COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER
to
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office of the Assistant Secretary for Preparedness and Response, Office of Preparedness and Emergency Operations; Privacy Act of 1974; Report of a New System of Records
Docket No. HHS-2007-0159

The Department of Health and Human Services (HHS) has issued a Privacy Act System of Records Notice (SORN) describing a new system of records: "The National Disaster Medical System (NDMS) Patient Treatment and Tracking Records System."[1] According to the notice, the purpose of the System is to "collect data from individuals using the medical care capabilities provided by NDMS."[2] Pursuant to that notice, the Electronic Privacy Information Center (EPIC) hereby files these comments. The Electronic Privacy Information Center is a not-for-profit research center based in Washington, DC. Founded in 1994, EPIC focuses on the protection of privacy and the First Amendment.

I. Introduction.

Natural and man-made disasters are unlike other human events—they may affect a large population and may tax the resources of local, state and federal entities. The chaotic and unpredictable nature of disasters, couple with the rapid collection and use of personal information, make this proposed records system of particular interest to privacy advocates. The general approach to data collection, sharing, and use by government agencies should incorporate appropriate privacy protections for victims of disasters. Victims will be dependent on the government for subsistence in the form of shelter, food, and medical care. The government will have easy access to their data, and part of the protection and care the government provides must include protecting the privacy of those who have been subjected to disasters.

The right of privacy in the post Hurricane Katrina environment was lost on a number of fronts. Both public and private efforts collected personally identifiable information on evacuees in the course of providing services as well as determining worthiness for receiving assistance. Instances of abuse of evacuees included the myriad of databases that cropped up on the Internet containing personal information of those who sought assistance from private and some public entities.[3] The privacy implications for those displaced by the disaster included the concerns of survivors of domestic violence regarding their location and the creation of medical prescription databases.[4] These experiences should caution NDMS as it builds a records system, so that among the care that NDMS provides is the protection of personal data.

---

[1] Report of a New System of Records, 72 Fed. Reg. 35,052 (June 26, 2007) [Hereinafter, NDMS Notice].
[2] *Id.*
[3] *See* Hurricane Katrina Evacuee Database, http://www.lsaii.org/shelters/. *See* also Hurricane Katrina Resident Evacuation Information, http://www.lnha.org/katrina/default.asp.
[4] Ryan Singel, *Katrina Whips Up Data Storm*, Wired News, May 5, 2006, http://www.wired.com/news/politics/privacy/1,70819-0.html.

The nature of this records system requires that great concern and care be taken with respect to privacy. In the NDMS system, individuals are being asked to turn over their data not just for care, but also for entry into a system of records that may not comport with their privacy preferences. Importantly, this is care delivered during a tumultuous exigency or catastrophe. Individuals may be seeking emergency care, be disoriented, and not be served by their traditional, familiar caregivers. They may also have other concerns on their minds, such as the situation of their family members, or how they will organize their lives after the disaster. These factors may affect an individual's ability to make decisions about the privacy and disclosures of their medical data. Their concerns about privacy should not limit their ability to get proper care. Because of the need to give data in order to gain proper care, any notion of implied consent to further uses of the data should be extremely limited. Protecting privacy and providing care will require that individuals have an ability to control their data, rather than simply exercising the choice to hand it over for proper care.

The system raises at least two specific privacy issues that need to be addressed in a revised system of records notice. First, the disclosures do not clearly comport with established medical privacy regulations. Second, the routine use disclosure to family members does not account for location privacy interests, specially those interests of domestic violence survivors. Fair Information Practices principles of accountability and use limitation provide solutions to both of these problems.

II. The NDMS Patient Treatment and Tracking System.

The NDMS records system will include all persons treated by NDMS disaster teams.[5] This also includes data on animals treated by the veterinary teams.[6] Records in the system include "all data pertaining to the treatment and movement of patients,"[7] and includes:

1. NDMS Team Identification.
2. Chart Number.
3. Time and Date Patient seeks treatment.
4. Triage Category and health status.
5. Location where Patient is seen and transferred.
6. Patient Identification--Name, Address, City, State, Zip, Date of Birth, Phone Number, Employment, Weight, Next of Kin.
7. Complaints/Symptoms.
8. Vital Signs/Treatment Recommended and/or Prescribed.
9. Discharge--Time, Date, Disposition, Recommendations.
10. Patient Authorization--Requires Patient Signature in Front of Witness and Witness Verification through Signature.
11. Any potential attachments such as X-rays and laboratory reports showing test results.[8]

Since the system also handles animals being evacuated, personal data will also include owner name, address and telephone number, but animal medical information will not be covered by the

[5] NDMS Notice, *supra* note 1 at 35,053.
[6] *Id.*
[7] *Id.*
[8] NDMS Notice, *supra* note 1 at 35,053.

Privacy Act.[9] The sources of this data are the patients themselves, those treating the patients, or by access to the personal health records of the patients.[10]

Agencies may disclose data according to "routine uses" so long as these are for a purpose compatible with the purposes for which it was collected and these uses are disclosed in the federal register notice.[11] The NDMS Patient Tracking System contains various routine uses which are of interest.

Routine use disclosures will be made to Department of Health and Human Services (HHS), the Department of Homeland Security (DHS), the Department of Defense (DoD) and the Department of Veteran's Affairs (VA).[12] According to the notice this is because the treatment and evacuation of patients is a shared responsibility among those agencies.[13] Routine use disclosures will also be made to contractors, grantees and consultants who need to have access to the records in order to perform a service related to the collection of the data.[14]

Patient status and location is also the subject of routine use disclosures. Disclosures will be made to state or federal agencies in order to make determinations about benefits or to collaborate with families in locating evacuated family members.[15] Lastly, disclosures will also be made directly to family members of a patient about their status and location.[16]

III. NDMS Should Have Meaningful and Enforceable Health Privacy.

Meaningful and enforceable health privacy protections will improve the quality of care as well as protect patient privacy. At a minimum, the privacy practices of Health Insurance Portability and Accountability Act (HIPAA) need to be followed. The system of records notice does not clearly describe the interaction between HIPAA and the system of records. Furthermore, the routine use disclosures must be clearly cabined by HIPAA, in order to provide patients with some enforceability. Besides HIPAA, other sources of medical privacy principles, such as the state laws and profession codes, should also guide NDMS privacy protections.

a. Good Care and Public Preferences Require Good Privacy.

Building strong privacy into the system will improve patient care and data integrity. Individuals know the value of sharing their health information with their service providers in order to get proper care. Americans are almost unanimous (97%) in thinking that doctors should have access to all of their information to provide care.[17] However, one in eight patients have

---

[9] *Id.* at 35,054.
[10] *Id.* at 35,055.
[11] 5 U.S.C. § 552a(b)(3) (referring to the definition in § 552a(a)(7) and disclosure requirement in § 552a(e)(4)(D)).
[12] NDMS Notice, *supra* note 1 at 35,054
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] Markle Foundation, *Americans See Access to Their Medical Information as a Way to Improve Quality, Reduce Health Care Costs*, (Dec. 7, 2006) *available at* http://www.markle.org/downloadable_assets/news_release_120706.pdf.

engaged in behaviors against their medical interest to protect privacy.[18] These included avoiding a regular physician, avoiding diagnostic tests and asking a physician to not report or report a less serious diagnosis.[19] Young people and those with disease were more likely to engage in these behaviors.[20] These behaviors hurt patients and show that patients are trading off proper care in the face of privacy uncertainty. Disaster patients should not be forced into similar situations.

A Gallup Survey clearly shows that public attitude does not favor disclosures of health records without permission.[21] Large number oppose their medical data being seen by government agencies (92%) or the police (88%) without permission.[22] Additionally, 88% opposed storing their medical records in a national database where others could access this information without the patient's permission.[23] Confidentiality is paramount, as 95% believe that statements made to a doctor in confidence should not be entered into national databases.[24]

As noted above, the nature of the system is such that great care needs to be taken to assure that patient privacy is protected. The public's general attitudes and demonstrated concerns raised by electronic medical records need to be addressed in the system of records notice.

b. HIPAA Compliance Should Be Clarified.

A step towards addressing the medical privacy concerns addressed above is to clarify how the system of records comports with established medical privacy regulations. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 directed the Department of Health and Human Services (HHS) to issue privacy regulations if Congress did not enact privacy legislation within 3 years.[25] After the time limit, HHS enacted a final rule and modification, now codified at 45 C.F.R. parts 160 and 164. Generally, the rules prescribe that covered entities must not disclose individually identifiable medical information.[26] The only mention of HIPAA in the System of Records Notice is in the records disposition section.[27] The section simply says that records covered by HIPAA will be moved to Washington National Records center 2 years after the end of the response activity, and will be destroyed in 75 years. [28]

According to the information in the System of Records Notice, NDMS is a covered entity if they are making certain electronic transmissions. Covered entities include a health care provider who transmits any health information in electronic form in connection with certain transactions.[29] Healthcare includes preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care.[30] NMDS teams provide both physical and mental healthcare.[31]

---

[18] California Healthcare Foundation, 2005 National Consumer Health Privacy Survey Executive Summary 4, (Nov 2005), *available at* http://www.chcf.org/documents/ihealth/ConsumerPrivacy2005ExecSum.pdf.
[19] *Id.*
[20] *Id.*
[21] The Gallup Organization for Institute for Health Freedom, Public Attitudes Towards Medical Privacy (Sept. 26, 2000) *available at* http://forhealthfreedom.org/Gallupsurvey/IHF-Gallup.pdf.
[22] *Id.* at 9.
[23] *Id.* at 11.
[24] *Id.* at 14.
[25] Pub. L. No 104-191, § 261-64, 110 Stat. 1936, 2021- 2034 (1996).
[26] 45 C.F.R. 164.502(a)
[27] NDMS Notice, *supra* note 1 at 35,054.
[28] *Id.*
[29] 45 C.F.R. § 160.103 (covered entity).
[30] 45 C.F.R. § 160.103 (healthcare).

NDMS keeps electronic copies of the information they collect[32] and collects health information (including all treatment information).[33] Although there is no mention of whether the information must be shared electronically, the notice does allow NDMS to transmit relevant data in a manner that is a transaction as defined by HIPAA.[34] Covered transactions are those that carry out financial or administrative activities related to health care. [35] Routine use disclosure #5, which includes disclosure for the purpose of determining benefit status,[36] falls within that definition.

At least some of the data is covered by HIPAA. The records disposition section of the notice discusses medical records covered by HIPAA.[37] Under HIPAA, protected data is defined as: individually identifiable health information that is transmitted by electronic media.[38] To be individually identifiable, the data must be a subset of health information that includes "demographic information collected from an individual," and it must identify the individual or provide a reasonable basis to believe it can be used to identify the individual.[39] The data proposed for collection under the NDMS includes but is not limited to: patient name; medical treatment history; preexisting conditions; address; contact information; gender; insurance information; and all treatment information (medications, diagnosis, and symptoms).[40]

Some of the routine use disclosures appear to raise HIPAA problems, while others appear compliant. Several of the disclosures are for treatment or billing purposes, which generally do not require patient consent.[41] Disclosure 6, which gives "location or the status" of a patient to family members, is not information needed for treatment or billing purposes.[42] Patient "status" will include individually identifiable health information which is protected data. [43] Generally, this release requires patient consent if it is not for treatment or billing purposes. [44] Lastly, the disclosure of location, under routine use 5(c) and 6, generally requires that an individual be given an opportunity to agree or object.[45] NDMS may have exceptions under HIPAA regulations that permit these disclosures, such as the release of health information to disaster relief entities.[46]

EPIC recommends that the interaction between HIPAA and the NDMS system of records, including the proposed routine uses, be further described in the system of records notice. This description should analyze under what HIPAA provisions the routine uses are being made.

c. Routine Use Disclosures Should be Cabined by HIPAA and Limited to Medical Uses.

---

[31] NDMS notice, *supra* note 1 at 35,052.
[32] NDMS notice, *supra* note 1 at 35,053.
[33] NDMS notice, *supra* note 1 at 35,053.
[34] NDMS notice, *supra* note 1 at 35,054 (Routine Uses of Records Maintained in The System)
[35] 45 C.F.R. § 160.103 (transaction).
[36] *Id.*
[37] NDMS notice, *supra* note 1 at 35,054.
[38] 45 C.F.R. § 160.103.
[39] *Id.*
[40] NDMS notice at 35053 (Categories of information collected).
[41] 45 C.F.R. § 164.506(a)(2).
[42] NDMS notice, *supra* note 1 at 35,054.
[43] 45 C.F.R. § 160.103.
[44] 45 C.F.R. § 164.506(a)
[45] 45 C.F.R. § 164.510(a).
[46] 45 C.F.R. § 164.512(b)(4).

Privacy Act enforcement procedures will help to assuage privacy concerns and allow individuals some control over their data. As noted above, describing the interaction with HIPAA will improve the public's understanding of the privacy practices of this system of records. This understanding is complemented when individuals have an ability to enforce their privacy preferences. As before, the exceptional nature of when and how this data is collected -- emergency treatment and during disasters -- means that great care should be taken to protect individual privacy. This care should be provided via the Privacy Act.

EPIC recommends that the system of records notice be revised to explicitly note that disclosures in violation of HIPAA are not covered as routine use disclosures. Disclosures in violation of HIPAA will therefore not be authorized without consent because they will not be "routine use" disclosures. Individuals then will have some method of redress when these improper disclosures are made.

Furthermore, under routine use #1, the Department of Defense, Veteran's Administration, and Department of Homeland Security will have access to the data.[47] Their uses of this data should be limited to the medical needs of the patient. Individuals should be able to expect that their privacy will be protected by these other agencies at least to the same level as HHS. Therefore routine use #1 should include a limitation that these agencies may not use this data outside of their NDMS function, and that they may not make any other disclosures of it.

The need to ensure full compliance with the Privacy Act is well established. In enacting the Privacy Act, Congress found that:

> (1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies
> (2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;
> (3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems'
> (4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and
> (5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.[48]

In passing the Privacy Act, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[49] The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[50]

---

[47] NDMS Notice, *supra* note 1 at 35,054.
[48] Pub. L. No. 93-579, 88 Stat. 1896 (1974).
[49] S. Rep. No. 93-1183, at 1 (1974)
[50] *Id.*

As the HHS acknowledges in the notice, "the Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates personally identifiable information."[51] One of the principles of fair information is that of enforcement.[52] One of the ways that the Privacy Act embodies enforcement is by providing for civil remedies for an agency's failure to comply with the act or rules in a manner that has an adverse effect upon an individual.[53]

An individual therefore has an ability to have civil enforcement against some improper disclosures. Improper disclosures include those that are not described as "routine uses" in the system of records notice. [54]

d. Other Established Sources of Medical Privacy Point to Need for Privacy Protection.

The federal constitution, state laws, and professional code of ethics also point to privacy protections. NDMS should comport with the Constitutional right to information privacy. In *Whalen v. Roe* the Supreme Court considered a New York database of medical prescriptions.[55] The database combined all prescriptions for certain dangerous but still medically legitimate drugs.[56] Hard copies were kept in a vault and destroyed after five years.[57] When the data was accessed from electronic storage, the computer was offline so no other access could be made.[58] Disclosures were prohibited and sanctioned by criminal penalties. [59] Only seventeen employees had access to the computer records.[60] These privacy features contrast with the NDMS system of records. The NDMS system contains comprehensive medical information,[61] not just dangerous prescriptions. The NDMS data is disclosed to a variety of state and federal agencies,[62] as opposed to just a few staff and investigators at once

The *Whalen* Court permitted the database to continue, noting however that "[t]he right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures."[63] NDMS should limit its disclosures of this information to the purpose of medical treatment. For example, routine use disclosure #1, to DoD, VA and DHS[64] should be clarified to limit the disclosure to those agencies to be for consented patient treatment uses only. Those agencies should not make further uses of the information, as these are unwarranted for the public purpose of the NDMS: disaster treatment.

---

[51] NDMS Notice, *supra* note 1 at 35,052.
[52] U.S. Dep't of Health, Educ. & Welfare, *Records, Computers and the Rights of Citizens,: Report of the Secretary's Advisory Comm. On Automated Personal Data Systems,* 40-41 (1973), *available at* http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm [hereinafter HEW Report].
[53] 5 U.S.C. § 552a(g)(1)(D).
[54] 5 U.S.C. § 552a(b).
[55] 429 U.S. 589 (1977).
[56] *Id.* at 592-3.
[57] *Id.* at 594.
[58] *Id.*
[59] *Id.* at 594-5.
[60] *Id.* at 595.
[61] NDMS Notice, *supra* note 1 at 35,053-54.
[62] NDMS Notice, *supra* note 1 at 35,054.
[63] Whalen v. Roe, 429 U.S. 589, 605 (1977).
[64] NDMS Notice, *supra* note 1 at 35,054.

Many states have medical privacy laws that limit the use and disclosure of patient health records. Often these laws are more comprehensive than the limited privacy protections found under HIPAA. For example, California's Confidentiality and Medical Information Act[65] governs the disclosure of medical information by health care entities as well as employers and it allows patients to restrict the use of their medical information pursuant to individual authorization.[66] The Confidentiality of Medical Records Act for Maryland also has an express authorization requirement.[67] In an emergency situation, individuals who reside in states with more comprehensive medical privacy laws may expect different privacy protections. To meet these privacy expectations, the uses of the data beyond immediate patient need should be limited.

The practitioner community has a code of ethics that govern their interactions with patients. A doctor's first responsibility is their patient.[68] Doctors should also safeguard patient confidences and privacy.[69] Lastly, doctors have a responsibility to seek changes in the laws that are contrary to the best interests of the patient.[70]

Because this code of ethics exists, patients expect doctors to safeguard their privacy. Under the NDMS system, physicians providing emergency care are entering patient data into a system of records that may make disclosures against the wishes of patients.[71] This is in tension with a doctor's code of ethics and may compromise the care received by individual patients. Good care requires that patients be forthcoming with their medical information. They may choose not to disclose relevant health information if they are concerned that their doctor's responsibility will be to a system of records, rather than the patient. An example of this concern is the broad disclosure to several agencies in routine use #1.[72] Instead, disclosure #1 should be limited to the initial emergency treatment situation.

IV. Protecting the Privacy of Domestic Violence Survivors.

Some of the routine use disclosures in the notice threaten the privacy of domestic violence survivor's personal information. Estimates range from 1 to 3 million incidents of domestic violence a year.[73] A count of 62% of the local domestic violence programs revealed that 47,000 adults and children sought and received services in a single day.[74] These statistics make it likely that patients treated under NDMS will also be domestic violence survivors.

Survivors and policymakers make continuous efforts to maintain certain information private. Those who fear victimization at the hands of their abusers should not have to withhold

---

[65] *See* Cal Civ. Code § 56.
[66] Cal. Civ. Code § 56.23.
[67] Md. Code Ann., Health-Gen. § 4-303(b).
[68] *See* Principles of Medical Ethics, American Medical Association, *available at* http://www.ama-assn.org/ama/pub/category/2512.html.
[69] *Id.*
[70] *Id.*
[71] NDMS Notice, *supra* note 1 at 35,054.
[72] *Id.*
[73] Family Violence Prevention Fund, *The Facts on Domestic Violence*, 1 http://www.endabuse.org/resources/facts/DomesticViolence.pdf.
[74] National Network to End Domestic Violence, *Domestic Violence Counts: A 24 Hour Survey of Domestic Violence Shelters and Services Across the United States*, 2 (2007), *available at* http://www.nnedv.org/census/DVCounts2006/DVCounts06_Report.pdf

the information they need to get proper care, nor turn away from the services of the NDMS for fear that their information will be used against them.

a. Domestic Violence Survivors and State and Federal Policymakers Recognize The Need for Privacy Protections.

Survivors take care to maintain their address and other information confidential. State and federal policymakers have also recognized the privacy needs of these individuals. The NDMS should as well.

Several states have formal programs to protect the location information of domestic violence survivors. Currently, twenty states provide address confidentiality programs for domestic violence survivors.[75] Generally, an individual in these programs will register with their state attorney general or secretary of state. The individual is provided with an address at that state office, which forwards correspondence to the individual. The state office address is used in official correspondence, and may be used by businesses. In this manner, individuals can protect their location information from an abuser. Some states also permit individuals to use a non-residential address on their driver's licenses: California,[76] Florida,[77] Montana,[78] New Mexico,[79] Oklahoma,[80] and Virginia.[81] Domestic violence survivors use these provisions to protect their addresses.

Congress has taken steps to protect the location and other personal information of domestic violence survivors. In the Violence Against Women Act (VAWA)[82] Congress ordered the postal service to issue regulations to secure the confidentiality of domestic violence shelters and abused person's addresses.[83] Congress also ordered the Department of Justice to prepare a report on the confidentiality of the addresses of victims of domestic violence.[84] When VAWA was reauthorized in 2005 it contained specific provisions to protect the personal information of domestic violence survivors.[85] VAWA 2005 requires recipients of grants to maintain confidential the information on domestic violence victims they serve.[86] Congress further prohibited personally identifiable data on domestic violence victims from being entered into Homeless Information Systems databases.[87] Lastly Congress prohibited the disclosure of information on certain applicants for visas used by victims of domestic violence.[88]

---

[75] *See* Nat'l Conference of State Legislatures, *States With Address Confidentiality Programs for Domestic Violence Survivors,* http://www.ncsl.org/programs/cyf/dvsurvive.htm (listing 19 states, not including the recent program in Maryland). *See also* Maryland Safe at Home Address Confidentiality Program, http://www.sos.state.md.us/ACP/Information.htm.
[76] Cal. Veh. Code § 12811(a)(1)(A).
[77] Fla. Stat. Ann. § 322.14(1)(a).
[78] Mont. Code. Ann. § 61-5-111.
[79] N.M. Stat. Ann. § 66-5-15 (1978).
[80] Okla. Stat. Ann. tit. 47, § 6-111(A)(1).
[81] Va. Code Ann. § 46.2-342(A1).
[82] Pub. L. No. 103-322, § 40001-40703, 108 Stat. 1796, 1902-1956 (1994).
[83] *Id*. at § 40281, 1938.
[84] *Id*. at § 40508, 1950.
[85] Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, 119 Stat. 2960 (2005).
[86] *Id*. at § 3, 2969-70
[87] *Id*. at § 605, 3041.
[88] *Id*. at § 817, 3060-61

Domestic violence advocates have noted the concept of separation violence.[89] Separation violence refers to incidents of violence perpetrated after separation, after the victim has left the abuser. As many as 75% of violent incidents occur after separation.[90] Thus the need for confidentiality of the location of a separated victim is of paramount importance.

These dangers, and demonstrated concerns of federal and state policy, show that it is unwise and dangerous for HHS to assume that a disclosure to a family member can be called "routine" or can be done without the consent of the patient.

b. Location Information Disclosures Should Be Made Only with Patient Consent.

As noted above, the Privacy Act embodies fair information practices. A further one of these is purpose limitation, that an individual must have a way to prevent information gathered for one purpose from being used for another purpose without their consent.[91] Consent-based purpose limitations have two main benefits for this system. First, they place the control of the information flow in the hands of the patient. Second, they free the NDMS from having to determine whether a person is a victim of domestic violence and whether the disclosure is proper. Instead NDMS can rely on the patient's control.

In practice, consent has meant that an "opt-in" or "opt-out" structure should be used to allow individuals to control how their information is used. Under an opt-in structure, disclosures of location and status would only be made to those individuals or entities that the patient has specifically indicated. In the face of silence from the patient, no disclosures could be made until affirmative consent was achieved. Under an opt-out structure, disclosures can be made per the current routine uses. However, patients must be meaningfully informed of this. After being informed, a patient may request that a disclosure not be made, say to a particular individual or entity. Following this request no further disclosures may be made if they have been disallowed by the patient.

EPIC recommends an opt-in structure. Under an opt-in structure there is a greater incentive to inform the patient of the purpose of the disclosure, and it makes the consent achieved more meaningful. Due to the nature of this data collection -- under tumultuous disaster conditions -- notions of implied consent should be limited. Instead, express permission should be sought in order to allow patient control of their information.

Regardless of which structure is chosen for consent, EPIC recommends at least some form of purpose limitation. A purpose limitation like this will allow domestic violence survivors to control their information and thus control their safety.

V. Conclusion.

The System of Records needs to protect medical privacy as well as the privacy of domestic violence survivors. Fair Information Practices, embodied in the Privacy Act, provide the solution for this privacy protection.

---

[89] *See* Separation Violence, http://www.aardvarc.org/dv/sepviolence.shtml.
[90] *Id*. citations omitted.
[91] HEW Report, *supra* note 52 at 41-42.

EPIC stresses that individuals have a strong medical interest in providing full information to NDMS in order to gain adequate treatment. Their decisions about disclosures will be made in disorienting disaster situations. In this setting, privacy interests should be protected to the utmost, so that individuals are not forced to trade off their privacy interest with their medical interest.

Specifically, EPIC recommends that the System of Records Notice be amended in the following manner:

- HIPAA compliance should be spelled out in the notice.
- The notice should make clear that there will be no "routine uses" that are in violation of HIPAA.
- The notice should make clear that the Department of Defense, the Department of Veterans Affairs, and the Department of Homeland Security may not use the data in the NDMS for purposes unrelated to patient treatment.
- Disclosure of patient status and location to family members or those acting on behalf of patients should be done only with the explicit consent of the patient. Preferably this should be done with an opt-in system, rather than an opt-out.

Respectfully submitted,

Marc Rotenberg
Executive Director
Electronic Privacy Information Center
1718 Connecticut Ave NW, #200
Washington DC, 20009
http://www.epic.org/
(202) 483-1140 (tel)
(202) 483-1248 (fax)

Lillie Coney
Associate Director

Guilherme Roschke
Skadden Fellow

Evan Stern & Aleah Yung
IPIOP Clerks

July 26, 2007