices present at a specific location and time, and then de-anonymize information about certain accounts that law enforcement identifies. Unlike regular warrants, which usually identify specific suspects, geofence warrants can be extremely broad and capture data about an unlimited number of individuals.

In states where abortion or other types of health care services are considered crimes, law enforcement may use geofence warrants to determine location history data from devices to investigate whether an individual sought, received, or assisted with abortion or other illegal health care services. For example, a geofence around a medical building or reproductive health clinic could reveal that an individual was present there during operating hours and for a certain duration, along with an accompanying family member or friend.

Fourth Amendment Issues

Geofencing warrants raise privacy concerns and constitutional issues around the Fourth Amendment's limits on unreasonable searches and seizures. In 2024, the Fourth and Fifth Circuit Courts of Appeals delivered opposing rulings on the constitutionality of geofence warrants that ordered Google to disclose information about devices present at the scene of a robbery. In *United States v. Smith*, the Fifth Circuit found that defendants had a reasonable expectation of privacy in geofence location data from their cell phones and that geofence warrants are "general warrants" that the Fourth Amendment categorically prohibits (110 F.4th 817 (5th Cir. 2024)).

Conversely, the Fourth Circuit in *United States v. Chatrie* held that since the defendant had voluntarily exposed his location information to Google by affirmatively selecting the optional location history setting and thus did not have a reasonable expectation of privacy in the mobile device location history data (107 F.4th 319 (4th Cir. 2024)). The court re-heard *Chatrie en banc* and affirmed the district court's judgment, with seven concurring opinions and one dissenting opinion (*US v. Chatrie*, 2025 WL 1242063 (4th Cir. April 30, 2025)). For more detail on these cases and an 11th Circuit decision in another geofencing warrant case, see Westlaw Today: 5th Circuit rules that geofence warrants are unconstitutional, creates circuit split and Fractured 4th Circuit affirms judgment in geofence warrant case.

Google has since updated its location history service (called Timeline) in response to excess law enforcement requests. The company now stores users' location history directly on their devices instead of on its servers and allows users more

control over their settings. This will minimize the reach of geofence warrants requesting data in Google's possession and will require law enforcement to have access to the device itself. (Google Product News: Updates to Location History and new controls coming soon to Maps; Forbes: Google To Stop Giving Location Evidence To Law Enforcement.)

State Efforts to Regulate Geofencing Warrants

In 2023, Utah became the first state to pass a law codifying the process by which law enforcement can obtain reverse-location information for devices within a geofence for a criminal investigation or prosecution (Utah Code §§ 77-23f-101 to 77-23f-109). The Utah law limits law enforcement's ability to obtain this information to cases involving felonies or certain class A and B misdemeanors where law enforcement can demonstrate an imminent, ongoing threat to public safety (Utah Code § 77-23f-102(1)). The law also sets out requirements for the content of the warrant application, including:

- A map or other visual depiction of the applicable geofence.
- A specific notice with language set out in the statute that describes the scope of reverse-location warrants and the electronic devices they may capture.

(Utah Code § 77-23f-102(2).)

Law enforcement is also required to establish probable cause that it will find evidence of a crime within the geofence during a specified time period (Utah Code § 77-23f-102(2)(b)). The Utah law sets out similar requirements for obtaining reverse-location information based on cell site records (Utah Code § 77-23f-103).

Any device data provided to law enforcement under the warrant must first be anonymized (Utah Code §§ 77-23f-102(3), 77-23f-103(3). Law enforcement must then establish probable cause that a particular device was used or otherwise implicated in a crime to de-anonymize the device data (Utah Code §§ 77-23f-105). The Utah law also contains exceptions and specifies requirements for law enforcement's use, disclosure, and destruction of reverse-location information (Utah Code §§ 77-23f-106 to 77-23f-109). The Utah Defense Attorney Association considers the law to be an "improvement on current practice," though it remains opposed to the "implicit legitimization of geofence warrants" (UDAA: Issues: Privacy). The American Civil Liberties Union (ACLU) celebrated the Utah Law's enactment and was involved in the legislative efforts in both Utah and in connection with a similar bill in New York (ACLU: Celebrating An Important Victory In The Ongoing Fight Against Reverse Warrants).

For several years, the New York state legislature has considered bills that limit law enforcement searches of geolocation and keyword data for those under no individual suspicion of having committed a crime, but who happened to be at a particular location at a specific time or searched certain words, phrases, or websites. The Reverse Location and Reverse Keyword Search Prohibition Act (SB404) proposes to amend New York's criminal procedure law to address these issues and limit the scope of searches. It was introduced in the New York state senate on January 8, 2025, and is currently in committee. Given the federal caselaw that is still developing and a possible US Supreme Court opinion on the issue, other states may start to introduce similar bills to limit the scope of geofencing warrants.

State Laws Against Geofencing

In response to privacy concerns around the sensitive data that geofencing can capture, several states have enacted laws designed to protect consumers' health data from geofencing practices, with some specifically addressing reproductive health data.

Washington

Washington's My Health My Data (MHMD) Act (RCW 19.373.005 to 19.373.900) grants Washington residents various rights regarding their consumer health data and imposes new requirements on businesses that collect, process, share, and sell consumer health data. It also includes a prohibition on geofencing around an entity that provides in-person health care services (RCW 19.373.080).

The MHMD Act broadly defines consumer health data as any information linkable to a person in Washington that identifies their past, present, or future health status and explicitly includes gender-affirming care information and reproductive or sexual health information (RCW 19.373.010(8)(a)). The MHMD Act also requires all persons who seek to sell consumer

health data to obtain express written authorization from the consumer and inform the consumer of the purpose of the sale and the contact information of the purchaser (RCW 19.373.070). Selling data under the MHMD Act means exchanging consumer health data for monetary or other valuable consideration (RCW 19.373.010(26)).

The MHMD Act's geofencing prohibition applies to all persons and entities and took effect on July 23, 2023. It defines geofencing to include technology that establishes or locates a consumer within 2,000 feet from the perimeter of a specific physical location using:

- Global positioning coordinates.
- Cell tower connectivity.
- Cellular data.
- Radio frequency identification.
- WiFi data.
- Another form of spatial or location detection.

(RCW 19.373.010(14).)

The MHMD Act prohibits any person from using geofencing to:

- Identify or track consumers seeking health care services.
- Collect consumer health data.
- Send consumers health data or health-care-service-related notifications, messages, or advertisements.

(RCW 19.373.080.)

For more information on the MHMD Act, see Practice Note, Understanding the Washington My Health My Data Act and Standard Document, Consumer Health Data Privacy Policy (Washington).

Nevada

Nevada amended its trade regulations statute (NRS 598.0901to 604D.900) effective March 31, 2024 (SB 370) to protect Nevada residents and individuals whose consumer health data is collected in Nevada (NRS 603A.400 to 603A.490) (Security and Privacy of Consumer Health Data). It broadly defines consumer health data as personal information, including a persistent unique identifier, that is linked or reasonably linkable to a consumer **and** that an entity also uses to identify that consumer's past, present, or future health status. This definition explicitly includes information relating to reproductive or sexual health care and gender-affirming health care. (NRS 603A.430). The law prohibits consumer data sales without the consumer's specific written authorization and defines sales as an exchange of consumer health data for money or other valuable consideration, with certain exceptions (NRS 603A.475 and 603A.535).

Nevada's consumer health data law defines geofencing as technology that establishes a virtual boundary with a radius of 1,750 feet or less around a specific physical location using methods similar to those set out in the MHMD Act (NRS 603A.540(2)(b)).

The law prohibits geofencing around an entity that provides in-person health care services to:

- Identify or track consumers seeking health care services.
- Collect consumer health data.
- Send consumers health data or health care service-related notifications, messages, or advertisements.

(NRS 603A.540(1).)

For more information on Nevada's consumer health data law, see Legal Update, Nevada Enacts Consumer Health Data Law and Modifies Data Breach Notification Requirements for Lenders.

Connecticut

A 2023 amendment to the Connecticut Personal Data Privacy and Online Monitoring Act (Conn. Gen. Stat. Ann. §§ 42-515 to 42-525) (CTDPA) extends its application to consumer health data controllers, defined as any person or entity that determines the purpose and means of processing consumer health data, whether alone or jointly with others (Conn. Gen. Stat. Ann. § 42-515(9)). As a result, consumer health data controllers will be subject to the same statutory obligations as other data controllers and processors under the CTDPA, even if the law's jurisdictional thresholds set out under Conn. Gen. Stat. Ann. § 42-516 would otherwise exclude them (Conn. Gen. Stat. Ann. § 42-526). The CTDPA defines consumer health data as any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, including gender-affirming, reproductive, or sexual health data (Conn. Gen. Stat. Ann. § 42-515(9)).

The law defines geofencing as a technology to establish a virtual boundary using methods similar to those set out in the MHMD Act (Conn. Gen. Stat. Ann. § 42-515(19)).

The CTDPA prohibits geofencing within 1,750 feet of any mental health, reproductive, or sexual health facility to:

- Identify or track consumers.
- Collect or sell consumer health information without consent.
- Send consumers health data or healthcare service-related notifications, messages, or advertisements.

For more information on the CTDPA, see Practice Note, Connecticut Personal Data Privacy and Online Monitoring Act (CTDPA) Quick Facts: Overview and Legal Update, Connecticut Amends Consumer Privacy Law to Protect Health Data and Child Online Safety.

New York

In 2023, New York passed SB4007, which prohibits a party from geofencing around any health care facility that the party does not own (N.Y. Gen. Bus. Law. § 394-g(2)). The law defines geofencing as a technology to establish a virtual boundary of 1,850 feet or less around a particular location that allows a digital advertiser to track an individual's location and electronically deliver targeted digital advertisements directly to the individual's mobile device upon their entry into the geofenced area (N.Y. Gen. Bus. Law. § 394-g(1)(b)).

Geofencing also includes the process of identifying whether a device enters, exits, or is present within a geographic area by using any information stored, transmitted, or received by the device, including various location data technologies (N.Y. Gen. Bus. Law. § 394-g(1)(b).)

The New York law bans persons or entities from:

- Establishing a geofence around a health care facility that they do not own to electronically deliver digital advertisements to individuals who enter the geofencing perimeter, build consumer profiles, or to infer health status, medical condition, or medical treatment.
- Using acquired consumer health information to send delayed advertisements to individuals after they leave the perimeter.
- Selling the acquired consumer health information without the user's consent.

(N.Y. Gen. Bus. Law. § 394-g(2).)

California

California law prohibits a person or business from collecting, using, disclosing, or retaining the personal information of an individual physically located at, or within a precise geolocation of, a family planning center, except as necessary to fulfill the individual's request (Cal. Civ. Code § 1798.99.90). It prohibits the sale of this type of personal information or sharing it for cross-context behavioral advertising (Cal. Civ. Code § 1798.99.90(c)). The law defines precise geolocation as a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet as derived from a device that is used or intended to be used to locate a person (Cal. Civ. Code § 1798.99.90(b)(5)).

The law does not apply to providers of health care, health care service plans, or contractors as defined under the Confidentiality of Medical Information Act (Cal. Civ. Code §§ 56 to 56.37) (Cal. Civ. Code § 1798.99.90(e)).

Aggrieved individuals or entities, including family planning centers, may bring a civil action against violators for injunctive and monetary relief. Recoverable damages include three times the amount of actual damages and any other expenses, costs, or reasonable attorney's fees incurred in connection with the litigation. (Cal. Civ. Code § 1798.99.90(d).)

In December 2024, California introduced AB 45, which seeks to expand the law's scope to prohibit geofencing around an entity that provides in-person health care services. The bill was passed by the Privacy and Consumer Protection committee on April 23, 2025 and referred to the Judiciary and Appropriations committees.

For more information on California's health data privacy laws, see Practice Note, California Privacy and Data Security Law: Overview: Health Information Privacy.

Virginia

In January 2025, SB1023 was introduced to the Virginia State Senate as an amendment to the Virginia Consumer Data Protection Act (VCDPA) (Va. Code

Ann. §§ 59.1-575 to 59.1-584), which has been in effect since 2023. The VCDPA already classifies collecting precise geolocation data (data that directly identifies a person's specific location within a radius of 1,750 feet) as sensitive data and generally prohibits data controllers from collecting it from a known child (Va. Code Ann. §§ 59.1-575 and 59.1-578(F)(1)-(2)). SB1023 sought to amend the VCDPA's data controller obligations section to include a prohibition on selling or offering for sale precise geolocation data concerning a consumer (proposed Va. Code Ann. §59.1-578(A)(6)). The bill passed the Virginia State Senate on February 4, 2025 but was removed from consideration by the House. For more information on the VCDPA, see Practice Notes, Understanding the Virginia Consumer Data Protection Act (VCDPA) and Virginia Consumer Data Protection Act (VCDPA) Quick Facts: Overview.

Looking Ahead

By restricting or prohibiting access to reproductive health data via geofencing, states seeking to protect individuals' access to abortion and other health care services have created robust privacy protections for reproductive health data. The tension, however, between states continuing to limit abortion access and those protecting such access, as well as between states' decisions to criminalize or protect access to gender-affirming care, may well result in legal conflicts requiring judicial intervention.

For example, in early 2025 a New York doctor was indicted by a grand jury in Louisiana, where abortion is banned, for prescribing an abortion pill to a pregnant teenager living in Louisiana. The teen's mother was also criminally charged for giving her the abortion pills. (Reuters: New York doctor indicted in Louisiana for prescribing abortion pill taken by teen.) New York Governor Kathy Hochul then signed a bill to shield the identity of doctors who provide abortion services to patients in other states; New York is one of eight states to enact a telemedicine abortion shield law. Governor Hochul also strongly rebuked and refused to sign a Louisiana extradition order for the indicted doctor (AB A2145A; New York State: Governor Hochul Makes a Reproductive Freedom Announcement). A New York county clerk also refused to enforce a $100,000 Texas civil judgment against the same doctor for allegedly sending abortion pills to patients in Texas, which also bans abortion (Reuters: NY official rejects Texas judgment against doctor in abortion pill case). These cases highlight the deep political divide that exists among the states over abortion and at least one of these cases is expected to make its way to the US Supreme Court.

Potential conflict between states and the federal government, depending on actions taken by Congress and the Trump administration on these topics, could also raise specific questions about federal preemption and state rights over data privacy. Upon taking office, the second Trump administration took steps to overturn most of the Biden administration's reproductive health policies.

President Trump issued an Executive Order on January 24, 2025, that revoked:

- Biden's Executive Order 14,076, which had directed federal agencies to take steps to protect access to reproductive health care and promote the safety and security of patients, providers, and clinics.
- Biden's Executive Order 14,079, which defined reproductive health care services and instructed the Department of Health and Human Services (HHS) to use Medicaid to advance access to reproductive health care services, including for individuals traveling across state lines for medical care.

(Exec. Order No. 14,182, 90 Fed. Reg. 8751 (Jan. 24, 2025).)

HHS announced that, in accordance with the Office of Management and Budget's January 27, 2025 memorandum "Temporary Pause of Agency Grant, Loan, and Other Financial Assistance Programs," the department will reevaluate all programs, regulations, and guidance to ensure that federal funds are not used "to pay for or promote elective abortion" (HHS: Statement from Dr. Dorothy Fink, Acting Secretary of the U.S. Department of Health and Human Services (Jan. 27, 2025)).

With a second Trump administration and conservative majorities in Congress and on the Supreme Court, it is unclear whether federal efforts seeking to address health data privacy concerns will remain in effect. Though the HHS final regulations amending the HIPAA Privacy Rule regarding reproductive health care privacy took effect in December 2024, the Trump administration may attempt to reverse these protections or simply refuse to enforce them (89 Fed. Reg. 32976 (Apr. 26, 2024)). Given the controversial nature of these regulations, which 17 state attorneys general challenged, it is possible that the final

regulations may be the subject of a post-*Chevron* challenge (in June 2024, the Supreme Court overruled its 40-year-old *Chevron* decision, which had required reviewing courts to defer to agency interpretations of ambiguous statutes that Congress authorized the agency to administer (known as *Chevron* deference) (*Loper Bright Enters. v. Raimondo*, 2024 WL 3208360 (June 28, 2024); see Legal Update, Supreme Court Overrules Chevron Framework for Interpreting Laws Administered by Federal Agencies)).

Federal courts are already hearing challenges to HIPAA's reproductive health data protections. In states that criminalize abortion, for example, plaintiffs allege that the HIPAA Reproductive Health Rule's prohibition on the disclosure of protected health information interferes with states' statutory authority to investigate potentially criminal behavior (see, for example, Compl., *Texas v. U.S. Dep't of Health & Hum. Servs.*, No. 5:24-cv-00204-H (N.D. Tex. Sept. 4, 2024); Compl., *Purl et al. v. U.S. Dep't of Health & Hum. Servs.*, No. 2:24-cv-00228-Z (N.D. Tex. Oct. 21, 2024); Compl., *Tennessee et al. v. U.S. Dep't of Health & Hum. Servs.*, No. 3:25-cv-00025 (E.D. Tenn. Jan. 17, 2025)). Although HIPAA traditionally permits covered entities to disclose PHI at their discretion in law enforcement and other legal proceedings, plaintiffs assert that the Reproductive Health Rule permits covered entities to withhold information pertinent to state investigations. If plaintiffs prevail, HIPAA-covered entities could be obligated to comply with state laws requiring disclosure of reproductive health-related PHI. For more information on these challenges, see Practice Note, HIPAA Privacy Rule: Reproductive Health Care: Litigation Involving 2024 Regulations.

As state lawmakers continue to scrutinize areas of concern around reproductive health privacy, including the impact of geofencing on the privacy of reproductive and other health care data, data privacy laws and their implications for reproductive and other health care services will likely remain an area of intense legal and political debate. Organizations in the health care space and those that collect and process consumer health data must closely monitor developing federal and state laws, regulations, enforcement, guidance, and judicial decisions around:

- Geofencing prohibitions and warrants.
- Reproductive health care privacy.
- Abortion services and medication.
- Consumer health data privacy.

For help tracking these topics, see:

- Practice Note, Health Care Provider Considerations for Reproductive Health Care Services Post-Roe
- State Consumer Privacy Legislation Tracker
- Quick Compare Chart, State Abortion Laws
- 2025 Trump Administration Transition Toolkit: The First 100 Days
- Abortion and Contraceptives Services for Group Health Plans Toolkit: Abortion-Related Legal Updates Involving Dobbs Ruling
- HIPAA and Health Information Privacy Compliance Toolkit: Legal Updates
- Trump Administration Toolkit