Big Data Profits If We Deregulate HIPAA

This blog post was written by Kenny Gutierrez, EFF Bridge Fellow.

Recently proposed modifications to the federal Health Insurance Portability and Accountability Act (HIPAA) would invade your most personal and intimate health data. The Office of Civil Rights (OCR), which is part of the U.S. Department of Health and Human Services (HHS), proposes loosening our health privacy protections to address misunderstandings by health professionals about currently permissible disclosures.

EFF recently filed objections to the proposed modifications. The most troubling change would expand the sharing of your health data without your permission, by enlarging the definition of "health care operations" to include "case management" and "care coordination," which is particularly troubling since these broad terms are not defined. Additionally, the modifications seek to lower the standard of disclosure for emergencies. They also will require covered entities to disclose personal health information (PHI) to uncovered health mobile applications upon patient request. Individually, the changes are troublesome enough. When combined, the impact on the release of PHI, with and without consent, is a threat to patient health and privacy.

Trust in Healthcare is Crucial

The proposed modifications would undermine the requisite trust by patients for health professionals to disclose their sensitive and intimate medical information. If patients no longer feel their doctors will protect their PHI, they will not disclose it or even seek treatment. For example,

since there is pervasive prejudice and stigma surrounding addiction, an opiate- dependent patient will probably be less likely to seek treatment, or fully disclose the severity of their condition, if they fear their diagnosis could be shared without their consent. Consequently, the HHS proposal will hinder care coordination and case management. That would increase the cost of healthcare, because of decreased preventative care in the short-term, and increased treatment in the long-term, which is significantly more expensive. Untreated mental illness costs the nation more than $100 billion annually. Currently, only 2.5 million of the 21.2 million people suffering from mental illness seek treatment.

The current HIPAA privacy rule is flexible enough, counter to the misguided assertions of some health care professionals. It protects patient privacy while allowing disclosure, without patient consent, in critical instances such as for treatment, in an emergency, and when a patient is a threat to themselves or public safety.

So, why does HHS seek to modify an already flexible rule? Two congressional hearings, in 2013 and 2015, revealed that there is significant misunderstanding of HIPAA and permissive disclosures amongst medical professionals. As a result, HIPAA is misperceived as rigidly anti-disclosure, and mistakenly framed it as a "regulatory barrier" or "burden." Many of the proposed modifications double down on this misunderstanding with privacy deregulation, rather than directly addressing some professionals' confusion with improved training, education, and guidance.

The HHS Proposals Would Reduce Our Health Privacy

Modifications to HIPAA will cause more problems than solutions. Here is a brief overview of the most troubling modifications:

1. The proposed rule would massively expand a covered entity's (CE) use and disclosure of personal health information (PHI) without patient consent. Specifically, it allows unconsented use and disclosure for "care coordination" and "case management," without adequately defining these vague and overbroad terms. This expanded exception would swallow the consent requirement for many uses and disclosure decisions. Consequently, Big Data (such as corporate data brokers) would obtain and sell this PHI. That could lead to discrimination in insurance policies, housing,

employment, and other critical areas because of pre-existing medical conditions, such as substance abuse, mental health illness, or severe disabilities that carry a stigma.
2. HHS seeks to lower the standard of unconsented disclosure from "professional judgment" to "good faith belief." This would undermine patient trust. Currently, a covered entity may disclose some PHI based on their "professional judgment" that it is in the individual's best interest. The modification would lower this standard to a "good faith belief," and apparently shift the burden to the injured individual to prove their doctor's lack of good faith. Professional judgment is properly narrower: it is objective and grounded in expert standards. "Good faith" is both broader and subjective.
3. Currently, to disclose PHI in an emergency, the standard for disclosure is "imminent" harm, which invokes a level of certainty that harm is surely impending. HHS proposes instead just "reasonably foreseeable" harm, which is too broad and permissive. This could lead to a doctor disclosing your PHI because you have a sugar-filled diet, you're a smoker, or you have unprotected sex. Harm in such cases would not be "imminent," but it could be "reasonably foreseeable."

Weaker HIPAA Rules for Phone Health Apps Would Hand Our Data to Brokers

The proposed modifications will likely result in more intimate, sensitive, and highly valuable information being sent to entities not covered by HIPAA, including data brokers.

Most Americans have personal health application on their phones for health goals, such as weight management, stress management, and smoking cessation. However, these apps are not covered by HIPAA privacy protections.

A 2014 Federal Trade Commission study revealed that 12 personal health apps and devices transmitted information to 76 different third parties, and some of the data could be linked back to specific users. In addition, 18 third parties received device-specific identifiers, and 22 received other key health information.

If the proposed HIPAA modifications are adopted, a covered provider would be required to share a patient's PHI with their health app's

developer upon the patient's request. This places too much burden on patients. They are often ill-equipped to understand privacy policies, terms of use, and permissions. They may also not realize all of the consequences of such sharing of personal health information. In many ways, the deck is stacked against them. App and device policies, practices, and permissions are often confusing and unclear.

Worse, depending on where the PHI is stored, other apps may grant themselves access to your PHI through their own separate permissions. Such permissions have serious consequences because many apps can access data on one's device that is unrelated to what the app is supposed to do. In a study of 99 apps, researchers found that free apps included more unnecessary permissions than paid apps.

Next Steps

During the pandemic, we have learned once again the importance of trust in the health care system. Ignoring CDC guidelines, many people have not worn masks or practiced social distancing, which has fueled the spread of the virus. These are symptoms of public distrust of health care professionals. Trust is critical in prevention, diagnosis, and treatment.

The proposed HHS changes to HIPAA's health privacy rules would undoubtedly lead to increased disclosures of PHI without patient consent, undermining the necessary trust the health care system requires. That's why EFF opposes these changes and will keep fighting for your health privacy.

Postal Code (optional)

Anti-spam question: Enter the three-letter abbreviation for Electronic Frontier Foundation:

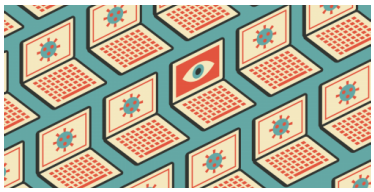
SUBMIT

RELATED UPDATES

DEEPLINKS BLOG BY JENNIFER LYNCH | JUNE 7, 2021

Maryland and Montana Pass the Nation's First Laws Restricting Law Enforcement Access to Genetic Genealogy Databases

Last week, Maryland and Montana passed laws requiring judicial authorization to search consumer DNA databases in criminal investigations. These are welcome and important restrictions on forensic genetic genealogy searching (FGGS)—a law enforcement technique that has become increasingly common and impacts the genetic privacy of millions of Americans.Consumer personal genetics companies...



DEEPLINKS BLOG BY ALEXIS HANCOCK, HAYLEY TSUKAYAMA | DECEMBER 16, 2020

Vaccine Passports: A Stamp of Inequity

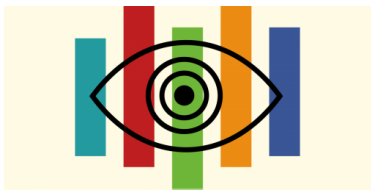
A COVID vaccine has been approved and vaccinations have begun. With them have come

proposals of ways to prove you have been vaccinated, based on the presumption that vaccination renders a person immune and unable to spread the virus. The latter is ...

PRESS RELEASE | NOVEMBER 16, 2020

EFF Urges Universities to Commit to Transparency and Privacy Protections For COVID-19 Tracing Apps

San Francisco—The Electronic Frontier Foundation (EFF) called on universities that have launched or plan to launch COVID-19 tracking technologies—which sometimes collect sensitive data from users' devices and lack adequate transparency or privacy protections—to make them entirely voluntary for students and disclose details about data collection practices.Monitoring public...



DEEPLINKS BLOG BY SAIRA HUSSAIN, JENNIFER LYNCH, NATHANIEL SOBEL | OCTOBER 22, 2020

EFF Files Comment Opposing the Department of Homeland Security's Massive Expansion of Biometric Surveillance

EFF, joined by several leading civil liberties and immigrant rights organizations, recently filed a comment calling on the Department of Homeland Security (DHS) to withdraw a proposed rule that would exponentially expand biometrics collection from both U.S. citizens and noncitizens who apply for immigration benefits and would allow...

PRESS RELEASE | AUGUST 20, 2020

EFF Calls on California Gov. Newsom To Mandate Data Privacy Protections for Californians Who Participate in COVID-19 Contact Tracing Programs

San Francisco—The Electronic Frontier Foundation (EFF) called on California Gov. Gavin Newsom and state lawmakers to ensure that all COVID-19 contact tracing programs include enforceable privacy protections that strictly limit how much and what kinds of data can be collected from Californians and prohibits using that data for anything other...

DEEPLINKS BLOG BY ADAM SCHWARTZ | AUGUST 17, 2020

No to Expanded HHS Surveillance of COVID-19 Patients

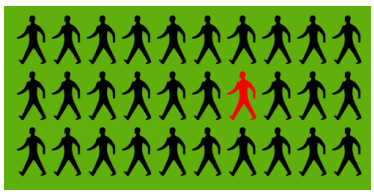
The federal government plans to process more of our personal data, in the name of containing COVID-19, but without showing that this serious privacy intrusion would actually do anything to protect public health. EFF filed comments in opposition to these new plans from the U.S. Department of Health and...

DEEPLINKS BLOG BY ALEXIS HANCOCK, KAREN GULLO | MAY 28, 2020

Immunity Passports Are a Threat to Our Privacy and Information Security

With states beginning to ease shelter-in-place restrictions, the conversation on COVID-19 has turned to questions of when and how we can

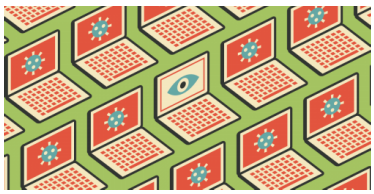
return to work, take kids to school, or plan air travel.Several countries and U.S. states, including the UK, Italy, Chile, Germany, and California, have expressed interest in...



DEEPLINKS BLOG BY MATTHEW GUARIGLIA | APRIL 15, 2020

Telling Police Where People With COVID-19 Live Erodes Public Health

In some areas of the United States, local governments are sharing the names and addresses of people who have tested positive for COVID-19 with police and other first responders. This is intended to keep police, EMTs, and firefighters safe should they find themselves headed to a call at the residence...



DEEPLINKS BLOG BY GENNIE GEBHART | MARCH 25, 2020

Verily's COVID-19 Screening Website Leaves Privacy Questions Unanswered

One week after Alphabet's Verily launched its COVID-19 screening website, several unanswered questions remain about how exactly the project will collect, use, and retain people's medical information.Verily, a healthcare data subsidiary of Google's parent company Alphabet, has until now operated its Project Baseline as a way to connect potential...

The Pregnancy Panopticon

WHITEPAPER

Women's health is big business. There are a staggering number of applications for Android and iOS which claim to help people keep track of their monthly cycle, know when they may be fertile, or track the status of their pregnancy. These apps entice the user to input the most intimate...