

# Unanswered Questions after *Dobbs* Part V: Personal Information and Privacy

Client Update  
June 28, 2022

```
#define ASM_VMX_VMREAD_RDX_RAX ".byte 0x0F, 0x77, 0x0F"
static __always_inline unsigned long vmcs_read(unsigned long vmcs_id,
        unsigned long vmcs_field)
{
    asm volatile (
        : "=r" (value) :
        : "cc" (ASM_VMX_VMREAD_RDX_RAX)
        : "memory"
    );
    return value;
}
#include <stdint.h>
int main(int argc, char *argv) {
    int64_t src = argc;
    int64_t dst;
    volatile
```

# Unanswered Questions after *Dobbs* Part V: Personal Information and Privacy

In our fifth installment of “Unanswered questions after *Dobbs*,” Reed Smith’s Reproductive Health Working Group addresses the potential impact of the *Dobbs* opinion on personal data and health information privacy. As discussed in our prior installments and in our June 13 Client Alert discussing California’s action to safeguard users’ reproductive health information with health apps, *Dobbs* will have far-reaching effects on the health care industry and on employers. This installment provides examples of questions and discusses issues that may arise for those health care providers and employers, as well as digital health technology companies and general-use, Internet-based services as individuals seeking health care interact with those services. Individuals and organizations need to navigate the already challenging web of federal and state privacy rules applicable to individual data, including personal health information regulated by the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA), and other federal and state privacy laws.

Below are some examples of questions that may arise as those stakeholders navigate this development:

## Unanswered Questions Post-*Dobbs*

### General Use Applications

- General-use applications on your phone and computer regularly track your search history and collect information about your preferences. In the context of *Dobbs*, this applies to, for example, searches for reproductive health clinics or providers, online pharmaceutical orders, and information collected by fertility-related applications (e.g., period, ovulation, and pregnancy trackers).
  - Will the developers of those applications have an obligation to provide search history, map search requests, and similar online or in-application activity to those states opting to criminalize (to varying degrees) abortion and those that aid or abet it?
  - What if an online ad for a reproductive health clinic is displayed to an individual living where the services provided by the clinic are illegal? Is the clinic, the advertising platform that facilitated the ad, and/or the website that displayed the ad potentially liable?
  - Will manufacturers of devices that incorporate patient health software and applications (e.g., watches that monitor health information) have any obligation to respond to requests from law enforcement or other third parties for reproductive or other health information about the person using their device?
  - Are any of these application developers or Internet search engines subject to HIPAA?
  - What are companies’ reporting responsibilities if they have data that indicates or suggests an individual is violating the law?

- Will state privacy laws or federal laws governing the expectation of privacy, including federal Constitutional limits, apply to protect this online activity and restrict the sharing of information?
- What right do police or other law enforcement authorities have to information that individuals willingly provide online or through applications?
- Do individuals seeking to enforce laws in states that permit individual rights of action have the ability to force disclosure of this information through civil litigation?
- Will federal or state lawmakers take action to bolster the protection of the sale or use of personal information provided online or in applications?

### **HIPAA Considerations**

- Those in the health care industry are familiar with HIPAA but may not always appreciate its nuanced application to permissive and required disclosures and safeguards that apply even when disclosure is appropriate.
  - To what extent will states utilize the “law enforcement” or similar exceptions to HIPAA to attempt to obtain information from health care providers, health plans, and other Covered Entities regarding abortions (or suspected abortions)?
  - Will Business Associates, such as electronic health records vendors and data management providers, be required or able to share protected health information under HIPAA with law enforcement?
  - Can providers or other actors take the view that seeking to have an abortion allows sharing of information under the HIPAA exceptions applicable to persons in imminent danger or other “public health” reasons?
  - Should HIPAA-covered entities and individuals reassess their policies regarding the “minimum necessary” requirement for permitted disclosures under HIPAA?
  - Relatedly, what data and information will health care providers, payors, and health information technology vendors have to share with other requestors, both in the health care industry and, with the patients consent, outside the industry, under the Office of the National Coordinator for Health Information Technology and Centers for Medicare & Medicaid Services Interoperability and Information Blocking Rules?

### **State v. Federal Laws**

- What about the states? Several states have imposed privacy laws in recent years that are stricter and broader in scope than their federal counterparts.
  - What information can a person or entity disclose if HIPAA or a federal law permits disclosure, but the laws of the state in which they operate or live do not?
  - Will states legislate to protect HIPAA-covered entities and individuals from disclosing information related to reproductive health services without consent or otherwise limiting extra-territorial judicial process for private information? (For example, see Public Act. No. 22-19 passed in Connecticut and applicable to Covered Entities.)
  - Should providers or other entities and individuals respond to letters or requests for information that are not court-issued subpoenas when the information requested is of a personal health nature, particularly requests from an out-of-state governmental body?
  - What if abortion information is made public due to a data breach? Can law enforcement and prosecutors use that information as part of enforcing criminal laws? What recourse do affected individuals have against the organization that experienced the data breach? Can affected individuals prevent the use of such information as evidence supporting criminal prosecution?
  - What rights or controls do individuals have to restrict the processing and/or disclosures of this information, which may be considered sensitive health information under applicable law?

Stay tuned for our next installment of “Unanswered questions after *Dobbs*.” Please reach out to a member of the Reed Smith Reproductive Health Working Group or the Reed Smith attorneys with whom you regularly work for more information or guidance on these or related issues. Reed Smith will continue to monitor developments and provide updates in response to the *Dobbs* opinion.

# Authors



**Nicole J. Aiken-Shaban**  
Partner  
Philadelphia  
+1 215 851 8173  
naiken-shaban@reedsmith.com



**Wendell J. Bartnick**  
Partner  
Houston  
+1 713 469 3838  
wbartnick@reedsmith.com

**Reed Smith is a dynamic international law firm, dedicated to helping clients move their businesses forward.**

Our long-standing relationships, international outlook, and collaborative structure make us the go-to partner for speedy resolution of complex disputes, transactions, and regulatory matters.



This document is not intended to provide legal advice to be used in a specific fact situation; the contents are for informational purposes only. "Reed Smith" refers to Reed Smith LLP and related entities. © Reed Smith LLP 2022

- ABU DHABI
- ATHENS
- AUSTIN
- BEIJING
- BRUSSELS
- CENTURY CITY
- CHICAGO
- DALLAS
- DUBAI
- FRANKFURT
- HONG KONG
- HOUSTON
- KAZAKHSTAN
- LONDON
- LOS ANGELES
- MIAMI
- MUNICH
- NEW YORK
- PARIS
- PHILADELPHIA
- PITTSBURGH
- PRINCETON
- RICHMOND
- SAN FRANCISCO
- SHANGHAI
- SILICON VALLEY
- SINGAPORE
- TYSONS
- WASHINGTON, D.C.
- WILMINGTON