TESTIMONY OF NICOLAS P. TERRY

"Electronic Health Records and Privacy"

NCVHS Subcommittee on Privacy

Hearings on Privacy and Health Information Technology

August 16-17, 2005

Hotel Monaco

501 Geary Street

San Francisco, CA 94102

Nicolas P. Terry

Chester A. Myers Professor of Law

Co-Director, Center for Health Law Studies

Co-Editor-in-Chief, Journal of Health Law

Saint Louis University School of Law

3700 Lindell Blvd., St. Louis, MO. 63108

Voice, 314-977-3998

Fax, 314-977-3332

Email: terry@slu.edu

I. Introduction

My name is Nicolas Terry. I am the Chester A. Myers Professor of Law and Co-Director, Center for Health Law Studies at Saint Louis University School of Law. I thank the subcommittee for this invitation to testify on some of the privacy and confidentiality implications of Electronic Health Record (EHR) models.

I pay tribute to the continuing leadership of NCVHS in recognizing and promoting the vital role of HIT in reducing error, improving efficiency, and better involving patients in the healthcare process.

In the course of this narrative I have sought to answer the specific questions posed by the subcommittee. In the attached Appendix to this testimony I include specific, detailed responses to those questions.

II. Patient and Physician Perceptions

Medical literature, opinion polls, UK and Australian EHR findings, and our own experiences (and interactions) suggest that patients and physicians are skeptical about the privacy, security, and safety of HIT systems. Consumers are told on almost a daily basis that their computers, particularly when attached to networks, are pathologically insecure. Physicians continue to push back on safety technologies and remain deeply suspicious (even resentful) of the HIPAA transactional and patient privacy constructs.

Recent media reports have informed us of stolen laptop computers containing medical data, the theft of a computer disk containing medical and financial information relating to 200,000 patients, the hacking of HIT systems, a disgruntled ex-employee of a managed care corporation linking her blog to the medical information of 140 patients, the theft of computer backups containing the personal information of 57,000 health insurance customers, hospital executives and security guards running through the streets to retrieve 3,000 patient records that fell from a truck and blew away, and the targeting of hospital and nursing home patients by identity thieves.

A rational policymaker may view these issues as merely transitional or as aberrations that are statistically insignificant. Yet public and professional perceptions of an EHR system are far different and potentially corrosive. The very nature of such a system is difficult to convey to the general public. A public perception of an EHR as a governmental "big brother" is extremely probable.

Recently, the HHS Office of Civil Rights added the following question to its HIPAA privacy FAQ, "Does the HIPAA Privacy Rule create a government database with all individuals' personal health information?" OCR's cogent and straightforward answer

to the possibly paranoid questioner was, "No. The Privacy Rule does not create such a government database or require a physician or any other covered entity to send medical information to the Federal government for a government database or similar operation." The difficulty, of course, is that once an interoperable EHR is in place the answer to this question will, of necessity, have to be far more nuanced.

AHRQ Director Dr. Carolyn Clancy has testified before Congress, "Unlike the baseball field in the movie Field of Dreams, we have dramatic examples of the building of health IT systems, whose designers found physicians and other clinicians neither came nor played."[1] If patients do not trust our EHR construct they will hide even more information from their doctors than they do today. And doctors will reduce or become more circumspect in their charting.

III. EHR Architectures

As the members of this NCVHS sub-committee are all too aware, the journey into the world of HIT is hindered by overlapping terminologies; a journey that is not eased by the alphabet soup of acronyms that litter the topology. For the purposes of examining issues of privacy and confidentiality I believe it is helpful to distinguish between five different EHR architectures. I label these as "Personal," "Shared," "Trustee," "System-wide," and "Interoperable." This final "Electronic Interoperable Health Record" (EIHR) category captures RHIOs or a NHIN. The architectures are discussed in an ascending order that reflects their impact on personal privacy.

A. Personal

In this scenario the patient is the dominant custodian; it is a patient-centric model. The data may be added to a web-based system by the patient and/or supplied by way of data export from something like the "Continuity of Care" record. One way to conceptualize a patient's interaction with such a system is to think of the financial software (Intuit's "Quicken" or Microsoft's "Money") used by millions of financial services customers. Say the consumer has 11 different bank accounts (the average number of siloed health records for U.S. residents). Only the consumer can download, view, combine, or process all those records. In the EHR context the patient would then be able to choose which records or parts of records he or she would export to a requesting physician.

[1] Testimony of Dr. Carolyn Clancy, Director of the Agency for the Healthcare Research and Quality, U.S. Department of Health and Human Services, Technology, Innovation, and Competitiveness Hearing: Health Information Technology, Senate Subcommittee on Technology, Innovation, and Competitiveness, June 30 2005, *at* http://commerce.senate.gov/pdf/clancy.pdf.

B. Shared

Here physicians retain control over their records silos; it is a physician-centric model, albeit one that likely will involve consultation with patients. The silos (individual EMR systems) are not interoperable (i.e., today's state). A physician, in consultation with his or her patients (and subject to the palette of opt-in, opt-out, etc., consents) could transmit all, parts, or a summary of such a record to another physician or to a data warehouse containing a centralized record. The most obvious example of this type of EHR is the Australian *HealthConnect* system.

HealthConnect does not create a true longitudinal record, but aggregates elements extracted from a patient's existing EMR(s). The elements extracted are known as "event summaries," defined as "electronic overview of a visit to a doctor or hospital, or some other health care event [containing] only the information that is relevant to the future health and care of the consumer, rather than the comprehensive notes that a doctor may keep as a record of a consultation."

HealthConnect utilizes a "push" model whereby data is sent from the local EMR to a centralized HealthConnect record, in contrast to a "pull" model generally associated with EIHRs, RHIOs, or a NHIN.

C. Trustee Model

A trustee model is an offshoot of a Personal EHR in that the data is in the control of the patient who then pushes all or some of the data to a trusted third party. The trustee could be a data warehouse or could be a "pointer" repository. The patient would set the terms of the trust, instructing the trustee about the management of that information, including to whom it may be disclosed, how long it may be kept, and who may add to the record. Such a model could also be an offshoot of physician-centric architecture in that the physician, in consultation with the patient, could initialize the "push" directly from his EMR to the trustee.

It is unclear how the dissemination or processing of the patient's data is controlled or limited after the trustee makes an authorized transmittal to the patient's (next) caregiver. One model would be for the information to then flow into that doctor's record. Another would be to limit the data to read-only (or use some other form of digital rights management) such that the control of the data remains with the trustee (and within the terms of the trust agreement).

D. System-wide

A system wide or institutional system is not an EHR in the strictest sense but an EMR adopted by (typically) a large system. It is an information silo, but a very large one. For its long-term patients it will capture longitudinal data that equates to data in an EIHR/NIHN. Examples include Kaiser Permanente, the largest non-profit HMO in the United States (KP HealthConnect) and the Department of Veterans Affairs (VistA).

For the purposes of our current discussion such systems have at least two noteworthy characteristics. First, the data in such a system is of immense value to the system and may not be willingly shared given the marginal nature of any additional patient information that may be received in return. Second, assuming the "closed" but system-wide warehouse is secure and subject to internal restrictions on data processing, systems may view opening up their EMRs to regional or national interoperability as reducing their data security/confidentiality to the level of the "weakest link" with which their data is shared.

E. EIHR

A fully longitudinal, interoperable EHR (EIHR), whether operating at a regional (RHIO) or national (NHIN) level, has the most fundamental implications for patient privacy, confidentiality, and security. EIHR discussions suggest that a RHIO or NHIN could utilize either a data warehouse or pointer/records locator technical model. These models may have different security implications, but they pose almost identical privacy and confidentiality issues.

An EIHR model is premised on the aggregation of existing EMR silos, common data standards, and (to improve usability and maximize the return on EMR/EHR investments) sophisticated data mining tools.

Making patient safety information available to all healthcare providers that are even tangentially involved in a patient's care renders the level of privacy and security accorded that data a function of the weakest link in the system. Fully interoperable data is also immeasurably more valuable for secondary uses (e.g., marketing) and is an irresistibly tempting target for commercial aggregators.

IV. Privacy & Confidentiality Laws

U.S. legal and regulatory systems utilize two basic models for the protection of personal information; *privacy* (collection control), and *confidentiality* (disclosure control).

A privacy model places limitations on data *collection*. Such a model could, for example, prohibit all collection in certain circumstances (e.g., the harvesting of genetic information by life insurers) or limit collection via a proportionality rule (e.g., only information necessary for the purposes of treatment). In the healthcare arena U.S. limitations on data collection are less than robust. For example, the Restatement's black-letter law of "privacy"[2] promises far more than it delivers. It fails to provide any general or comprehensive "right of privacy" and is no more than a listing of modest protections—nominate and discrete tort actions applicable in a narrow range of circumstances rather than fact-sensitive applications of a general principle or theory of privacy. Of these nominate actions only the protection against "unreasonable intrusion upon the seclusion of another" is in any way applicable to the patient-provider relationship. However, this seclusion-based privacy action has seldom been applied to the health domain and its doctrinal elements have limited its applicability to outlying cases.

The second protective model is to place limitations on data *disclosure* (e.g., hospital records may be disclosed to physicians but not drug companies). In contrast to collection-centric rules, this protective model, whereby limitations are placed on data *disclosure*, is well established in U.S. law. Although frequently described in terms of "privacy" and "privacy law," the legal protections applied to patient health information by the common law, state statutes, or the HIPAA federal standards have very little to do with either. Aside from the few "intrusion upon the seclusion" actions, the modern law of health "privacy" resides in the far narrower, disclosure-centric doctrine captured in cases, statutes, and regulations dealing with *breach of confidence*. A patient *exercises* his right of privacy (as recognized by the ethical domain) when he chooses to provide information to his physician (albeit a "right" that is illusory if it is a condition of treatment). Thereafter, dissemination of that information by the physician is limited by ethical *and* legal standards of confidence. Today, when courts and regulators speak of medical "privacy" they are usually in error, mislabeling obligations of "confidentiality."

Long before the promulgation of the federal standards, most states had developed common law and statutory protections applicable to the confidentiality of health information. Languidly, the courts articulated a cause of action for breach of confidence. The development of the common law of confidentiality has been "distinguished" by quite arcane discussions as to the correct doctrinal basis for protecting patient confidences (including implied contract, breach of a fiduciary relationship, and even "privacy"). Only recently could it be said that "[s]lowly and unevenly, through various gradations of evolution, courts . . . moved toward the inevitable realization that an action for breach of confidence should stand in its own right, and increasingly courts have begun to adopt it as an independent tort in their respective jurisdictions."[3]

---

[2] RESTATEMENT (SECOND) OF TORTS § 652A(2) (1965).

[3] Biddle v. Warren Gen. Hosp., 86 Ohio St.3d 395, 715 N.E.2d 518, 523 (Ohio 1999).

Generally, state statutory models have been more successful in reflecting the realities of modern healthcare delivery and the particular issues posed by informational privacy. Although still generally limited to a disclosure-centric approach (and, unfortunately, also mislabeled as going to *privacy* rather than *confidentiality*), these statutes have tended to be more comprehensive and coherent than their common law progenitors. Such statutes frequently are more explicit in extending the duty of confidence to the myriad of providers and insurers involved in modern healthcare delivery. These state "privacy" statutes, however, have not supplanted the common law action for breach of confidence, primarily because the legislation in most states does not permit a private right of action by patients.

The HIPAA federal standards apply to a broad range of "covered entities"[4] including, for example, health, but not life, insurers. These providers,[5] such as hospitals, physicians, and health plans, are subject to the regulations if they transmit health information "in electronic form in connection with a [HIPAA-EDI transaction]."[6] The federal standards place limitations on the disclosure of "protected health information,"[7] including information that "relates to the past, present, or future physical or mental health or condition of an individual"[8] and identifies or could identify the individual.[9] Thereafter, the provider may only disclose private health information (PHI) as permitted by the federal standards.[10] Modeled, as they are, on existing state statutory protections the HIPAA standards do not protect health privacy. The standards are in essence a federal *confidentiality* code.

V. EIHR Privacy & Confidentiality Models

These privacy and confidentiality models for EHRs primarily are addressed in the context of an EIHR (NHIN or RHIO). However, most of the models discussed also have potential applicability to all non-Personal EHR architectures, such as Physician-centric and Trustee types.

[4] 45 C.F.R. § 164.502(1).

[5] Defined in 45 C.F.R. § 160.103.

[6] 45 C.F.R. § 160.102.

[7] 45 C.F.R. § 164.501.

[8] 45 C.F.R. § 160.103.

[9] 45 C.F.R. § 164.501.

[10] 45 C.F.R. § 164.502(a).

A. General Data Carve-outs

The U.S. privacy-confidentiality legal model has generally endorsed the approach that *any and all* personal information (be it financial, medical, etc.) may be collected, processed, and disseminated *if* the data subject consents to/authorizes same.

The primary operational objection to this approach is that "consent" processes are imperfect in situations involving parties with radically different bargaining strengths and in informational asymmetry regarding the implications of any such consent or authorization.

Legislation could carve-out some forms of data collection or dissemination that would improve trust in an EIHR. For example, federal legislation could prohibit employer or insurer access to patient-specific genetic information, collection of RFID data from patients outside of a healthcare provider's premises, and secondary uses or commercial aggregation of patient-specific information.

B. Patient-Specific Non-Participation

An EHR system may permit patients to decide whether or not to participate in any way in an EHR system. While an "opt-in" model is most consistent with patient autonomy the practical, processing implications likely would overwhelm the system. An "opt-out" model likely would be more operationally friendly. Legislation would be required to eliminate discrimination against patients who opt-out.

C. Patient-Specific Data Carve-Outs

Assuming a patient opted-in or declined to opt-out of general inclusion in an EMR, the patient could still be given rights to carve-out certain types or uses of data in the system. There are three models that could be adopted; a secure "envelope," limiting disclosure by context, and an access-edit model.

1. Secure "Envelope"

This model assumes that the patient opts-in to the system (or is not given the choice) but is permitted to tag specific data as, say, "highly confidential." This data is then specially coded (e.g., with a DRM layer) and, although it circulates within the EIHR along with the patient's other health data, it is not generally readable. The secure "envelope" could only be opened with a specific additional consent from the patient or in the case of a particular medical interaction. Examples of the latter might include: "To be

opened if I'm unconscious in an ER," "To be opened if I have a OB/GYN emergency," or "To be opened if psychotropic medications are to be prescribed."

Research would be required to determine how the conditions "on" the envelope could be coded so that they do not defeat the exercise by, for example, hinting at the secure data contained within the envelope.

2. Contextual Disclosure

Context-specific disclosure requires the patient (likely in consultation with his provider) to create different "layers" of health information that are made available to the EIHR. These layers would then provide for context-specific disclosure. For example, OB/GYN-related data would only be available to that sub-class of providers, or existing prescriptions of certain classes of medication (e.g., psychotropics) would only be disclosed to treating psychiatrists.

Research would be required to determine the impact on such limitations on health quality or medication safety. For example, if a patient was taking Lithium and presented at an ER following an overdose, absent knowledge of the medication or underlying diagnosis, the patient would be at extreme risk as there is no screening test for detecting Lithium. Similarly, if medication data pertaining to sexual dysfunction were limited to treating urologists, ER physicians would be unable to safely treat cardiac chest pain.

Patient-initiated carve-outs aside, an EIHR system likely would have to be coded for some "layer" restrictions on data because of existing restrictions on the transparency of data involving, for example, HIV/AIDS or child abuse.

3. Access and Edit

Envelope storage or context restrictions generally are discussed in the context of restrictions placed on the data at the time of input. However, similar rights could be given to patients using an Access/Edit model similar to that used by the HIPAA standards or some state statutes. Thus, a patient could be permitted to access his record, and remove (request removal) of specific data, or place restrictions on its dissemination (e.g., by specifying a context or moving it to a secure envelope).

D. Proportionality Limitation

As discussed below, existing U.S. confidentiality provisions do little to limit the dissemination of patient-specific health information within the health domain. That is,

once the data is entered it is freely available to health care providers. Patient confidentiality would be better served if the data and its dissemination were subject to a limitation based on necessity or proportionality. For example, a "privacy" rule could limit the collection of patient data to that required for the contemplated procedure. Equally, a "confidentiality" rule could limit the dissemination of the patient data to those providers directly involved in the patient's current treatment—restricted to the "circle of care."

VI. Revisiting HIPAA in the EIHR Context

I am aware that this is not the occasion to debate the merits of HIPAA. Nevertheless the sub-committee should be aware of some general and specific issues with the current federal confidentiality code that may adversely impact patient and physician trust (and hence participation) in an EIHR.

Unfortunately the federal standards are flawed and, as currently written, will do little to create trust in an EIHR. First, the standards concentrate almost exclusively on the *process* of patient consent to disclosure. A true privacy-confidentiality regime should be more *substantively* concerned with limiting the collection and dissemination of personal health information. Only at the margins should questions of patient consent to disclosure need to be addressed.

Second, the standards now lack any consent-to-disclosure provision for most healthcare activities, thus, denying a privacy-autonomy "moment" at the commencement of the provider-patient relationship.

Third, although HIPAA confidentiality is premised on national standards, this model is undercut by the confusing and operationally obstructive "more stringent" partial preemption rule, the so-called HIPAA floor.[11] The result is that simply establishing the applicable standard of health privacy protection in a particular state requires complex (and ongoing) analysis.

Fourth, the federal standards apply broad, arguably overbroad, exceptions (public health, judicial, and regulatory) where patient consent to data processing is not required.[12]

Fifth, the privacy standards are still too lax regarding secondary uses of patient information. There are still many unrestricted uses of patient information outside of treatment and billing; in too many situations patient consent for secondary uses is not required[13] and in other situations, consideration should have been given to prohibiting

[11] 45 C.F.R. §§160.202.

[12] 45 C.F.R. § 164.512.

[13] *See generally* 45 C.F.R. §§ 164.505, 164.508, 164.510.

some consented-to secondary uses (e.g., the sale of patient data for pharmaceutical marketing).

Sixth, because of limitations in the enabling legislation the federal standards could not simply include all medical data or all users of such data. There are gaps in the legislation caused by the "entities" or HIPAA-EDI premises that arguably deny protection to data held in some Personal or Trustee EHRs. Additionally, the "business associate" extension is a cumbersome and inefficient extension of the regulatory reach and of dubious effectiveness as EIHR data processing is moved offshore.

Finally, as we consider how to build patient and physician trust in an EIHR, one transcending problem with the HIPAA standards may have to be addressed. The standards are fatally flawed because they lack transparency and clarity. They may be labeled as promotional of "privacy" (of course, mislabeled because they deal only in confidentiality) but their sheer weight and obliqueness detracts from any educative or principled "message." What was required of the federal standards was a more generalized statement of principle based clearly on an autonomy-focused rationale; a legal guarantee that patients have control of their health information. And, as follows from earlier comments, exceptions should have been far more narrowly constructed and tightly controlled by concepts of proportionality and the circle of care.

VII. Conclusion

There is little doubt that a well-constructed, secure EIHR can improve the quality of our healthcare, reduce medical and medication errors, and provide a platform for patients to better understand and participate in their healthcare. However, progress towards these laudable goals has, so far, reflected institutional interests and priorities. It has been an example of "insider baseball," that has focused primarily on architecture and technical standards. As the debate is broadened to reflect the interests and participation of patients and physicians a principled, autonomy-based, and *simple* privacy-confidentiality structure must be articulated. Without such a structure patient and physician participation in the endeavor will be jeopardized.

I thank the members of sub-committee for their attention and trust that your questions will help me clarify my testimony.

Appendix: Specific Questions Posed

With respect to the design of a National Health Information Network (NHIN) do you prefer a model based on a regional health information organization, a model where individuals carry their own personal health information on a device, a trustee model, or something else? Why? What implications does your preferred model have for privacy and confidentiality?

This question captures one of the fundamental conflicts in the EHR arena. Intrinsically, the more inefficient a health records system—the more it is silo-based and makes interoperability (data exchange) difficult—the fewer privacy and security issues it will pose. However, from a patient safety perspective an EIHR (such as NHIN or RHIO) is vastly preferable to all other models because of its potential to reduce errors, improve quality, and promote outcomes research.

Within the population of EHRs other than EIHRs the confidentiality issues are at their lowest with Personal EHRs (Patient-centric). First, the data in Personal EHRs will not always be comprehensive (longitudinal), and seldom will be coded for interchange or interoperability. Second, a Personal EHR is, by definition in the control of the patient. A trustee model also has limited privacy and security implications in that it is the patient who decides what data is transferred to the trustee and agrees to a trust agreement that governs further distribution.

Of course, once any part of a Personal EHR or Trust EHR leaves the control of the patient and enters the control of a physician or system, more typical privacy, confidentiality, and security issues arise. However, Personal and Trust models could be designed (e.g., by incorporating digital rights management) such that recipient healthcare providers have read-only privileges. Liability and other concerns suggest that the recipient physician nevertheless would have to record some elements of the disclosed data in his patient record.

A fully interoperable records system, whether a RHIO or NHIN, creates the most fundamental privacy, confidentiality, and security problems.

What are the implications of permitting patients to control whether their records are part of the NHIN? If permitting this option is appropriate, what mechanism should be used to obtain individual consent or authorization?

This is an area that would benefit from additional research. The matrix is quite complex. First, an EIHR system might permit patients to keep all of their records out of an EIHR (i.e., an all or nothing choice) or to selectively keep some information out of the system. Second, there are a number of operational variables on participation depending

on patient choice models—e.g., opt-in or opt-out, envelope, or access/edit. Intuitively, it is be likely that patients will be less likely to opt-out than to opt-in. I am not aware of any research that suggests the levels of patient participation that could be anticipated using these different models. Neither am I aware of any research suggesting the level of patient participation that would be required in order to meet patient safety goals (either patient-specific or population-wide).

While consent/authorization is a valid model for determining patient participation it is not the only one. A hard line "privacy" rule could be used to exclude entire classes of data (e.g., genetic or RFID tracking). Further, a consent/authorization model is only valid if it involves real choice—non-participation should not lead to a lower standard of care.

What information, if any, should individuals be able to exclude from their electronic health record or the NHIN? What, if any, limits should apply to these exclusions?

Again, this is an area that would benefit from additional research. The literature refers to psychiatric presentations or ob-gyn records/events as typical. However, who will decide what information can be excluded? Will regulators list certain objective types of data that the patient may exlude/place conditions of dissemination on? Or will the individual patient have complete discretion? Will the class of excludable events be limited to treatment or medication types or could it include occasions of poor (in the patient's judgment) interpersonal interaction with a specific physician or provider?

What limitations, if any (beyond those of the HIPAA Privacy Rule) should be placed on access to personal health information in the NHIN? How should such limitations be developed and applied?

These are detailed in the section "EIHR Privacy & Confidentiality Models," above.

Should individuals have the option of having their health records maintained only in paper form?

Although siloed EMRs share some privacy and security issues with EHRs they are intrinsically more secure. The error reduction and cost savings inherent in EMRs overwhelm the risks associated with electronic rather than paper storage. Further, it is extremely unlikely that providers will exercise the same level of concern over an "old" technology while investing in EMRs. Also, records expertise for securing paper records will decline as EMRs take root. Finally, providers may refuse to accept paper records or,

if otherwise required to by force of law, will gradually lose the ability to integrate the data into their error-reducing systems, etc.

What other measures are needed to protect the privacy and confidentiality of personal health information and to build public trust in the NHIN?

Assuming movement towards a fully interoperable national EHR and full inclusion of patient and physician stakeholders in its development the most important measure would be a federal statute that overrides any consent/authorization regime and guarantees that certain types of private information cannot find their way into the EIHR. Second, a similar provision should lock out secondary uses and commercial aggregation.