Law Enforcement & National Security Access to Medical Records

July 11, 2013

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

1. Section 215 of the PATRIOT Act
2. HIPAA Privacy Rule
3. Protections for Records of Federally-Funded Substance Abuse Treatment Facilities and Programs ("Part 2")

Recent revelations about the activities of the National Security Agency (NSA) and their secret surveillance programs have raised a number of serious concerns for health policy makers and practitioners. In one leaked program called PRISM [1], the NSA obtains the contents of Internet communications to or from targeted individuals who are outside the US (which may include communications with people inside the US). Under a second program, the government uses court orders issued under Section 215 of the PATRIOT Act to obtain call detail records for all telephone calls inside the US [2], both foreign and domestic.

What are the implications of these surveillance programs in terms of access to medical records and information? Can the government and law enforcement officials freely access identifiable health information in the name of national security? This CDT Policy Post explains how government access to identifiable health information is addressed by the PATRIOT Act, the HIPAA Privacy Rule, as well as the statutes and regulations protecting the confidentiality of patient information that is held by federally funded substance abuse treatment facilities and programs.

---

1. Section 215 of the PATRIOT Act

The PATRIOT Act is a broad federal statute adopted in the wake of the September 11, 2001 attacks. It amended numerous existing laws to grant federal law enforcement and intelligence officers increased powers to obtain and share records for counter-terrorism purposes. Specifically, the PATRIOT Act allows the Federal Bureau of Investigation (FBI), including when it is acting on behalf of the NSA, to petition a federal judge for an order to obtain any business records. Such records can include medical records.

Under Section 215 of the PATRIOT Act, an order compelling disclosure of records is issued by a Foreign Intelligence Surveillance Court (FISA Court) judge based on an application from the FBI Director or his designee. The application must include (1) a statement of facts showing that there are reasonable grounds to believe that the records sought are relevant to an authorized investigation to obtain foreign intelligence or to protect against international terrorism and (2) an enumeration of the minimization procedures applicable to retention and dissemination of the records. If the judge finds that the application meets those two requirements, the judge shall issue an order approving the release of the records. The statute specifies that records are presumptively relevant to an authorized investigation if the applicant shows that they pertain to a foreign power, an agent or suspected agent of a foreign power, or an individual in contact with a suspected agent of a foreign power. However, that is not the only way to show relevance. As we learned from the recent disclosures, the government was able to convince judges of the FISA Court that entire databases of call detail records are relevant to an authorized investigation, in circumstances where it would seem there was no reason to believe that all or even any of the records specifically pertained to a foreign power or an agent of a foreign power.

The application for an order and the process before the FISA Court are secret, and those who receive an order for disclosure of records are required by the law not to disclose the request.

The law does provide one small additional protection for medical records: the application for the order may come only from the FBI Director, the Deputy Director, or the Executive Assistant Director for National Security.

---

2. HIPAA Privacy Rule

Disclosure for National Security Purposes

The HIPAA Privacy Rule provides a broad exception for national security purposes. Under the Rule, a covered entity may disclose any and all protected (identifiable) health information (PHI) for “lawful intelligence, counter-intelligence and national security purposes” (emphasis added). On its face, the Rule does not require a court order or any other enforceable or formal demand; disclosure may be completely voluntary and may be initiated by the covered entity even in the absence of a request from a government official. There is no guidance from the Office of Civil Rights (which has oversight over the Privacy Rule) on what is meant by the terms “lawful intelligence” or “national security purposes” either on its website [3] or in the regulatory materials that accompanied the publication of the Rule.

Disclosure for Law Enforcement Purposes

In addition to the permissive exception for national security requests, the HIPAA Privacy Rule provides seven means by which PHI can be disclosed to law enforcement officials.1 Law enforcement is defined broadly in the Privacy Rule as “any government official at any level of government authorized to either investigate or prosecute a violation of the law.” In summary terms, the seven permitted disclosures of PHI for law enforcement are:

1. Where the disclosure is required by law (such as a state reporting law).
2. Pursuant to a court order or other legal process. HHS guidance states [4] that administrative requests issued without a court order must be accompanied by a written statement that the information requested is relevant and material, specific and limited in scope, and de-identified material cannot be used.
3. For the purposes of identifying or locating a suspect, fugitive, material witness or missing person However, the information that may be disclosed is limited to information that would help locate the person, such as name, date of birth, Social Security Number, and distinguishing physical characteristics.
4. About an individual who has been the victim of a crime. Generally, the individual must provide consent. If the covered entity cannot obtain consent because the individual is incapacitated or it is an emergency, PHI can be disclosed only if the requesting officer states that the information obtained will not be used against the victim and that the request cannot wait, and the covered entity determines the disclosure would be in the individual’s best interest.
5. About a deceased individual when the covered entity has reason to believe death was caused by a criminal action.
6. If the covered entity believes, in good faith, that the information constitutes evidence of a crime that has occurred on the premises.
7. If the entity is providing emergency health care and if disclosure is necessary to alert law enforcement to either the commission of a crime, the location of a crime, or the identity or location of a perpetrator of a crime.

Accounting of Disclosures

In general, the HIPAA Privacy Rule provides individuals with the opportunity to request from their doctor or insurer an accounting of disclosures of their PHI made over the past six years. However, an entity may exclude disclosures for national security or intelligence purposes from an accounting of disclosures. As noted above, Section 215 affirmatively bars entities from telling anyone, including the patient, about disclosures under that section. As a result, an individual may never know that her PHI was disclosed for national security or intelligence purposes.

For disclosures for law enforcement purposes, law enforcement may request that such disclosures be kept out of an accounting of disclosures. If the request is in writing, that ban can be for any length of time; if the request is verbal, the ban is for 30 days after the request.

Breach Notification

The HIPAA Privacy Rule also requires that covered entities notify affected individuals when a breach of unsecured protected health information occurs. However, it also requires that a breach notification be delayed when a law enforcement official specifies that a notification to the patient would impede a criminal investigation or cause damage to national security. The prohibition on notification is valid for the length of time specified by the law enforcement official if the request for delay is in writing, but only for 30 days when the request is made verbally.

---

3. Protections for Records of Federally-Funded Substance Abuse Treatment Facilities and Programs ("Part 2")

While the HIPAA Privacy Rule permits law enforcement officials to access protected health information in specific circumstances and explicitly permits wide-ranging access for national security and intelligence purposes, access to health records relating to treatment in federally funded substance abuse facilities and programs is more strictly limited under the federal confidentiality statute (42 U.S.C. § 290dd-2) and accompanying regulations commonly known as "Part 2."

Under the Part 2 regulations, information from a medical record relating to substance abuse treatment may be disclosed to law enforcement officials when the patient either commits a crime on the program's premises or threatens to harm program personnel. In these circumstances, only the name, address, and last known whereabouts of the suspect may be released.2

In addition, under the statute, treatment records may be disclosed if authorized by an appropriate order of a court of competent jurisdiction granted after application showing good cause. In assessing good cause the court shall weigh the public interest and the need for disclosure against the injury to the patient, to the physician-patient relationship, and to the treatment services. Upon the granting of such order, the court, in determining the extent to which any disclosure of all or any part of any record is necessary, shall impose appropriate safeguards against unauthorized disclosure.

Under the Part 2 regulations, special procedures apply if the records are going to be used to criminally investigate or prosecute a patient. A court may authorize disclosure only if the crime is extremely serious (loss of life, bodily injury, etc.), there is reasonable likelihood that the disclosure will be of substantial value to the investigation or prosecution, and there is no other way of obtaining the information.3 The Part 2 regulations provide that, in cases where the records are sought for investigation or prosecution of a crime, the substance abuse program must be given the opportunity to appear in court before a request for records identifying the patient can be compelled.3

Interaction Between Part 2 and the PATRIOT Act

We are unaware of any circumstances where the government has sought to use an order under Section 215 to obtain disclosure of records covered by Part 2, and such a request is probably quite unlikely. (Of course, since Section 215 proceedings and orders are secret, we might never know.) However, it should not be assumed that Section 215 trumps 42 U.S.C. § 290dd-2. "Where there is no clear intention otherwise, a specific statute will not be controlled or nullified by a general one, regardless of the priority of enactment." Morton v. Mancari, 417 U.S. 535, 550-551 (1974). (In this case, of course, the specific statute is the substance abuse treatment law and the general one is Section 215.) Moreover, "when two statutes are capable of coexistence, it is the duty of the courts, absent a clearly expressed congressional intention to the contrary, to regard each as effective." Id. at 551. A court considering a Section 215 application for records covered by Part 2 might reconcile the two statutes by referring to the good cause test spelled out in 42 USC § 290dd-2 in deciding whether the records are "relevant" to an authorized intelligence or counter-terrorism investigation and subject to adequate minimization rules.5 Generally, records obtained under Section 215 are not used in criminal investigations or prosecutions, but such use is not flatly prohibited; in other contexts data obtained for intelligence purposes may be used in criminal matters. In the remote situation

where Section 215 was used to obtain disclosure of substance abuse treatment records and the government sought to use such records in a criminal investigation or prosecution, there might be a conflict between Section 215 and the Part 2 regulations. It is hard to say how such a conflict would be reconciled.

For more information, please contact Christopher Rasmussen (chris@cdt.org [5]), Policy Analyst, Health Privacy Project.

1. 1. 45 CFR 164.512(f). As HHS warns on its website, “For a complete understanding of the conditions and requirements for these disclosures, please review the exact regulatory text … .”
2. 2. 42 CFR 2.12(c)(5).
3. 3. 42 CFR 2.65.
4. 3. 42 CFR 2.65(b).
5. 5. “In assessing good cause the court shall weigh the public interest and the need for disclosure against the injury to the patient, to the physician-patient relationship, and to the treatment services. Upon the granting of such order, the court, in determining the extent to which any disclosure of all or any part of any record is necessary, shall impose appropriate safeguards against unauthorized disclosure.” 42 USC § 290dd-2(b)(2)(C).

Copyright © 2013 by Center for Democracy & Technology.
The content throughout this website that originates with CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.
Source URL: https://www.cdt.org/policy/law-enforcement-national-security-access-medical-records

Links:
[1] http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html
[2] http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order
[3] http://www.hhs.gov/hipaafaq/permitted/law/505.html
[4] http://www.hhs.gov/ocr/privacy/hipaa/faq/disclosures_for_law_enforcement_purposes/505.html
[5] mailto:chris@cdt.org