Testimony of Sarah Tucker to the National Committee on Vital and Health Statistics

June 15, 2010

I thank you for the opportunity to appear today to discuss the handling of sensitive information contained within health records. I have reviewed the Committee's February 2008 letter and the recommendations clearly reflect the thoughtful, deliberate process the Committee has undertaken. On behalf of victims of domestic violence, stalking, and sexual assault, I thank you for your serious consideration of the issues surrounding the handling of sensitive health information. The intimate nature of sexual assault and domestic violence mean that these crimes often go unreported. When victims do have the courage to seek medical attention for injuries, they should be able to do so knowing that the information they provide to their physician is kept as secure, safe, and private as possible. A clear, comprehensive understanding of the risks and benefits of the electronic exchange and the option to sequester sensitive information are critical to ensuring that victims of domestic and sexual violence trust and participate in electronic health records and health information exchanges (HIEs). Additionally, victims must be able to trust that the people who access their records have the appropriate role-based and relationship-based credentials and that their own access is highly secure and based on in-person authentication. Finally, victims must be able to trust that records used for research are truly anonymized and do not hold any risk to their safety.

I am here today representing the Safety Net project at the National Network to End Domestic Violence, a social change organization dedicated to creating a social, political, and economic environment in which violence against women no longer exists. Founded in 1995, the National Network to End Domestic Violence (NNEDV) represents 56 state/territory domestic violence

coalitions who in turn represent over 3,000 local domestic violence service providers across the country.

Since 2005, I have worked as part of the Safety Net Project at NNEDV to educate victims of sexual and domestic violence, their advocates and the public on the strategic use of technology to increase personal safety and privacy. Safety Net is the only national initiative addressing the intersection of domestic violence and all forms of technology. Looking beyond the traditional "digital divide," our project is ardently working to increase the technology knowledge and skills of victims, advocates, law enforcement, and allied organizations in every state and each of the local shelter and hotline programs across the country. Safety Net also tracks emerging technology issues and their impact on victim safety, working with local, state and federal agencies to amend or create policies that enhance victim safety and confidentiality. I have been working to end violence against women for over 10 years and have focused on the intersection of technology and domestic violence since 2005.

Domestic and sexual violence is a terrifying reality for women and children across the United States.[1] Millions of women are physically abused by their husbands or partners each year[2] and sexual assaults are a common tactic of intimate assailants. Disclosure of the location of such victims can create life-threatening danger and life-changing stigma for victims. Sadly, domestic violence is quite prevalent, and women continue to be the vast majority of victims. The National Institute of Justice reported that 4.9 million intimate partner rapes and physical assaults

[1] Because the vast majority of victims of domestic violence and sexual assault are women, we primarily use female nouns and pronouns throughout these comments. See Callie Marie Rennison & Sarah Welchans, U.S. Department of Justice, Intimate Partner Violence, at 1 (2000) (estimating that 85% of reported assaults on partners or ex-partners are committed by men against women). We acknowledge that men are also victims of domestic violence, especially in same-sex relationships.

[2] See Patricia Tjaden & Nancy Thoennes, Nat'l. Inst. of Justice, Prevalence, Incidence and Consequences of Violence Against Women: Findings from the National Violence Against Women Survey, at 2, 7 (1998). In fact, the National Institute of Justice reported that 5.9 million assaults are perpetrated against women annually. See id. at 11. See also United States v. Morrison, 529 U.S. 598, 632 (2000) (Souter, J., dissenting) (citing estimate of four million women assault victims every year).

are perpetrated against U.S. women annually.[3] Leaving the relationship does not stop the violence. In fact, the most dangerous time for a victim of domestic violence is when she takes steps to leave the relationship.[4] An average of three women are killed by their current or former intimate partner every day in the US.[5] Many victims are stalked relentlessly for years after having escaped from their partners. Fifty-nine percent of female stalking victims are stalked by current or former intimate partners,[6] and 76% of women killed by their abusers had been stalked prior to their murder.[7] Batterers who stalk their former partners, determined to hunt them down, are the most dangerous and pose the highest lethality risk.[8] The severity of this "separation violence" often compels women to stay in abusive relationships rather than risk greater injury or death to themselves or their children. Many of those who succeed in leaving their abuser live in constant fear of being found. This constant fear of being found is only exacerbated by the potential for a victim's abuser to obtain important information about the victim's location and activities through databases like the Nationwide Health Information Network (NHIN)

There are currently significant legal protections and precedent for protecting victims of domestic violence. Advocate confidentiality laws protecting victim records (akin to attorney-client privilege) exist in nearly every state. One federal example, The Violence Against Women Act (VAWA) of 2005, prohibits VAWA-funded domestic violence and rape crisis programs from disclosing personally identifying information about any victims they serve. Personally

---

[3] Patricia Tjaden and Nancy Thoennes, National Institute of Justice and the Centers of Disease Control and Prevention, *Extent, Nature, and Consequences of Intimate Partner Violence (2000);* Dr. Callie Marie Rennison, Department of Justice, Bureau of Justice Statistics, *Intimate Partner Violence, 1993-2001* (February 2003).
[4] Ronet Bachman and Linda Salzman, Bureau of Justice Statistics, *Violence Against Women: Estimates From the Redesigned Survey* 1 (January 2000).
[5] U.S. Department of Justice, Prevalence, Incidence, and Consequences of Violence Against Women: Findings from the National Violence Against Women Survey (1998).
[6] Tjaden &Thoennes. (1998) "Stalking in America," NIJ.
[7] McFarlane et al. (1999). "Stalking and Intimate Partner Femicide," *Homicide Studies.*
[8] Barbara J. Hart, *Assessing Whether Batterers Will Kill.* (This document may be found online at: http://www.mincava.umn.edu/hart/lethali.htm), Jacqueline Campbell, *Prediction of Homicide of and by Battered Women,* reprinted in *Assessing Dangerousness: Violence by Sexual Offender, Batterers, and Sexual Abusers* 96 (J. Campbell, ed., 1995).

identifying information is information likely to disclose the identity or location of a victim of domestic violence, dating violence, sexual assault, or stalking, including name, address, contact information (postal or e-mail, internet protocol address, telephone, or facsimile), Social Security number or "any other information, including date of birth, racial or ethnic background, or religious affiliation, that, in combination with any of the above would serve to identify an individual.[9]"

The federal health privacy regulations of HIPAA and ARRA have been an important step toward stronger privacy protections. But these regulations are not comprehensive and do not meet the privacy standards for victims of domestic and sexual violence. Currently, health information can be accessed by a large audience, and the creation of the NHIN means that breaches of confidentiality at one healthcare provider will have statewide effects. Personal, confidential information of victims will be exposed to anyone in the state with authorized access, increasing victims' vulnerability to being tracked down by their abusers.

The NHIN and regional Health Information Exchanges (HIE's) will allow the electronic exchange of medical information and patient records. Although the highest levels of security will be enacted, no computer security system is infallible. Balancing the convenience of electronic exchange with the significant security concerns is not an easy task. In fact, since April, electronic health records have been breached in DC, CA, KY, NM, MA, and SC.[10] Regardless of the safety and security precautions taken, electronic health records cannot be 100% secure.

---

[9] VAWA 2005, 42 USC §13925(a)(18)(2008)

[10] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html; http://www.esecurityplanet.com/features/article.php/3882536/Laptop-Medicaid-Patients-Data-Disappear.htm; http://louisville.bizjournals.com/louisville/stories/2010/05/31/daily10.html

Overall, however, the highest danger to domestic violence victims lies in the simple fact that an electronic health record exists at all. The most sensitive information for a victim of domestic violence is often basic demographic information, including name, age, date of birth, address, city, state, social security number, phone number, email address, number of children, and more. The fact that this record can be located and accessed through the NHIN or a local HIE exacerbates the danger. Therefore, we are providing the following recommendations to ensure that personally identifiable medical information is kept as secure as possible.

Recommendation #1: We recommend that HHS encourage HIEs to adopt an opt-in policy for all patients. Patients are not truly choosing to participate in the system unless they are fully educated about the risks and benefits, and freely give their fully informed consent.

Patients are largely unaware of how their medical information is used and exchanged, and it is often difficult for them to truly grasp the path of their personal information, especially in the midst of a medical trauma. Because of this, it is crucial that patients are not automatically included in a statewide information exchange. Opt-in consent will better protect patient privacy and facilitate patient trust in the privacy and security of their health information. Additionally, communities implementing HIE's must carefully consider the process for opting-out after someone has been in the system for some period of time. Someone in an abusive relationship may opt-in when the HIE is initially enacted, but may later need to opt-out to keep herself and her children alive and safe. All HIE's must have a transparent, easily accessible process to allow victims, and all patients, to opt out from the exchange.

Recommendation #2: We recommend that domestic and sexual violence be added as categories of sensitive information.

Domestic violence, sexual assault, and stalking are the most personal of crimes, and the more personal information that the perpetrator has about his victim, the more dangerous and

damaging the perpetrator can be. For victims of domestic violence, the medical part of their medical record may not be the most sensitive; rather the victim's contact information may be the information that could compromise the victim's safety. "Who" sees their record is of paramount importance. Unlike a blood alcohol level test or HIV medications, there is typically no specific medical test or medication that indicates that a person is a victim of domestic violence. Sometimes, domestic violence is indicated by simply glancing at the list of the providers with whom the patient met. If a woman has come into a hospital and staff observe that she may be a victim of abuse, her record may indicate that staff requested a consultation with a social worker. For those hospitals that have specialized domestic or sexual violence units or social workers, the record would clearly indicate that the domestic violence/sexual violence team was called in.

Many hospitals routinely screen for domestic violence by asking patients a question like "Are you being hurt by anyone in your home?" The answer to this question blatantly indicates domestic violence and is a clear example of information that should be sequestered. However, more often than not, any mention of domestic violence in the health record is recorded in the physician's notes. For this reason, it is critical that the NHIN allow the sequestration of physician notes. This will overwhelmingly increase the number of victims of domestic and sexual violence who are comfortable with participating in the exchange. We acknowledge that physicians will be reluctant to endorse a system that allows sequestration of their notes, as many genuinely feel that they need all possible information to treat a patient. However, without the sequestration of physician notes, many consumers will completely opt-out of the exchange, therefore leaving physicians with NO information. We strongly believe that *some* information is better than no information. Additionally, other aspects of the medical record including lab tests and diagnoses will give medical professionals a general idea of questions to ask and information

to consider. Certainly, all medical systems and HIE's have or are developing procedures or policies to protect, segment, and sequester portions of VIP files (governors, celebrities, etc). Protecting victims of domestic violence merely extends these protections already afforded to others.

The ability to choose which parts of their medical record to sequester is extremely critical for victims of sexual assault. For these victims, all information regarding that assault, including tests for STD's, emergency contraception, forensic exams, consultation with a social worker, etc., should be sequestered as sensitive health information. The victim may choose to disclose information to certain practitioners; however she may also choose not to disclose a rape that happened 5 years ago to her current ophthalmologist, podiatrist, or dermatologist.

Recommendation #3: We recommend that records from which sensitive information has been sequestered are not marked in any way.

While we strongly support the sequestration of sensitive information, we are concerned that records with sensitive information withheld will be marked as "incomplete," essentially putting a scarlet letter on those patients. The very concept of needing to indicate that something is withheld from these records presupposes that all medical professionals should have access to all patients' complete medical histories at all times. This access does not currently exist nor has it ever existed, and it precariously skirts the line of sharing information simply because it is possible. Because of HIPAA's very narrow definition of "sensitive" information, we are concerned that physicians may erroneously assume that any record that indicates that sensitive information has been removed is because the patient is a recovering alcoholic or has a mental health condition, leading the physician to attribute the patient's symptoms to "depression" or rather than actually investigating the patient's symptoms. One alternative is to label all patient

records with a standard disclaimer indicating that some information may be withheld. This removes the stigma and reminds the physician that electronic records are no substitute for a thorough discussion to both learn information and build rapport with the patient. Physicians currently ask patients about information that is not provided for them and there is no reason to believe that they would stop having these important dialogues with patients.

Recommendation #4: We recommend that HHS mandate strict role-based and relationship-based authentication to access the NHIN.

Currently, even without computerized statewide or national health information exchanges, victims have been located because the children were covered by the abuser's health insurance. We are concerned that the implementation of the NHIN and regional HIEs will exacerbate this problem. In one situation, a victim took her children to a new physician in a new town, and informed the office manager that she wished to pay by cash. Someone in the chain of treatment/payment processing entered the children's social security numbers into a database and learned that the children were still insured under their father's plan. In summary, the medical bills were processed through the insurance company, the abusive husband received a copy of the explanation of benefits from the insurance company, and he was able to discover where the victim and children were hiding, causing them to once again have to flee and relocate.

Abusive partners are cunning and manipulative. If a friend, relative, or neighbor works in the medical field, it is quite likely that an abusive partner will try to convince that person to look up information about the victim. This has also happened with police records[11], motor

11 May 19, 2006 911 dispatcher misuses database, kills ex-girlfriend By Declan McCullagh Staff Writer, CNET News http://news.cnet.com/Police-blotter-911-dispatcher-misuses-database,-kills-ex-girlfriend/2100-1030_3-6074559.html

vehicle[12] records, state department records[13], and others. In 2003, a 911 dispatcher in Pennsylvania misused law enforcement databases to locate his ex-girlfriend and her new boyfriend. Even though disciplinary actions were brought against him, by that time, he already had the victim's sensitive information. Armed with her current address, the dispatcher proceeded to purchase a gun and fatally shoot both his ex-girlfriend and her new boyfriend. This horrific incident shows that both role-based access and relationship-based access are essential to reducing the number of people who have access to a patient's record. Because of the wide range of sizes and types of medical practices, it is impractical to suggest that these access levels be uniformly set across healthcare practices and systems. Rather, we advocate that access to a patient's medical record should be limited by role (physicians should have a different access level than an x-ray technician) and by relationship (a nurse in the pediatric ward of the hospital should not have access to the records of someone in the geriatric ward). By limiting access to the fewest people possible, potential danger to victims of domestic violence will be greatly reduced.

Reactionary security measures, such as audit trails, are not sufficient. While audit trails are useful to show who accessed information after the incident, we cannot rely on audit trails to prevent unauthorized access. For audit trails to prevent personal harm, the NHIN would need to create a "flagging system" that would flag the accounts of elected officials, undercover agents, and victims so that when their records are queried, an immediate alert would be sent to a supervisor or internal affairs unit to investigate. Without a real-time flagging system, audit trails will not prevent a domestic violence homicide, but merely assist in the prosecution after the fact.

---

[12] 12[1] Kevin Murphy, *Officer's Actions will Cost 25,000*, GAZETTEXTRA, Feb. 15, 2007, *available at* http://www.gazetteextra.com/mezera021507.asp.

[13] Sharon Gaudin, "Federal Agent Indicted For Using Homeland Security Database To Stalk Girlfriend," Information Week, Sept 20, 2007. Available at: http://www.informationweek.com/shared /printable Article.jhtml?articleID=201807903.

Recommendation #5: We recommend that the security of patients' access to their own medical records is enhanced by a one-time, in-person identity authentication.

While we highly support the right of a patient to access her own medical records, we do suggest extreme caution regarding remote access via the Internet and user authentication. In situations of domestic violence the patient's intimate partner knows so much about her life and can easily answer questions regarding maiden name, social security number, city of birth, and other personal questions used to authenticate a user's identity. Simply requiring a password and a "secret question" doesn't provide adequate security for such sensitive personal information. After all, a complete stranger was able to access vice-presidential candidate Sarah Palin's email account by researching the answer to her secret question. We recommend that patients be provided with a pin code, available at any medical office with access to the NHIN. After appearing in person and showing photo identification, the medical provider can request that the computer generate a pin code, and then provide that pin code to the patient.

Recommendation #6: We recommend that HHS offer guidance regarding a clearer definition of "anonymized" medical records.

In the past year, numerous celebrities have had their medical records breached by medical professionals, purely out of curiosity or a desire to make money by selling the information to tabloids or others[14]. Similarly, database vendors are already offering multi-million discounts to health systems if they share their patients' "anonymized" medical records. Quite often, when records are "anonymized" for research, only the name and social security number are stripped and additional demographic information is not removed. As Carnegie Melon professor Dr. Latanya Sweeney found, date of birth, gender and a person's five-digit zip code alone can

[14] A *New York Times* story highlights multiple examples of unauthorized searches: (a) when Bill Clinton had surgery in 2004, (b) 1,500 attempts to see a local athlete, and (c) dozens of attempts to view the records of a victim of a domestic homicide. Available at: www.nytimes.com/2006/12/03/business/yourmoney /03health.html?ex= 1322802000&en=b2c0f7946b4e3d9d&ei=5090.

identify 87 percent of the people in the United States. So even without a social security number, a person can be identified nearly nine out of ten times. In 2005 Dr. Sweeney testified before the Department of Homeland Security noting that in 1997 she was able to identify the medical record of Former Massachusetts Gov. William Weld by using just his date of birth, gender and zip code.[15] Anonymized records reach hundreds of third-parties and thousands of employees, exponentially increasing the number of people who have access to victims' information.

Data brokers clamor for these "anonymized" records, and software companies who implement health information exchanges often sell "anonymized" data to drug companies, insurance companies, or other medical providers. A May 17 article in the Dallas Morning News stated:

> "Cerner Corp. - a Kansas City-based electronic health record vendor with 200 Texas customers, shares unidentifiable patient records with drug companies and researchers looking for patients to participate in clinical trials, says a company spokeswoman. Cerner electronically gives drug companies a patient's medical record that does not reveal that person's name or Social Security number."
>
> "AthenaHealth Inc., the Watertown, Mass., company that implemented an electronic records program for Cook Children's Health Care System in Fort Worth TX, has offered Cook Children's a multi-million discount in exchange for sharing their patients' data. Rather than pay $50 million to $120 million installing software for its 400 physicians in 55 locations, it paid less than $1 million for an online record-keeping service."

As budget-conscious states across the nation begin to implement HIE's, vendors are luring them to use their electronic record systems with these multi-million dollar discounts. The very fact that healthcare systems are putting a price on privacy is unfathomable. The privacy of victim of domestic violence is not an exercise in theory or philosophy. These are very real situations that far too often end in death. Because of discounts like the one described above, we are concerned

[15] Testimony of Latayna Sweeney, PhD before the Privacy and Integrity Advisory Committee of DHS, "Privacy Technologies for Homeland Security" – June 15, 2006

that patients will be pressured to opt-in to systems with misleading statements regarding the reduced quality of care they will receive if they do not opt-in. Additionally, we are highly concerned that large healthcare systems will place extensive pressure on their physicians to reach a certain rate of "opted-in" patients.

Patient privacy must be paramount during the development of the NHIN. The benefits of electronic health systems cannot be realized unless individuals are confident that strong privacy protections are in place. Without privacy protection, individuals will avoid treatment and be much more selective about the information they share with their doctors. In fact, the California Health Care Foundation found that one in eight Americans have put their health at risk *because of privacy concerns*. Survey participants admitted that because of privacy concerns, they avoid seeing their regular doctor, ask their doctor to alter diagnosis, pay for tests out-of-pocket, or avoid tests altogether. More than half (52%) of respondents were concerned that employers may use health information to limit job opportunities.[16] In another study, the Rand Corporation found that 150,000 soldiers suffering from PTSD do not seek treatment because of privacy concerns, contributing to the highest rate of suicide among active duty soldiers in 30 years[17] Patients MUST believe that healthcare providers and HIE administrators are doing all that they can to mitigate the risks of medical identity theft, unauthorized access by insurance companies, and other risks.

In conclusion, I sincerely appreciate your consideration of this topic. Victims of domestic violence face an increased risk when data is collected, kept and breached. They risk much more than identity theft or other types of fraud; they risk their lives and the lives of their

[16] National Consumer Health Privacy Survey 2005, California Health Care Foundation, available at: http://www.chcf.org/publications/2005/11/national-consumer-health-privacy-survey-2005

[17] "Invisible Wounds of War", the RAND Corp., p. 436, (2008)

children. It is so important that victims are informed about the risks and benefits of the NHIN and that these risks are reduced by proactive steps such as recognizing domestic and sexual violence as categories of sequestered information and limiting access to the NHIN to those that have been carefully authenticated based on their role and relationship to the patient. Additionally, it is essential that the NHIN proactively address attempts at patient impersonation through a security measure like in-person access codes, and that medical information is truly anonymized before being released to third parties.

Once again, thank you for the opportunity to testify today. It means so much to victims of domestic violence and stalking that you are carefully considering all aspects of this complex issue and are contemplating privacy protections for all citizens, including these vulnerable victims.