KRISTEN POLI SECURITY AUG 21, 2023 8:00 AM

The Most Popular Digital Abortion Clinics, Ranked by Data Privacy

Telehealth companies that provide abortion pills are surging in popularity. Which are as safe as they claim to be?

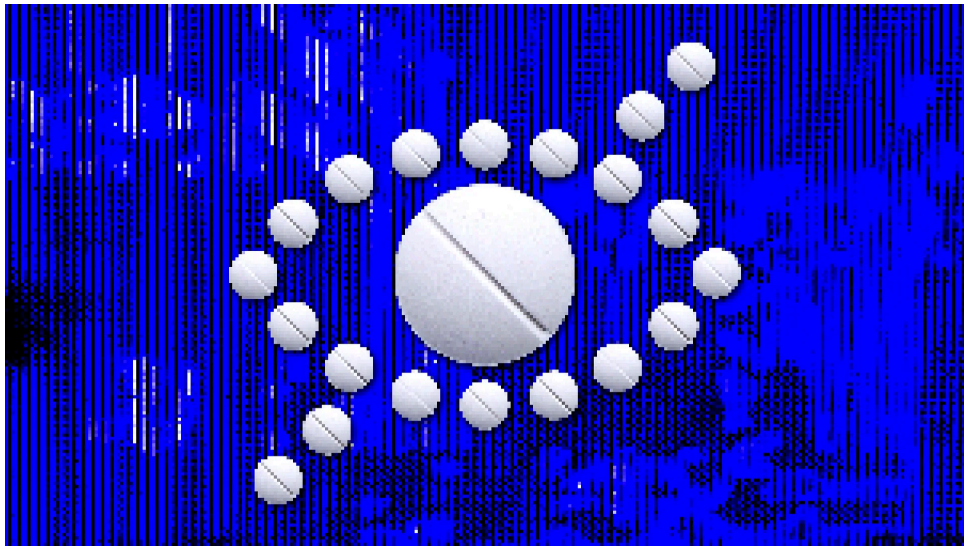

ILLUSTRATION: JACQUI VANLIEW; GETTY IMAGES

SAVE

If you buy something using links in our stories, we may earn a commission. Learn more.

A NEW CLASS of health care startups has emerged in response to the US Supreme Court's decision to overturn the federal right to abortion last year. These "digital abortion clinics" connect patients with health care providers who are able to prescribe mifepristone and misoprostol, a course of care commonly described as the "abortion pill."

These services, many of which were founded before *Dobbs v. Jackson*, are poised to eliminate a major paradox in the field of reproductive health: Medication abortion is currently the most common way to terminate a pregnancy, yet only 1 in 4 adults are familiar with it, according to a recent study by KFF.

These clinics operate in different ways—some provide live video visits with doctors and nurse practitioners, while others offer asynchronous counseling—but many have experienced a record number of patient orders (and increased VC funding) over the past year. According to Elisa Wells, cofounder of the nonprofit Plan C, their appeal is straightforward. "Their pricing is quite affordable, and there's convenience in placing an order and getting pills delivered to your mailbox in three to four days," she says.

Recent data suggests that telehealth clinics have been effective in expanding access to abortion care, especially for people living in remote areas or in states where the procedure has been criminalized, a finding that Wells' team corroborates. Thanks to a new series of "shield laws" protecting clinicians from out-of-state prosecution—passed in 12 states, including New York, Maryland, and Illinois—these clinics are positioned to expand their reach even further.

Following the lead of other companies in the femtech space (a category that includes everything from kegel trainers to period-tracking apps), leaders at digital abortion clinics like Hey Jane and Choix have publicly expressed their commitment to users' privacy as they grow. In a recent interview with *Vogue*, Hey Jane cofounder Kiki Freedman said that the service is "HIPAA-compliant and encrypted." In an interview with *Ms.* magazine this January, a representative from Choix highlighted its "HIPAA-compliant texting platform," while another interviewee suggested that "most telehealth providers are not checking IP addresses." (Read more about how HIPAA actually works here.)

A common belief about virtual clinics is that they offer more discretion than their brick-and-mortar counterparts. "There's definitely a privacy factor—these sites don't ask a lot of questions," says Wells. In a 2020 study of over 6,000 abortion seekers, 39 percent reported choosing a telemedicine option specifically to preserve their privacy. While some providers' intentions seem genuine, privacy experts have pointed out that their services may not be as secure as users expect them to be (even if they are compliant with US law).

Last July, a team of researchers at the Markup reported that Hey Jane's site passed along user information to Meta and Google, the world's largest digital advertisers. While providers may not restrict access via IP addresses, our analysis found that most providers readily collected them. For telehealth abortion clinics, HIPAA compliance is just one part of the puzzle.
So which virtual abortion clinics take users' privacy seriously, and which do not? How can users approach these services with safety in mind? Does HIPAA protect all information sent to telehealth providers? To find out, we teamed up with experts to analyze the privacy policies of five popular abortion-by-mail providers: Wisp, Choix, Hey Jane, Carafem, and Aid Access.

While the American Bar Association reported in April that "high-tech tactics" (like sending court orders to femtech apps) have not been used to successfully convict abortion seekers, prosecutors have used women's text messages and search histories as evidence in a number of abortion-related cases. Because of this precedent, users should proceed with caution when handing their personal information over to telehealth providers. It's not uncommon for vulnerable data to end up in the hands of third-party brokers who compile digital profiles of users before selling their information to the highest bidder. Michele Gilman, professor of law at the University of Baltimore, says: "Reproductive health data is being sold and transported into a much larger system."

To make matters worse, the absence of a comprehensive federal privacy law, like the EU's General Data Protection Regulation (GDPR), leaves the burden of evaluating privacy policies to individual users. Considering that these policies have gotten longer and more difficult to decipher in recent years, this is a serious burden. For our evaluation, we consulted frameworks from the University of Texas at Austin's Privacy Lab and the Digital Standard to arrive at four core factors.

Here's what we found:

Data Collection (PII)

The GDPR's American cousin, the California Consumer Privacy Act (CCPA) has inspired proposed state legislation that supports greater protections for a specific category of data—personally identifiable information. While PII is broadly defined, Google interprets it as including your email address, full name, precise location, phone number, and mailing address.

The safest websites to use won't collect your PII at all, but offering a mailing address to a virtual clinic is a matter of necessity here. In this context, it's helpful to distinguish between companies that use your personal information to provide essential services and those that share this information with third parties. Austria-based nonprofit Aid Access fared the best in this category, encouraging users to access the service with virtual anonymity in its policy. Wisp fared particularly poorly here, citing its ability to send specific geolocation data to advertisers.
The majority of providers we analyzed categorize email addresses and the like as "personal information," which is only protected by HIPAA if it's stored alongside medical information. This makes it difficult to judge whether it's being used appropriately.

Low Risk: *PII is not recorded,* ***Some Risk****: PII is used for intended service,* ***High Risk:*** *PII is used by third parties*

Law Enforcement

According to bioethics expert Sharona Hoffman, there's a common misconception that HIPPA protects your medical information from being shared outside of your doctor's office. The reality, she says, is that "HIPAA isn't that protective. Consumers need to know that HIPAA has exceptions for law enforcement and public health."

While the law provides safeguards for a particular subset of information (personal health information), it doesn't cover all of the information you provide to a telehealth service. Even if it did apply, the rule *allows* (but does not *require*) health care providers to expose PHI when presented with a search warrant or other legal document. While providers could technically refuse these requests, most don't. "It's easier to comply rather than involve your medical office in litigation," says Gilman.

Aid Access is a notable exception and has a track record of standing up to law enforcement (it even sued the US Food and Drug Administration last year.) When examining privacy policies, UT's Privacy Lab recommends looking at companies' willingness to hand over any data in the absence of a warrant or other legal document. Neither Carafem, Wisp, Hey Jane, nor Choix specify that they would require a warrant before sending information to government agencies or other legal entities.

Low Risk: *PII is not recorded,* ***Some Risk:*** *Legal documents are required to comply with law enforcement,* ***High Risk:*** *Legal documents are not required to comply with law enforcement*

Data Control (Deletion)

Sites that offer users more control over their data can deliver better privacy than those that don't. While low-risk sites will allow you to delete and edit your information freely, some medical information that users provide to virtual clinics will still be out of reach. This is due to state-specific medical record retention laws, which can require health care entities to retain some records for up to 25 years.

Examining how much control companies give users over other information is a better proxy for understanding their general safety. While most of the providers we analyzed included data deletion protocols in their privacy policies, Choix and Hey Jane's do not. In addition, the latter confirms that it retains data for an unspecified ("reasonable") period of time.

While Wisp does offer a deletion protocol, it admits that requests can be refused for a variety of reasons, including "exercising free speech" and "internal and lawful uses" on behalf of itself or its affiliates. In addition to responding to requests, privacy-forward organizations will also proactively delete sensitive information, something Carafem does. However, Carafem does not specify a timeline or provide a general deletion request protocol. By contrast, Aid Access allows users to file deletion requests at will for most information.
Low Risk: *Users can edit or delete data,* ***Some Risk:*** *Users can edit data,* ***High Risk:*** *Users cannot edit or delete data*

Third-Party Sharing (Ads and Marketing)

Research scientist and privacy expert Razieh Nokhbeh Zaeem calls personally identifiable information the "currency of the internet" because of the myriad ways individualized data is collected, bought, and sold across industries. While almost all websites work with third parties in some way, telehealth companies should not sell or share your information with advertisers—but many do, as evidenced by Betterhelp's recent settlement with the Federal Trade Commission.

If a company is collecting sensitive information and using it to market products and services to you, that presents some risk. If a company shares this information with *other* companies to support *their* marketing efforts, it's a major red flag. As the Markup rightly points out in its privacy policy guide, mentions of "personalization" and "improving services" in these documents usually equate to ad tracking.

According to its privacy policy, Hey Jane uses personal data (and PII) to market its own services ("inform you about products"), while Carafem, Wisp, and Choix reserve the right to pass along information to third-party marketing partners. Choix's policy claims that it "will never sell your data for third-party marketing purpose[s]" in one section but reserves the right to disclose data to its affiliates for "marketing" purposes in another.

Rather than limiting or removing the third-party trackers installed on their sites, some providers recommend that users generally opt out of cookie-based advertising within their policies, a strategy that is far from foolproof.

Low Risk: *PII is not used for marketing or advertising,* ***Some Risk:*** *PII is used for marketing/advertising,* ***High Risk:*** *PII shared with third parties for marketing/advertising*

The Bottom Line

In a post-*Roe* America, virtual abortion clinics provide an essential service, especially for people living in states that criminalize care. Early indicators have shown that they increase access to safe and effective abortion medications, but they don't offer as much privacy as users are led to believe. With the exception of Aid Access, all of the providers we analyzed have a long way to go when it comes to protecting users' privacy and earning their trust.

To manage risk when approaching these services (and accessing other information about abortion in hostile states), educators at the Digital Defense Fund recommend reducing your footprint by using privacy-forward search engines like DuckDuckGo, creating temporary email accounts for abortion care, and turning off location tracking on all of your devices.

While engaging in defensive tactics like these are practically useful, legal scholars like Gilman suggest that the reproductive justice movement will advance only when federal and state governments no longer rely on an outdated "notice and consent" paradigm for data privacy. "We need *meaningful* consent in the reproductive health space," says Gilman. "Privacy policies today are more like adhesion contracts—suggesting that users 'take it or leave it.' It's not realistic or fair to tell people they can't engage with technology if they want to protect their privacy."

Gilman recommends advocating at the state level for better privacy standards, especially if your representatives are considering new legislation. She also encourages people to demand increased protections from private companies, many of which are more flush with the "currency of the internet" than they would have us believe.
