Civil Society Consultation on the Universal Periodic Review Recommendations on National Security supported by the U.S.

The Right to Health Privacy: Human Rights and the Surveillance and Interception of Medical and Health Records by Security Agencies

Submitted by:
World Privacy Forum
October 7, 2014

The World Privacy Forum respectfully submits these comments to the Civil Society Consultation on the Universal Periodic Review Recommendations on National Security supported in whole or in part by the U.S. The World Privacy Forum is a 501 (c)(3) non-profit public interest research group based in the United States. We focus exclusively on privacy and security issues and have substantive expertise in health privacy.

1. Our comments focus on the issue of the U.S. National Security Agency's (NSA) interception of, acquisition of, and access to the health (including physical and mental health) records held by health care providers, health insurers, and health care clearinghouses located in the United States or otherwise subject to U.S. health privacy law.

2. The Universal Declaration of Human Rights, in Article 12 and 25, provides that individuals should be free to seek health care without intrusion by their government. The United Nations General Assembly adopted resolution 68/167 in December 2013, which expresses concern regarding the negative impact that surveillance and interception of communications may have on human rights. The United States in the 2010 UPR supported the right to privacy, and the goal of legislation or regulations that would work to prevent the violations of individual privacy, including "constant intrusion," by its intelligence and security organizations. Specifically, the U.S. supported in part:

- § **59:** Legislate appropriate regulations to prevent the violations of individual privacy, constant intrusion in and control of cyberspace as well as eavesdropping of communications, by its intelligence and security organizations.

- §**187:** Guarantee the right to privacy and stop spying on its citizens without judicial authorization.

3. The World Privacy Forum acknowledges that there are lawful reasons for access to health records for investigations.

4. We are, however, most concerned that non-transparent access to patient health files by national security agencies occurs in two circumstances: 1.) When the files are held by health care providers, and 2.) When the files are in transmission between providers, insurers, and other lawful users. In these comments, we discuss the issue of a lack of transparency and oversight regarding the acquisition and use of health records by federal agencies with national security functions and, in particular, by the NSA.

I. The lack of transparency regarding U.S. security agency acquisition of health records when held by health care providers and other entities covered under health privacy legislation.

5. There are no meaningful procedures or protections established by federal law governing the the acquisition or interception of patient health records by national security agencies from a health care provider, insurer, or clearinghouse.

6. U.S. health care providers are regulated under the federal health privacy rule. Federal law includes a broad national security exemption that offers no effective restrictions on the disclosure of health records by health care providers for national security and intelligence activities. The exemption [45 CFR 164.512(k)(2)] states:

> (2) *National security and intelligence activities.* A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, *et seq.*) and implementing authority (*e.g.,* Executive Order 12333). [45 CFR 164.512(k)(2)].

7. Because of the breadth of this exemption, it is lawful for health care providers and other entities covered by the law to disclose health records to national security agencies without any procedural standards, any formal judicial request, any showing of relevance or importance, any probable cause, or any reasonable cause. The law does not require a written -- or indeed any -- request for it to be lawful for a covered entity to hand over patient health files. Further, there are no adequate procedures under which a record keeper or record subject can challenge a request for the records as unlawful, inappropriate, or as not in accordance with statutory procedures.

II. The lack of transparency regarding the U.S. security agency acquisition of health records in transmission outside of the health care provider context

8. Events since 2010 have better informed the public and the world about health record privacy and national security investigation activities, including interception of health records in bulk collections. We are most concerned about examples regarding the

NSA's activities.

9. The NSA has broken the encryption that in the past has protected health records. (NewYork Times, *Top Secret NSA Program Cracks Most Internet Encryption Tools*, Sept. 05, 2013.) While this does not prove that the NSA is deliberately intercepting health records, it does indicate that traditional means of making health files private are no longer reliable against intrusion, particularly during transmission, even when the security meets the requirements set out in the federal health security rule. We certainly have no confidence that standard encryption protocols protect health records against NSA capabilities.

10. Health records of individuals, including non-targeted individuals, have been routinely intercepted by the NSA. A reporter at the Washington Post who received copies of intercepted files from former NSA contractor Edward Snowden documented this issue, noting the presence of health files. He wrote: "About 16,000 of the data files contained the text of intercepted conversations. The rest were photographs or documents such as **medical records,** travel vouchers, school transcripts and marriage contracts." (Barton Gellman, The Washington Post, *How 160,000 intercepted communications led to our latest NSA story*, July 11, 2014. <http://www.washingtonpost.com/world/national-security/your-questions-answered-about-the-posts-recent-investigation-of-nsa-surveillance/2014/07/11/43d743e6-0908-11e4-8a6a-19355c7e870a_story.html>.

11. The U.S. Executive Branch acknowledged in 2013 that the business records provision of the USA PATRIOT ACT had been re-interpreted to allow the U.S. government to collect the private records of large numbers of ordinary Americans via bulk collection. A bi-partisan group of U.S. Senators wrote to the Director of National Intelligence on June 27, 2013 requesting answers to issues regarding interception of health records:

> "We are troubled by the possibility of this bulk collection authority being applied to other categories of records. The bulk collection authority could potentially be used to supersede bans on maintaining gun owner databases, or laws protecting the **privacy** of **medical records,** financial records, and records of book and movie purchases. These other types of bulk collection could clearly have a significant impact on Americans' privacy and civil liberties as well." <http://www.wyden.senate.gov/download/?id=87b45794-0fa4-4b1a-b3a6-e659a91a5042&download=1>.

12. No existing legal mechanisms provide appropriate standards, transparency, or oversight in the use of health records for national security investigations.

III. The importance of health privacy as a human right and value worth protecting

13. We are concerned that individuals may be chilled from seeking necessary and even life-saving health treatment due to legitimate privacy concerns regarding their health records. As health records become increasingly digitized, routine access to patients' electronic health records by U.S. intelligence and security agencies becomes

more likely. We include remote electronic access to this assessment.

14. The goals of UPR § 59 are that countries "Legislate appropriate regulations to prevent the violations of individual privacy, constant intrusion in and control of cyberspace as well as eavesdropping of communications, by its intelligence and security organizations. These goals are not being met in the United States with respect to disclosure and interception of health records by national security agencies.

IV. Recommendations

15. The World Privacy Forum recommends the following steps be taken:

Recommendation 1. Change U.S. law so there are more accountability and better procedures for national security requests, demands, and interceptions. Specifically, we recommend the following changes to U.S. law with respect to access by or disclosure of health records to U.S. national security agencies:

a. Health information should only be disclosed for national security purposes pursuant to a judicial warrant.
b. There must be procedures under which record keepers can challenge national security demands for health records that are unlawful or inappropriate.

If there is no requirement for a judicial warrant, then we offer these further recommendations:

c. Requests for health information by all national security agencies must meet standards of reasonable or probable cause.
d. Formal requests by all national security agencies for health records should be subject to the supervision of the federal courts.

Recommendation 2. The U.S. should accept the letter and spirit of §59 and §187 and should take immediate corrective action.

16. The lack of sufficient human rights protections for health privacy and health records in the U.S. erodes the values expressed in the Universal Declaration of Human Rights, in Article 12 and 25.

Thank you for your attention to this matter.

Respectfully submitted,

Pam Dixon, Executive Director
World Privacy Forum
www.worldprivacyforum.org
3108 Fifth Ave, Suite B,
San Diego, CA 92103