HEALTH INFORMATION TECHNOLOGY EXCHANGE OF CONNECTICUT

Advisory Committee on Patient Privacy and Security Regular Meeting

MEETING MINUTES FOR
Wednesday, January 25, 2012
3:30 – 5:00 PM

Legislative Office Building, Room 1A
300 Capitol Avenue, Hartford

The meeting commenced at 3:40 p.m.

Committee members present:

Ellen Andrews, Steven Casey, Audrey Chapman, Michelle DeBarge, Ludwig Johnson, Robert McLean, and Demian Fontanella (for Victoria Veltri).

Members of the public wishing to acknowledge their attendance:
Sheldon Taubman, New Haven Legal Assistance Association
(illegible name), CT Legal Rights Project
Nicole Netkins-Collins, Advocacy for Patients with Chronic Illness
Susan Isreal, MD
Domenique Thornton, Mental Health Association (MHAC)

1. Approval of Minutes

The minutes were approved with the following changes requested by Ellen Andrews:

- Ellen Andrews expressed concern with the delay in appointing the Committee members and the delay between the enactment of the Committee's enabling legislation (effective July 1, 2011) and the first meeting of the Committee, January 11, 2012.

- Ellen Andrews emphasized the desire to have the Committee address at the outset the current consent model adopted by the HITE-CT Board and that the legislation enables the Committee to do so.

2. Presentation by Dave Gilbertson, CEO of HITE-CT

Dave Gilbertson gave an overview of HITE-CT, including the status of the work of the IT vendor (Axway), the HITE-CT's privacy and security and operational policies and procedures, and the work of the HITE-CT's committees. There was discussion and debate around how information will be exchanged, planned security features of the exchange, public and provider education, the State's consent model, and the process for HITE-CT decision-making to date. There was debate about the pro's and con's of the Connecticut consent model.

3. Discussion of Trends Regarding HIE Consent Model

In light of the debate during Dave Gilbertson's presentation about the pro's and con's of Connecticut's consent model, Michelle clarified again her view of the role of the Committee, which is to report to the HITE-CT Board on regional and national trends.

Michelle led off the discussion of regional and national trends regarding HIE consent models by summarizing her review of secondary sources in connection with regional and national trends:

> In general, the consent models are "all over the map." There are opt-in and opt-out as well as hybrid models across the country. One secondary source indicated the majority of consent models are opt-out, while another source indicated a trend toward opt-ins. The ONC Tiger team has not blessed any one model, but has recommended that consent must be "meaningful." There is also an eight-state HIE collaborative underway; the members are a mixture of opt-in and opt-out states, although the majority are opt-in. The National Committee on Vital and Health Statistics has made some recommendations around the definition and protection of "sensitive information." State law appears to have been a driver of the models' ultimately adopted; i.e., many opt-in states have laws in place that would not support an opt-out model. However, stake-holder interests, in addition to legal considerations, have also played a role.

Discussion followed with some Committee members emphasizing that the majority of states surrounding Connecticut have an opt-in model and that what State law permits should not be the only consideration. Further and extensive debate followed about opt-in versus the opt-out model and the importance of consent being "meaningful," with virtually no discussion about national and regional trends. Members of the public actively participated in the discussion.

4. Next Steps and Meeting Schedule

Michelle emphasized the need for the Committee to stay focused on its charge: assessing and reporting on trends rather than re-examining Connecticut's consent model as the main and overwhelming focus of the Committee's time, although discussion of Connecticut's model has its place in the broader review of trends. Some members of the Committee and the public expressed disagreement and again emphasized the desire to focus on the consent model, while other Committee members expressed support for the need to focus future discussions on regional and national trends.

Given the late hour, it was agreed that Michelle will circulate a proposed meeting schedule. Consensus was that the meetings should be on a consistent day/time each month and that monthly meetings, or meetings every two months, were in order.

5. Public Comment

Susan Isreal read portions of a statement/submission, which she asked to be included with the minutes. The submission is attached to these minutes.

6. Adjourn

The meeting was adjourned at 5:10 p.m.

1\301\2658926.1

January 25, 2012 Public Comment to the Advisory Committee on Privacy and Security

Re: Health Information technology Exchange of Connecticut, HB 6652, HB 6678, PA 10-117

The Human Services and the Public Health Committees had it largely right with SB 1147. Perhaps that law could be revisited.

It would seem that our right to privacy and ownership of our body's information has been sacrificed by the federal and state governments, in order to make it easier and more expedient for the insurers, providers and government agencies to service patients and supposedly for them to achieve better and cheaper care. We, patients, should be the ones to decide how much risk to our privacy we wish to take for our medical care, as amassing so much centralized data, inevitably puts the data at risk for breaches of all sorts. As a society, we need to guard against setting up mechanisms that could potentially be abused in ways that J. Edgar Hoover did with government data or as warned against by George Orwell. There are many ways in which medical data can be used against us, such as for employment, insurance coverage, etc. At this point, is there any technology that can guarantee keeping data from hackers or any laws that can totally protect data from misuse or breach? So patients must be able to choose which data, if any at all, should go into an electronic exchange. (Data left out could be indicated with an asterisk.) If HIE systems have to answer directly to patients to process their data, they will be more careful about maintaining their security and privacy systems.

In a nut shell, first, it is hoped that the consent policy of the HIE will be changed to one of Opt-in with *restrictions*, meaning that no data at *all* goes into the exchange for *any* purpose (treatment, payment operations (TPO), public health, research, quality control) without the consent of the patient. (Restrictions would mean that the patient can choose which of their data goes into the exchange. An all or nothing consent policy would make it easier for providers and the systems but would put patients over a barrel which can force them into the exchange.) And second, it is hoped that the legislation of CT will be changed to require only *unidentifiable* (not easy to achieve) data be sent to the Dept. of Public Health, except in very limited medical circumstances such as the reporting of tuberculosis and other very contagious diseases.

It seems that the current Opt-out policy means that patients can opt-out of their data being seen by providers, not opt-out of their data being seen by many other people without their explicit consent for treatment, payment, operations (see the long list of what is included), quality control, public health, research etc. It is not clear if patients can completely opt-out of their data being seen in an emergency, nor what will be the exact status of "sensitive" information (mental health, HIV status, substance abuse, etc.) in terms of it being seen by Public Health and during TPO access. Also it is not clear whether the intention is to send only the "meaningful use" data (problem list, meds, labs, allergies) or the whole patient record. There are also many concerns regarding the definition of a breach, the notification policies, and the technology mechanisms for security, etc.

As it stands now, a provider does not even have to grant a patient's request to keep their data out of the exchange totally or to keep some data private unless it is that specifically mandated by law. (Will abortion data be kept out of a women's OB-GYN record, as it is listed first in her record by a numbering

system that is standard to the record? Does everyone need to know her method of birth control?) A patient should not have to depend on their provider to control who can have access to their data or on their government to decide what is the acceptable risk of a breach to receive treatment. Once data is "outed," the damage is done.

Apparently, we have these threats to our privacy because in 1996, the HIPAA statute expanded law enforcement and public health access to patient data without their consent. Then in 2002-3, Health and Human Services ruled that patient data can be serviced and accessed by many business entities for providers and insurance companies without explicit patient consent, as long as they sign privacy agreements and are compliant with the HIPAA privacy regulations. The American Reinvestment and Recovery Act of 2009 (ARRA) and the Patient Protection and Affordable Care Act (PPACA)and CT legislation have further expanded what must be sent to Public Health and the federal government without patient consent. They currently mandate that "meaningful use" data of the medical record of Medicaid and Medicare patients go the federal government which hopes to have all patient data go to it, as part of the Nationwide Health information Network (NHIN) of which the HIE is a precursor. These uses of patient data may be legal, but are they constitutional? The government cannot search your house without a warrant, but can have access to one's most intimate private information without one's consent. I guess the laws are functioning as a global warrant on everybody.

As for the Connecticut laws, HB 6652, PA 11-61, Sec. 143, (b) mandates that hospitals send our "identifiable inpatient discharge data and emergency department data to the Office of Health Care Access" ... of the DPH and "may be submitted through a contractual arrangement with an intermediary;" (c) that at least some of our outpatient data be sent by 2015 as well, without our consent; (d) "The office may release de-identified data" which is not reassuring as even the federal government acknowledges data can be re-identified fairly easily; (e) the state Comptroller can access the data with permission. So this law seems to mandate that if I have a late term abortion, a private company may process my data and the CT Dept. of Public Health will have access to my most personal information. If it is determined that abortion is classified as "Sensitive" Protected Health Information (PHI), I do not know if it will go to the state in an identifiable form, but other diagnoses will surely go to the state. What about mental health admissions, will they go to the state as well?

HB 6678 PA 09-232 Sec. 7 calls for a tumor registry for all cancers. The state also wants occupational, demographic, etc. data. It is not clear whether this is identifiable data or not. However, (d) says that the DPH "may enter into a contract for the storage, holding and maintenance of the tissue samples under its control and management." So now the state of CT owns our body parts? What if the state rules or someone surreptitiously decides to do DNA testing on our tissue? Would patients even know as the tissue is out of their control?

The DPH website cites HB 6678 PA 09232 Sec. 74-77 as one of the laws underpinning their work. Sec. 77 (a) (1) (A) calls for an "electronic health record that provides access in real –time to a patient's complete health record," (D) "electronic alerts and reminders to health care providers to improve compliance with best practices, promote regular screening and other preventive practices, and facilitate diagnoses and treatments" and (F) tools to allow for the collection, analysis and reporting of data on adverse events,

near misses and the quality and efficiency of care, patient satisfaction and other healthcare-related performance measures." So does this mean that our State is going to oversee and monitor our treatment and in a sense be in the exam room with us and our providers? Would it be possible to do this without knowing our identities?

Also it is not clear from what has been written whether or not the HIE intends to just use "meaningful use" data or the whole medical record. The website also cites PA 10-117, Substitute Senate Bill 428, sec. 82 (e) says that the health information technology plan is for the "implementation of an integrated state-wide electronic health information infrastructure for the sharing of electronic health information among health care facilities, health care professionals, public and private payors, state and federal agencies and patients." So which state and federal agencies will have access to our medical records without our explicit consent, as the HIE will comply with "existing laws, i.e. Public Health"?

The DPH website under Policies and Procedures, Meaningful Use and Public Health explains that it will use the HIE according to the provisions in ARRA and the HITECH Act. It states that "meaningful use is defined in a specific way, requiring fifteen "core" and ten "menu" criteria. Of the ten menu options, three require reporting to public health:"

"Submit electronic data to public health immunization registries/systems."

"Provide electronic submission of reportable lab results to public health agencies" - This is a very long list, including lead levels, which goes way beyond communicable diseases. And it may mean that your teenager's sexually transmitted infection lab results will be reported directly to the CT DPH, probably in an identifiable form.

"Provide electronic syndromic surveillance data to public health agencies." - This could mean that identifiable patient data on weight, smoking, etc. will be seen by the DPH. How broad will the definition, of what medical data falls under surveillance, be without our consent?

So there are two arms of the consent model for the HIE that need to be addressed. One is the consent for use by providers, and the other is that for payment, operations, research and federal and state agencies. Please note that the HIPPA form, that patients are asked to sign, really just notifies patients that their data can be accessed by many business employees as long as they conform to the HIPAA privacy regulations. Most patients know that their doctor cannot talk to their mother without their consent, but they do not know that the doctor's accountant, for example, can see their record without their consent, as long as that person is a "business entity" conforming to HIPPA, which is, in fact, how the HITE-CT will be formatted.

Included is material from where I have taken quotations and other supporting material that underscore threats to our privacy involved in electronic health records.

Thank you very much for this opportunity.

Susan Israel, M.D. Susan Israel

BACK TO TOP

has been so little study of UPIs, it's difficult to say whether those fears are valid. But having patients decide which doctor gets which data is the wrong choice. Doctors need full access to all of a patient's data, so they can deliver the appropriate care. That is the essence of the doctor-patient covenant. Furthermore, in critical-care situations, the patient might be unconscious and, therefore, unable to grant access to essential health information.

While narrowing access isn't optimal for patient care, new UPI technology does make it possible. For example, one type of UPI could be used for patients who want all of their physicians to have broad access to their medical data, while another would indicate the patient must first authorize access. Patients get to choose.

Even with all these protections, not every person will trust the system. Studies show that many people already refuse testing and treatment because they are worried it could be used to discriminate against them. UPI critics say a universal health-care ID system will only undermine trust further, but I would argue the opposite is true. Problems related to misidentifying patients and accessing their health information in a timely manner have eroded trust in the current low-tech system, which is why we need a new approach. Building an efficient records system that is more secure and offers better coordinated care can only enhance trust between patients and providers.

Congress should lift the ban on federal funding for UPI research, and we should better inform patients about the benefits of UPIs. No one wants medical data to fall into the wrong hands, but neither do we want patients to suffer because their medical information cannot be accessed.

Dr. Collins, a board-certified physician in internal medicine, is chancellor of the University of Massachusetts Medical School in Worcester, Mass. He can be reached at reports@wsj.com.

No: Privacy Would Suffer

By Deborah C. Peel

Doctors and patients need to find a better way to collect and share personal medical records from the innumerable places health data are collected and stored. But linking people to their health data via a unique identifying number isn't the answer.

Steven Noreyko

'History shows that universal IDs are always used in unintended ways.' -- DEBORAH C. PEEL

Yes, assigning everyone a universal patient identifier, or UPI, would improve doctors' ability to share information and make it easier for hospitals to differentiate one John Smith from another. But a universal health ID system would empower government and corporations to exploit the single biggest flaw in health-care technology today: Patients can't control who sees, uses and sells their sensitive health data.

Searching for sensitive patient information would take just one number, not dozens of account numbers at professional offices, hospitals, pharmacies, labs, treatment facilities, government agencies and health plans. UPIs would make it vastly easier for government, corporations and others to use the nation's health information for their own gain without patients even knowing it.

What's more, any benefits associated with UPIs would be erased when patients, knowing their doctors have no control over where health-care data go, refuse to share sensitive information about their minds and bodies. This is a very real issue: Without privacy, patients won't trust doctors. In 2005, a California Healthcare Foundation survey found that due to the lack of privacy, one in eight patients lies, omits critical details, refuses tests or otherwise keeps sensitive health information private. *Six hundred thousand* people per year avoid early diagnosis for cancer alone.

Invitation to Snoop

We are in the midst of an unprecedented data-privacy crisis. Changes to federal regulations in 2002 eliminated patient control over who sees personal health information and led to explosive growth in the data-mining industry. Pharmacies, health-care IT vendors, insurers and others routinely sell and commercialize prescription records, genetic tests, hospital and office records, and claims data to drug companies and any willing purchasers. Even with names and key identifiers stripped off, it's simple to reidentify patients. Under the guise of improving health, lowering costs or promoting innovation, even government agencies sell and give away large databases of patient records.

Universal health-care IDs would only exacerbate such practices.

Further, UPIs would encourage the government and corporations to build massive, centralized databases of health information, rich targets for data theft and abuse. UPIs would become a de facto universal identification system far more harmful than Social Security numbers, enabling millions of government and corporate workers to snoop into anyone's medical records.

But concerns about health IDs go much deeper. UPIs exacerbate the commoditization of patients by encouraging the perspective that government agencies and corporations have superior rights to decide and control core aspects of who we are. A unique ID system is like giving master keys to millions who work in health care—they no longer need to ask patients to see records.

In the end, cutting out the patient will mean the erosion of patient trust. And the less we trust the system, the more patients will put health and life at risk to protect their privacy.

Such an obvious outcome makes a mockery of claims that UPIs would "reduce errors" and improve "patient safety." Similarly, claims that UPIs will be kept separate from personal and financial IDs are wishful thinking. All health records have financial records attached. But more important, history shows that universal IDs are always used in unintended ways. Social Security numbers were to be used only for payroll taxes, but morphed into universal IDs for health and commerce. UPIs will share the same fate.

Patients in Control

If a single ID number isn't the answer, what is? The best way to share sensitive health information is to build electronic-records systems where patients are in control of their own medical records, not government and industry. Health professionals should seek permission to see personal data, but only patients should release or link it. This is how it works with paper records systems, and there's no reason we should be less concerned about privacy in the digital age.

Existing technologies can allow patients to set default rules to govern data exchanges electronically, such as: "In emergencies, treating physicians may access my entire medical record" or "Anytime I receive health treatment, send copies to my family doctor." Consent rules can be changed instantly online, and sensitive information can be selectively withheld at the patient's discretion.

Unique patient IDs are unnecessary for this system. Much like using online banking to pay bills, patients can use online health systems to send encrypted information from medical accounts to whomever they choose.

Decentralized systems with smaller data sets protect privacy because if any account is broken into, only some information is compromised. More important, they require mediation by the patient. Imagine a universal ID system for all financial transactions where all retailers had our IDs. Commercial transactions would be more efficient if retailers could see and debit our accounts without consent. But it would be unacceptable—and it should also be unacceptable for others to use your health records without permission

I agree that we need to transform the health-IT system so health professionals and researchers can electronically tap into complete and accurate health information. But any such technology should allow professionals to treat patients as individuals whose needs come first. That won't happen if we create an electronic medical-record system that no one trusts.

Dr. Peel, a psychiatrist and health-privacy expert in Austin, Texas, is the founder of Patient Privacy Rights and leader of the bipartisan Coalition for Patient Privacy. She can be reached at reports@wsj.com.

may be referenced as an 'individual', which means the person who is the subject of protected health information.

Health Care Operations
Any of the following activities of the covered entity to the extent that the activities are related to covered functions: (1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; (3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of 45 CFR §164.514(g) are met, if applicable; (4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; (5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and (6) Business management and general administrative activities of the entity, including, but not limited to: (i) Management activities relating to implementation of and compliance with the requirements of this subchapter; (ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer. (iii) Resolution of internal grievances; (iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and (v) Consistent with the applicable requirements of 45 CFR §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. 45 CFR 164.501

Health Information Technology Exchange of Connecticut (HITE-CT)
A quasi-public agency of the State of Connecticut charged by statute with promoting, planning and designing, developing, assisting, acquiring, constructing, maintaining and equipping, reconstructing and improving healthcare information technology, including the electronic exchange of health information. Also, HITE-CT is a business associate of all participating members pursuant to the HITECH Act.

HITE-CT Infrastructure Service Provider
The entity operating and managing the core services supporting the HITE-CT systems (e.g. Provider Registry, Patient Identity Cross Reference Index Manager, Audit Record Repository, Document Registry, Document Repository, etc.).

Individually Identifiable Health Information

- **Public Health**
  - *Public Health Surveillance, Disease Control:* To inform persons or processes with responsibility to monitor populations or sub-populations for significant health events and then intervene to provide health care or preventive care services to relevant individuals.
  - *Public safety emergency:* To inform persons with responsibility for the protection of the public in a situation in which there is considered to be a significant risk to one or more members of the public, possibly needing to over-ride the policies and consents pertaining to Public Health Surveillance, and Disease Control (examples include: prevention of harm to another, outbreak management, containment of a bio-terrorism attack).
  - *Population health management:* To inform persons or processes with responsibility to monitor populations or sub-populations for health events, trends or outcomes in order to inform relevant strategy and policy.

The following uses of HITE-CT systems are not permitted at this time:

- **Research**
  - To support the discovery of generalizable knowledge.
- **Market Studies**
  - To support the discovery of product or organization specific knowledge.
- **Legal Investigation or Inquiry**
  - To inform persons or processes responsible for enforcing jurisdictional legislation, or undertaking legal or forensic investigation.
- **Education**
  - To support the learning and professional development.
- **Not Specified or Unknown**
  - Disclosure on the basis of authorizations not requiring a purpose to be declared, or where the purpose is not known, or purposes for which the other categories in this clause do not apply.

Policy Maintenance

The Legal and Policy Committee is responsible for monitoring and maintenance of policies.

General Assembly

Raised Bill No. 1147

January Session, 2011

LCO No. **3202**

*03202_____HS_*

Referred to Committee on Human Services

Introduced by:

(HS)

AN ACT CONCERNING PATIENT CONSENT FOR THE EXCHANGE OF ELECTRONIC HEALTH INFORMATION.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. Section 19a-25c of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2011*):

A health care institution licensed by the Department of Public Health pursuant to chapter 368v may create, maintain or utilize medical records or a medical records system in electronic format, paper format or both, provided such records or system is designed to store medical records or patient health information in a medium that is reproducible and secure.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*October 1, 2011*	19a-25c

Statement of Purpose:

To protect patient privacy by requiring a patient to opt-in to the exchange of electronic health records.

[

]

<<< Previous Level
Welcome
HITE-CT
HITE-CT Activities
Meetings
Policies and Procedures
Meaningful Use and Public Health
Cooperative Agreement
Presentations
Resources/Links
Get Involved
Contact us
DPH Main

Health Information Technology and Exchange

Printable Version

Welcome

The Connecticut Health Information Exchange Program

In March 2010, the Connecticut Department of Public Health (DPH) was awarded $7.29 million from the Office of the National Coordinator for Health Information Technology (ONC) through the State Health Information Exchange Cooperative Agreement Program. Connecticut is one of the fifty-six recipients of this four-year cooperative agreement. The purpose of the State HIE Program is to support states in establishing health information exchanges (HIE) capability across the health care system - among healthcare providers and hospitals- within and across states.

The Connecticut HIE Program is responsible for developing and implementing the Strategic & Operational Plan to ensure measurable progress within the state towards universal adoption of HIE. Additionally, the Health Information Technology Exchange of Connecticut (HITE-CT), a newly formed quasi-governmental agency, will work with the CT DPH to promote the development of health information technology, increase adoption and meaningful use of electronic health records, assure the privacy and security of electronic health information, and collaborate with the State's Medicaid agency and Regional Extension Center to enable information exchange and support monitoring of provider participation in the HIE.

The Connecticut Department of Public Health (DPH) is the State Designated Entity (SDE) for the State Health Information Exchange Cooperative Agreement Program through the Office of the National Coordinator (ONC). To protect the public health and health care needs of Connecticut residents, the DPH serves as an advocate, regulator, and consumer of the health information exchange.

The 2009 congressional passage of the Health Information Technology for Economic and Clinical (HITECH) Act, included in the American Recovery and Reinvestment Act (ARRA) of 2009, provided a unique opportunity for states to access federal funds to plan, design, and implement a health information exchange that will encourage the adoption and use of electronic health records and allow for the exchange of health information across institutions and providers.

Concurrently in 2009, DPH published the Connecticut State Health Information Technology Plan (2009), which established portions of the framework for the statewide health information exchange and its technology. In June 2009, DPH was designated by legislation to establish the Health Information Technology and Exchange Advisory Committee (HITE-AC) This advisory committee consisted of a broad array of health care stakeholders and provided advice and guidance in the development of the 2010 strategic and operational plan, established goals, and instituted a long-term plan for sustaining a HIE in Connecticut. The Advisory Committee was comprised of health care professionals, policy makers, payers and consumer representatives from around the state.

- Public Act 09-232, *"An Act Concerning Revisions to the Department of Public Health Licensing Statutes,"* Sec. 74-77 (codified at CGS §19a-25f -§19a-25h)

Then the 2010 Connecticut General Assembly and Governor Rell created the Health Information Technology Exchange of Connecticut (HITE-CT) as a quasi-public agency managed by an appointed Board of Directors to coordinate and oversee Health Information Exchange (HIE) activities in the state on January 1, 2011. The Board of Directors were appointed and held their first meeting in October 2010.

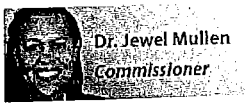
- Public Act 10-117, *"An Act Concerning Revisions to Public Health Related Statutes and the Establishment of the Health Information Technology Exchange of Connecticut,"* Sec. 82-90,96 (codified at CGS §19a-750(c)(1))

Additional information can be found on the Health Information Technology Exchange of Connecticut (HITE-CT) page found on the left hand side menu.

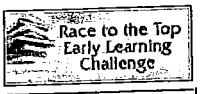
Content Last Modified on 1/12/2012 2:53:32 PM

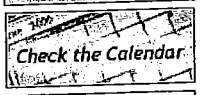
Printable Version

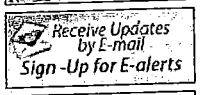
410 Capitol Avenue Hartford, CT 06134 / Phone: 860-509-8000



<<< Previous Level
Welcome
HITE-CT
HITE-CT Activities
Meetings
Policies and Procedures
Meaningful Use and Public Health
Cooperative Agreement
Presentations
Resources/Links
Get Involved
Contact us
DPH Main







Health Information Technology and Exchange

Printable Version

Policies and Procedures
Meaningful Use and Public Health

The American Recovery and Reinvestment Act of 2009 (ARRA) enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act to accelerate the adoption of health information technology. The ARRA offers incentives to eligible providers and hospitals to adopt health information technology and use it in a "meaningful" way. Meaningful Use is defined in a specific way, requiring fifteen "core" and ten "menu" criteria. Of the ten menu options, three require reporting to public health:

- Submit electronic data to public health immunization registries/systems.
- Provide electronic submission of reportable lab results to public health agencies.
- Provide electronic syndromic surveillance data to public health agencies.

Connecticut Department of Public Health (DPH) is currently working towards accepting immunization data, electronic laboratory reports for notifiable diseases and conditions, and syndromic data in a meaningful manner to improve public health from providers, hospitals, and electronic health records vendors.

Current project status (11/23/2011)
DPH is currently working on the infrastructure to support the submission of electronic laboratory reports, immunization data and syndromic surveillance. Please check back for further updates.

- Electronic Laboratory Reports
- Immunization Data
- Syndromic Surveillance

Information for Providers

The Medicare and Medicaid EHR Incentive Programs will provide a financial incentive to eligible providers, hospitals and critical care hospitals as they adopt, implement, upgrade or demonstrate "meaningful use" of certified EHR technology. By putting into action and meaningfully using an EHR system, providers will reap benefits beyond financial incentives–such as reduction in errors, availability of records and data, reminders and alerts, clinical decision support, and e-prescribing/refill automation.

- The Official Website for Medicare and Medicaid Electronic Health Records (EHR) Incentive Programs
- Additional assistance to Providers about meaningful use and the EHR Incentives program can be obtained from the **Connecticut Regional Extension Center** (REC)

Participation in the Connecticut Medicaid Electronic Health Record Incentive Program
Eligible Professionals who are planning to participate in the Connecticut Medicaid Electronic Health Record (EHR) Incentive Program are required to register with the Medical Assistance Provider Incentive Repository (MAPIR). The MAPIR is targeted to launch by summer 2011. Please check the official Connecticut Medicaid Incentives EHR Incentive Program website for information and updates.

Registration with Centers for Medicare and Medicaid Service's National Level Repository (NLR)
Eligible Professionals are also required to register with the Centers for Medicare and Medicaid Service's National Level Repository (NLR). Registration for the NLR is now open! Follow the link below for registration and additional information on the Medicaid EHR Incentive Program.

Additional Meaningful Use websites:

- Meaningful Use Final Rule - July 2010 (276 pages)
- Meaningful Use Final Rule - Standards & Criteria for EMRs (66 pages)
- Meaningful Use for Consumers
- Meaningful Use for Providers

Information for EHR Vendors

The Medicare and Medicaid EHR Incentive Programs require the use of certified EHR technology. Standards, implementation specifications, and certification criteria for EHR technology have been adopted by the Secretary of the Department of Health and Human Services. EHR technology must be tested and certified by

lots, points of highway access and interior roads, including routes between highway access and parking lots; (15) the plans for telephone service, including the source, number and location of telephones; (16) the plans for camping facilities, if any, including facilities available and their location; (17) the plans for security, including the number of guards, their deployment, and their names, addresses, credentials and hours of availability; (18) the plans for fire protection, including the number, type and location of all protective devices including alarms and extinguishers, and the number of emergency fire personnel available to operate the equipment; (19) the plans for sound control and sound amplification, if any, including the number, location and power of amplifiers and speakers; (20) the plans for food concessions and concessioners who will be allowed to operate on the grounds including the names and addresses of all concessioners and their license or permit numbers.

Sec. 7. Section 19a-72 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2009*):

[The Connecticut Tumor Registry shall include in its information center an occupational history of each newly diagnosed and reported cancer patient in the state, beginning January 1, 1981. Instructions for generating and including such an occupational history shall be provided by the Department of Public Health to each tumor registrar by October 1, 1980.]

(a) As used in this section:

(1) "Clinical laboratory" means any facility or other area used for microbiological, serological, chemical, hematological, immunohematological, biophysical, cytological, pathological or other examinations of human body fluids, secretions, excretions or excised or exfoliated tissues, for the purpose of providing information for the diagnosis, prevention or treatment of any human disease or impairment, for the assessment of human health or for the presence of drugs, poisons or other toxicological substances;

(2) "Hospital" means an establishment for the lodging, care and treatment of persons suffering from disease or other abnormal physical or mental conditions and includes inpatient psychiatric services in general hospitals;

(3) "Health care provider" means any person or organization that furnishes health care services and is licensed or certified to furnish such services pursuant to chapters 370, 372, 373, 375 to 384a, inclusive, 388, 398 and 399 or is licensed or certified pursuant to chapter 368d; and

(4) "Reportable tumor" means tumors and conditions included in the Connecticut Tumor Registry reportable list maintained by the Department of Public Health, as amended from time to time, as deemed necessary by the department.

(b) The Department of Public Health shall maintain and operate the Connecticut Tumor Registry. Said registry shall include a report of every occurrence of a reportable tumor that is diagnosed or treated in the state. Such reports shall be made to the department by any hospital, clinical laboratory and health care provider in the state. Such reports shall include, but not be limited to, information obtained from records of any person licensed as a health

care provider and may include a collection of actual tissue samples and such information as the department may prescribe. Follow-up data, demographic, diagnostic, treatment and other medical information shall also be included in the report in a form and manner as the department may prescribe. The Commissioner of Public Health shall promulgate a list of required data items, which may be amended from time to time. Such reports shall include every occurrence of a reportable tumor that is diagnosed or treated during a calendar year. On or before July 1, 2010, and annually thereafter, such reports shall be submitted to the department in such manner as the department may prescribe.

(c) The Department of Public Health shall be provided such access to records of any health care provider, as the department deems necessary, to perform case finding or other quality improvement audits to ensure completeness of reporting and data accuracy consistent with the purposes of this section.

(d) The Department of Public Health may enter into a contract for the storage, holding and maintenance of the tissue samples under its control and management.

(e) The Department of Public Health may enter into reciprocal reporting agreements with the appropriate agencies of other states to exchange tumor reports.

(f) (1) Failure by a hospital, clinical laboratory or health care provider to comply with the reporting requirements prescribed in this section may result in the department electing to perform the registry services for such hospital, clinical laboratory or provider. In such case, the hospital, clinical laboratory or provider shall reimburse the department for actual expenses incurred in performing such services.

(2) Any hospital, clinical laboratory or health care provider that fails to comply with the provisions of this section shall be liable to a civil penalty not to exceed five hundred dollars for each failure to disclose a reportable tumor, as determined by the commissioner.

(3) A hospital, clinical laboratory or health care provider that fails to report cases of cancer as required in regulations adopted pursuant to section 19a-73 by a date that is not later than nine months after the date of first contact with such hospital, clinical laboratory or health care provider for diagnosis or treatment shall be assessed a civil penalty not to exceed two hundred fifty dollars per business day, for each day thereafter that the report is not submitted and ordered to comply with the terms of this subsection by the Commissioner of Public Health.

(4) The reimbursements, expenses and civil penalties set forth in this section shall be assessed only after the Department of Public Health provides a written notice of deficiency and the provider is afforded the opportunity to respond to such notice. A provider shall have not more than fourteen business days after the date of receiving such notice to provide a written response to the department. Such written response shall include any information requested by the department.

HB 6678 PA 09-232

Sec. 77. Section 19a-25d of the general statutes is repealed and the following is substituted in lieu thereof (*Effective from passage*):

(a) As used in this section:

(1) "Electronic health information system" means an information processing system, involving both computer hardware and software that deals with the storage, retrieval, sharing and use of health care information, data and knowledge for communication and decision making, and includes: (A) An electronic health record that provides access in real-time to a patient's complete medical record; (B) a personal health record through which an individual, and anyone authorized by such individual, can maintain and manage such individual's health information; (C) computerized order entry technology that permits a health care provider to order diagnostic and treatment services, including prescription drugs electronically; (D) electronic alerts and reminders to health care providers to improve compliance with best practices, promote regular screenings and other preventive practices, and facilitate diagnoses and treatments; (E) error notification procedures that generate a warning if an order is entered that is likely to lead to a significant adverse outcome for a patient; and (F) tools to allow for the collection, analysis and reporting of data on adverse events, near misses, the quality and efficiency of care, patient satisfaction and other healthcare-related performance measures.

(2) "Interoperability" means the ability of two or more systems or components to exchange information and to use the information that has been exchanged and includes: (A) The capacity to physically connect to a network for the purpose of exchanging data with other users; (B) the ability of a connected user to demonstrate appropriate permissions to participate in the instant transaction over the network; and (C) the capacity of a connected user with such permissions to access, transmit, receive and exchange usable information with other users.

(3) "Standard electronic format" means a format using open electronic standards that: (A) Enable health information technology to be used for the collection of clinically specific data; (B) promote the interoperability of health care information across health care settings, including reporting to local, state and federal agencies; and (C) facilitate clinical decision support.

(b) On or before November 30, 2007, the Department of Public Health, in consultation with the Office of Health Care Access and within available appropriations, shall contract, through a competitive bidding process, for the development of a state-wide health information technology plan. The entity awarded such contract shall be designated the lead health information exchange organization for the state of Connecticut for the period commencing December 1, 2007, and ending June 30, 2009. The state-wide health information technology plan shall include, but not be limited to:

such provider fills an area of need of expertise for the exchange, and (B) such employee does not have an ownership interest in a professional health care practice.

(3) No employee of the exchange shall, for one year after terminating employment with the exchange, accept employment with any health carrier that offers a qualified health benefit plan through the exchange.

(4) Any employee of the exchange [who sells, solicits or negotiates insurance or will sell, solicit or negotiate insurance to individuals and small employers shall be licensed, not later than one year after such employee begins employment with the exchange, as an insurance producer under chapter 701a of the general statutes] whose primary purpose is to assist individuals or small employers in selecting health insurance plans offered on the exchange to purchase shall be licensed as an insurance producer under chapter 701a of the general statutes not later than eighteen months after such employee begins employment with the exchange.

Sec. 143. Section 19a-654 of the general statutes, as amended by section 12 of house bill 6308 of the current session, is repealed and the following is substituted in lieu thereof (*Effective July 1, 2011*):

(a) As used in this section:

(1) "Patient-identifiable data" means any information that identifies or may reasonably be used as a basis to identify an individual patient; and

(2) "De-identified patient data" means any information that meets the requirements for de-identification of protected health information as set forth in 45 CFR 164.514.

(b) Each short-term acute care general or children's hospital shall

submit patient identifiable inpatient discharge data and emergency department data to the Office of Health Care Access division of the Department of Public Health to fulfill the responsibilities of the office. Such data shall include data taken from patient medical record abstracts and bills. The office shall specify the timing and format of such submissions. [including submissions by outpatient surgical facilities as provided for in subsection (c) of this section. If a hospital or outpatient surgical facility submits data through an intermediary, the hospital or the outpatient surgical facility shall] Data submitted pursuant to this section may be submitted through a contractual arrangement with an intermediary and such contractual arrangement shall (1) comply with the provisions of the Health Insurance Portability and Accountability Act of 1996 P.L. 104-191 (HIPAA), and (2) ensure that such submission of data is timely and accurate. The office may conduct an audit of the data submitted through such intermediary in order to verify its accuracy.

(c) [With respect to the submission of outpatient data, an] An outpatient surgical facility, as defined in section 19a-493b, a short-term acute care general or children's hospital, or a facility that provides outpatient surgical services as part of the outpatient surgery department of a short-term acute care hospital shall submit to the office the data identified in subsection (c) of section 19a-634. The office shall convene a working group consisting of representatives of outpatient surgical facilities, hospitals and other individuals necessary to develop recommendations that address current obstacles to, and proposed requirements for, patient-identifiable data reporting in the outpatient setting. On or before February 1, 2012, the working group shall report, in accordance with the provisions of section 11-4a, on its findings and recommendations to the joint standing committees of the General Assembly having cognizance of matters relating to public health and insurance and real estate. Additional reporting of outpatient data as the office deems necessary shall begin not later than

July 1, 2015. On or before July 1, 2012, and annually thereafter, the Connecticut Association of Ambulatory Surgery Centers shall provide a progress report to the Department of Public Health, until such time as all ambulatory surgery centers are in full compliance with the implementation of systems that allow for the reporting of outpatient data as required by the commissioner. Until such additional reporting requirements take effect on July 1, 2015, the department may work with the Connecticut Association of Ambulatory Surgery Centers and the Connecticut Hospital Association on specific data reporting initiatives provided that no penalties shall be assessed under this chapter or any other provision of law with respect to the failure to submit such data.

(d) Except as otherwise provided in this subsection, patient-identifiable data received by the office shall be kept confidential and shall not be considered public records or files subject to disclosure under the Freedom of Information Act, as defined in section 1-200. The office may release de-identified patient data or aggregate patient data to the public in a manner consistent with the provisions of 45 CFR 164.514. Any de-identified patient data released by the office shall exclude provider, physician and payer organization names or codes and shall be kept confidential by the recipient. The office may not release patient-identifiable data except as provided for in section 19a-25 and regulations adopted pursuant to said section. No individual or entity receiving patient-identifiable data may release such data in any manner that may result in an individual patient, physician, provider or payer being identified. The office shall impose a reasonable, cost-based fee for any patient data provided to a nongovernmental entity.

(e) Not later than October 1, 2011, the Office of Health Care Access shall enter into a memorandum of understanding with the Comptroller that shall permit the Comptroller to access the data set forth in subsections (b) and (c) of this section, provided the

CT PA 10-117 Sec. 82(e)
Substitute Senate Bill 428

proceedings and maintain and be custodian of all books, documents and papers filed with the authority and of the minute book of the authority.

(e) The board shall direct the authority regarding: (1) Implementation and periodic revisions of the health information technology plan submitted in accordance with the provisions of section 74 of public act 09-232, including the implementation of an integrated state-wide electronic health information infrastructure for the sharing of electronic health information among health care facilities, health care professionals, public and private payors, state and federal agencies and patients; (2) appropriate protocols for health information exchange; and (3) electronic data standards to facilitate the development of a state-wide integrated electronic health information system, as defined in subsection (a) of section 19a-25d of the general statutes, for use by health care providers and institutions that receive state funding. Such electronic data standards shall: (A) Include provisions relating to security, privacy, data content, structures and format, vocabulary and transmission protocols; (B) limit the use and dissemination of an individual's Social Security number and require the encryption of any Social Security number provided by an individual; (C) require privacy standards no less stringent than the "Standards for Privacy of Individually Identifiable Health Information" established under the Health Insurance Portability and Accountability Act of 1996, P. L. 104-191, as amended from time to time, and contained in 45 CFR 160, 164; (D) require that individually identifiable health information be secure and that access to such information be traceable by an electronic audit trail; (E) be compatible with any national data standards in order to allow for interstate interoperability, as defined in subsection (a) of section 19a-25d of the general statutes; (F) permit the collection of health information in a standard electronic format, as defined in subsection (a) of section 19a-25d of the general statutes; and (G) be compatible with the requirements for an electronic health information system, as defined in subsection (a) of section 19a-25d of the general statutes.

(f) Applications for grants from the authority shall be made on a form prescribed by the board. The board shall review applications and decide whether to award a grant. The board may consider, as a condition for awarding a grant, the potential grantee's financial participation and any other factors it deems relevant.

(g) The board may consult with such parties, public or private, as it deems desirable in exercising its duties under this section.

(h) Not later than February 1, 2011, and annually thereafter until February 1, 2016, the chief executive officer of the authority shall report, in accordance with section 11-4a of the general statutes, to the Governor and the General Assembly on (1) any private or federal funds received during the preceding year and, if

Protection of the Right to Health Information Privacy: A Prerequisite for Health IT

I. Any health IT system must

A. Recognize the patient's right to health information privacy;

B. Provide an opportunity for that right to be exercised through informed consent;

C. Provide notice to the patient of actual or suspected breaches of health information privacy; and

D. Provide access to an effective remedy for breaches.

II. Two practical reasons

A. "In short, the entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers. HHS Finding, 65 Fed. Reg. at 82,467 (Dec. 28, 2000).

B. Failure to protect the right to health information privacy leads to less, rather than more, health information because communications between practitioners and patients "would surely be chilled". Supreme Court finding, Jaffee v. Redmond, 116 S. Ct. 1923, 1929 (1996).

III. What is the right to health information privacy?

A. Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data.

B. Confidentiality is the obligations of those who receive information to respect the privacy interests of those to whom the data relate.

C. Security is the physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access of disclosure. Report of the National Committee on Vital and Health Statistics to Secretary Leavitt (June 22, 2006).

IV. What are the sources of the right to health information privacy?

A. "Privacy and confidentiality [of health information] are neither new concepts, nor absolutes. Since the time of Hippocrates physicians have pledged to maintain the secrecy of information they learn about their patients, disclosing information only with the authorization or the patient or when necessary to protect an overriding public interest, such as public health. Comparable provisions are now contained in the codes of ethics of virtually all health professionals." Report to HHS, NCVHS (June 22, 2006).

B. Federal courts have found consistently that the right to informational privacy, as distinct from the right to decisional privacy, is protected by the Fourteeth, Fifth and Fourth Amendments to the United States Constitution. Whalen v. Roe, 97 S. Ct. 869, 877 (1977); Ferguson v. City of Charleston, 121 S. Ct. 1281, 1288 (2001), ("The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."); U.S. v. Scott, 424 F.3d 888 (9th Cir. 2005); Douglas v. Dodds, 419 F.3d 1097 (10th Cir. 2005).

C. In fact, the constitutionally protected right to privacy of highly personal information is so well established that no reasonable person could be unaware of it. Sterling v. Borough of Minersville, 232 F.3d 190, 198 (3rd Cir. 2000).

D. Ten states have a right to privacy expressly recognized in their state constitutions.

E. A physician-patient privilege is recognized in the laws of 43 states and the District of Columbia. The State of Health Privacy, Health Privacy Project (2000).

F. A psychotherapist-patient privilege is recognized in the laws of all 50 states and the District of Columbia. Jaffee v. Redmond, 116 S. Ct. 1923, 1929 (1996).

G. All 50 states and the District of Columbia recognize in tort law a common law or statutory right to privacy of personal information. HHS finding 65 Fed. Reg. at 82,464.

H. The right to not have health information disclosed without consent is reflected in the Hippocratic Oath dating from the 5th Century B. C. which is taken by most medical school graduates and in the standards of professional ethics adopted by virtually every segment of the medical profession. 65 Fed. Reg. at 82,472; The Use of the Hippocratic Oath: A Review of 20th Century Practice and a Content Analysis of Oaths Administered in Medical Schools in the U.S. and Canada in 1993, R. Orr, M. D. and N. Pang, M. D.

V. How do most Americans feel about health IT and privacy?

A. Most Americans are "highly concerned" about the privacy of their health information. UPI Poll: Concern on Health Privacy (February 21, 2007).

B. 62% to 70% of Americans are worried that sensitive health information might leak because of weak data security; that there could be more sharing of patients' health information without their knowledge; that computerization could increase rather than decrease medical errors; that some people won't disclose necessary information to healthcare providers because of worries that it will be stored in computerized records; and that existing federal health privacy rules will be reduced in the name of efficiency. Testimony of the Markle Foundation before the Senate

Committee on Homeland Security and Governmental Affairs (February 1, 2007).

C. 66% of Americans believe Congress should make protecting information systems and networks a higher priority.

1. Of that group, 46% said they would have "serious" or "very serious" doubts about political candidates who do not support quick action to improve current laws. Federal Computer Week (May 23, 2006).

D. 42% of Americans feel that "privacy risks outweigh expected benefits" from health IT. Harris/Westin poll on EHR and Privacy (2006).

VI. Health IT poses a threat to the right to health information privacy.

A. Congressional findings:

1. "Congress finds that...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 disseminiation of personal information;...the right to privacy is a personal and fundamental right protected by the Constitution of the United States...". Pub. L. 93-579, section 2(a)(2) and (4).

B. Presidential findings:

1. The nation's interconnected electronic information systems are "highly vulnerable" to attacks,

2. The number of attacks is growing by "over 20 percent annually", and

3. The vulnerabilities can only be addressed by "fundamental research" to design security into IT systems "from the ground up." "Cyber Security: A Crisis in Prioritization", President's Information Technology Advisory Committee, 5-12 (February 28, 2005).

C. HHS findings:

1. "The electronic information revolution is transforming the recording of health information so that disclosure of information may require only a push of a button. In a matter of seconds, a person's most profoundly private information can be shared with hundreds, thousands, even millions of individuals and organizations at a time." 65 Fed. Reg. at 82,465.

D. Findings of the National Committee on Vital and Health Statistics (NCVHS):

1. "An EHR system creates greater risks to confidentiality because the comprehensive disclosures might include much more information than is necessary to the particular decision at hand." NCVHS report to HHS (June 22, 2006).

E. Numerous articles in major publications over the past two years have detailed the privacy and other problems with electronic information systems.

1. "Data Theft Believed To Be Biggest Hack", The New York Times (March 30, 2007).

2. "Medical Data on Empire Blue Cross Members May Be Lost", The New York Times (March 14, 2007).

3. "Warnings Over Privacy of U.S. Health Network", The New York Times (February 18, 2007).

4. "Veterans Administration Loses Data", Consumer Affairs (February 13, 2007).

5. "Have You Resold Your Data to Crooks?" Computer World (February 16, 2007).

6. "Kaiser Has Aches, Pains Going Digital. Patients' Welfare at Stake in the Electronic Effort, Experts Say", L. A. Times (February 15, 2007).

7. "Second Hospital Reports Lost Data. St. Mary's Notifies 130,000 Days After Hopkins' Notice", The Baltimore Sun (February 13, 2007).

8. "Lost Computer Tapes Had Details of 135,000 Workers, Patients", The Washington Post (February 8, 2007).

9. "GAO Report Confirms IT's Threat to Privacy", Modern Healthcare (February 6, 2007).

10. "Diagnosis Identity Theft: For $60, a Thief Can Buy Your Health Records—and Use Them to Get Costly Care. Guess Who Gets the Bill", Business Week (January 8, 2007).

11. "Spread of Records Stirs Patient Fears of Privacy Erosion", The New York Times (December 26, 2006).

12. "LINK BY LINK; An Ominous Milestone: 100 Million Data Leaks", The New York Times (December 18, 2006).

13. "Major Breach of UCLA's Computer Files", L. A. Times (December 12, 2006).

14. "Health Providers' Social Security Numbers Posted on State Site", Associated Press (December 8, 2006).

15. "Health Hazard: Computers Spilling Your History", The New York Times (December 3, 2006).

16. "Setting the Records Straight—When You Sign Medical-Privacy Forms, What Exactly Are You Agreeing To? Probably Not What You Think." The Wall Street Journal (October 21, 2006).

17. "Medicare and Medicaid Gaps Are Found", The New York Times (October 8, 2006).

18. "ID Theft Infects Medical Records", L. A. Times (September 25, 2006).

19. "Patient Data Stolen—Nurse Loses Beaumont Laptop With 28,000 Names, The Detroit News (August 23, 2006).

20. "Survey: 81% of U.S. Firms Lost Laptops With Sensitive Data In the Past Year", Computerworld (August 16, 2006).

21. "Vast Data Cache About Veterans Is Stolen", The New York Times (May 23, 2006).

22. "Hacker Steals Air Force Officers' Personal Information", The Washington Post (August 23, 2005).

23. "Regulators Fine Kaiser Unit $200,000—The State Imposes the Penalty For Breaching Patient Confidentiality in Exposing Health Records on the Web." The L. A. Times (June 21, 2005).

24. "Searches Conducted in Hacking Probe—LexisNexis Estimates Breach Affects 310,000 People", CNN.com (May 26, 2005).

25. "Personal Data for the Taking", The New York Times (May 18, 2005).

VII. How well has the federal government protected the patients' right to health information privacy?

A. HHS "replaced" the patients' right of consent in the Original HIPAA Privacy Rule with "regulatory permission" for covered entities and their business associates to routinely use and disclose virtually any health information without the patient's permission and over the patient's objection. (August 14, 2002).

B. "Co-chair of HHS Advisory Panel Quits, Says Inadequate Progress on Privacy Protections", BNA Health Care Daily (February 26, 2007).

C. "Loss of Personal Data at Federal Agencies Is Widespread", The Washington Post (October 16, 2006).

D. "To Agency Insiders, Cyber Thefts And Slow Response Are No Surprise", The Washington Post (July 18, 2006).

E. "Medical Privacy Law Nets No Fines—Lax Enforcement Puts Patient Files At Risk, Critics Say", The Washington Post (June 5, 2006).

F. HHS Receives an "F" on its Computer Security Report Card for 2005 and 2004 from the House Government Reform Committee (March 16, 2006).

G. GAO has repeatedly found HHS fails to adequately protect the patient's right to health privacy.

1. "Health Information Technology: Early Efforts

Initiated but Comprehensive Privacy Approach Needed for National Strategy", GAO-07-238 (January 10, 2007).

2. "Privacy: Domestic Offshore Outsourcing of Personal Information in Medicare, Medicaid, and TRICARE", GAO-06-676 (September 5, 2006).

3. "Information Security: The Centers for Medicare & Medicaid Services Needs to Improve Controls Over Key Communication Network", GAO-06-750 (August 30, 2006).

4. "Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data", GAO-06-674 (June 26, 2006).

5. "Information Security: Department of Health and Human Services Needs to Fully Implement Its Program, GAO-06-267 (February 24, 2006).

6. "Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems, GAO-05-231 (May 13, 2005).

James C. Pyles
On behalf of the American Psychoanalytic Association
Powers, Pyles, Sutter & Verville, P.C.
1501 M Street, 7th Floor
Washington, D. C. 20005
(202) 466-6550
jim.pyles@ppsv.com

April 17, 2007

HIPAA – The Intent vs. The Reality

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) began as a "portability act" to help individuals keep their health insurance coverage as they moved from one job to another. HIPAA evolved to include much more than portability. It is a complex set of rules that cover patient privacy and the use of information technology to transfer your medical records.

Lawmakers began nearly a decade ago to try and blend the ancient ethical tradition of patient privacy with the health information technology advances that can save lives and reduce costs. Congress intended for the HIPAA Privacy Rule to bring the healthcare industry into the 21st century while saving citizens billions of dollars.

Effective April 14, 2003, patients were required to sign new "Privacy Forms" that gave the ***illusion*** that their records were, well, private.

The Elimination of Consent

1996	Congress passed HIPAA, but did not pass a federal medical privacy statute, so the Dept. of Health and Human Services (HSS) was required to develop regulations that specified patients' rights to health privacy.	*"...the Secretary of Health and Human Services shall submit to [Congress]... detailed recommendations on standards with respect to the privacy of individually identifiable health information."*
2001	President Bush implemented the HHS HIPAA "Privacy Rule" which recognized the "right of consent".	*"...a covered healthcare provider must obtain the individual's consent, in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment or health care operations."*
2002	HHS amended the HIPAA "Privacy Rule", eliminating the "right of consent".	*"The consent provisions... are replaced with a new provision...that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, or health care operations."*

Download the Elimination of Consent as a PDF file.

HIPAA – The Reality

The "Privacy Rule" Became the "Disclosure Rule"

HIPAA produced absurd results because patients were no longer asked what medical information they wanted shared and what information they wanted to be kept private. Barriers were created that patients didn't want, and **access was granted to private corporations, individuals and government agencies that patients would never have agreed to.**

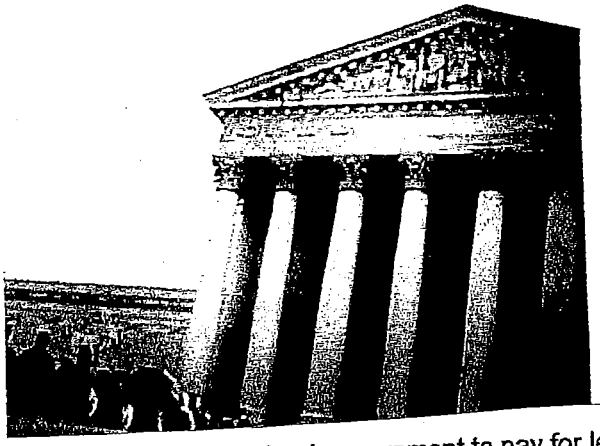
Even more damaging, the amendments to the "Privacy Rule" opened the nation's sensitive health records to millions of providers, employers, government agencies, insurance companies, billing firms, transcription services, phamacy benefit managers, pharmaceutical companies, data miners, creditors and more for any "routine" use.

- You will not receive any notice of "routine" use and disclosure of your health information.
- There are no audit trails of "routine" uses and disclosures
- Access to you health record is retroactive, regardless of whether you paid out-of-pocket or were guaranteed privacy at the time. This means your health records from birth to death are available to others.

High Court To Hear HIV-Positive [illegible]

by NINA TOTENBERG

November 30, 2011 text size A A A



The U.S. Supreme Court hears arguments Wednesday in a case testing whether the federal government is liable for damages when it violates the Privacy Act by disclosing that an individual is HIV-positive. The government does not dispute that it broke the law, but it asserts that the Privacy Act authorizes damage suits only for violations that cause economic harm, not for emotional harm.

Now he wants the federal government to pay for legal violations it committed. Social Security medical records are strictly confidential. Disclosure of the records to another agency, without consent, is clearly illegal. Indeed, the Privacy Act specifically provides that the "United States shall be liable" for "actual damages" sustained by an individual as the result of any violation of the law.

But it was too late. Unbeknownst to him, the FAA and the Social Security Administration had teamed up to find pilots who hid medical conditions. The joint operation, dubbed Operation Safe Pilot, fed in the names of 45,000 pilots in Northern California, cross-referenced them with the names of those who got any Social Security benefits, and came up with some 3,200 violators. Because Cooper had gotten disability benefits for 12 months when he was sick in 1995, his name popped out. He was charged with three felonies and eventually pleaded guilty to one misdemeanor false statement charge. He was sentenced to two years of unsupervised probation and fined $1,000.

So Cooper sued, contending he had suffered "humiliation, embarrassment, mental anguish ... and emotional distress."

A federal district court agreed that the Social Security Administration had violated the Privacy Act, but it threw out the case because Cooper did not claim economic damages. A federal appeals court, however, reinstated the suit, and the Obama administration appealed to the Supreme Court, where the justices hear arguments Wednesday.

The administration concedes that the language of the Privacy Act could be read as allowing damages for emotional harms, but it maintains that the language is ambiguous, and thus that the government gets the benefit of the doubt. If Congress wants to authorize such lawsuits, it can do so, the administration says. But it must do so clearly and unequivocally, which it did not here.

Cooper counters that the FAA and Social Security Administration deliberately and knowingly engaged in a massive violation of privacy involving thousands of individuals, and that the Privacy Act was meant to provide a remedy for those harmed by such a scheme. "They stole my privacy," he says, his voice breaking slightly.

Cooper notes that the government did exactly what it promises in writing not to do — it shared confidential medical information with those not authorized to receive it.

"This was a fishing expedition," he says. "This was a witch hunt where they just ran Social Security numbers of pilots though the Social Security disability databases and saw what fell out."

Indeed, though Cooper is still a licensed pilot, having met the current medical criteria, his name and HIV status are still posted on a government website.

Â

It is correct that the exchange, which is a business contract between provider and it, can be set up because we lost our right of consent in 2002-3?Â yes

Do we actuallyÂ have a constitutional right to privacy and is it now being violated?Â yes

Â

Â

ARRA says that Medicare and Medicaid records, in meaningful use form or other, must Â go to the federal govt? yes for truly unlimited purposes/uses without consent.

Â

Â

What is the time line for all other EHR'S to go to the feds? very soon---the goal is every Americans will have an electronic health record by 2014 and ALL are required to be data mined without consent for a myriad of purposes by the federal govt

Â

Â

Once the rules are published in the CT Law Journal, which will be soon, I will contact our ACLU to comment.Â Â But where are they anyway with all these issues? the ACLU has been a VERY BIG help at the federal level---and also in some states---state chapters vary on how much they are doing about this--hopefully the CT chapter is strong--they would be your best ally

Â

Â

I also need toÂ confirm hereÂ that the records in the exchange will be used for TPO and expanded public health uses without patient consent.Â ABSOLUTELY yes---the thing is a corporation just has to claim they are doing "research" or research for public health and they have access! There is no definition of "research" in federal law and what we see are corporations like IBM claiming to do research as a way to justify the use and access of sensitive personal health information (PHI). For example IBM "research" has developed a software tool for pediatricians desktop computers that can give the doctor actionable plans for obese kids based on their health data, family finances, where parks are for exercise, and where healthy fresh vegetables and foods are sold nearby, etc . etc--IBM has sucked up huge amounts of personal information about all these kids and families BEFORE they give consent for such intrusive use and surveillance of their lives to produce this supposedly helpful tool to combat obesity. That is just one example. See attachment.

Â

Â

SEE STORY BELOW: IBM launches massive health data research project

IBM plans to bring together personal data on individuals far beyond what is available in the healthcare system – including environmental and financial data on individuals---to "pinpoint incentives governments and businesses might offer" to patients to improve health. The plan is to first study childhood obesity.

The problem is IBM's research project does not appear to be start with obtaining informed consent from the individuals (or their parents) whose data will be collected and studied.

There is no mention of the legal or ethical authority or basis that permits IBM corporation to collect, analyze, and do research on so much sensitive personal information on individual children, in order to decide which "actions" to incentivize to improve a particular child's health.

Yet IBM's research aims to help doctors treating specific individual patients: "all these complex issues need to meld into a single thread of conversation as I talk to my patient".

The story mentions numerous groups IBM is working with, but it appears that no consumer, patient, child, or privacy advocacy organizations are "partners" in this massive research project.

Quotes:

• project will combine and analyze massive data sources that have never before been integrated to simulate the cause-and-effect relationships between agriculture, transportation, city planning, eating and exercise habits, socio-economic status, family life, and more

• project could help pinpoint incentives governments and businesses might offer or what types of investments might be needed and how to prioritize them • it's been impossible to understand and to quantify precisely how each factor in our environment plays a role

• IBM researchers said they will partner with public policy and food experts, medical clinicians, economists, simulation experts, industry leaders, universities and others in this collaborative endeavor

• In many cases, the data and models exist. They just need to be put together in a consumable way that shows the wider connections and potential actions that can enhance individual and community health," said Paul Maglio, an IBM researcher.

Deborah C. Peel, MD

Healthcare IT News Healthcare IT News PUBLISHED IN PARTNERSHIP WITH HIMSS

IBM launches massive health data research project

May 06, 2010 | Diana Manos, Senior Editor

SAN JOSE, CA – IBM has announced it has launched a multi-year research project to connect and analyze enormous collections of data from a wide variety of sources to find ways to improve health. The project will initially focus on childhood obesity.

The IBM Research project will combine and analyze massive data sources that have never before been integrated to simulate the cause-and-effect relationships between agriculture, transportation, city planning, eating and exercise habits, socio-economic status, family life, and more, researchers said.

"Our ability to advance the health of our population is currently limited to maintaining healthy life choices and working within a health care delivery system because it's been impossible to understand and to quantify precisely how each factor in our environment plays a role," said Martin Sepulveda, MD, IBM fellow and vice president of Integrated Health Services at IBM.

"We hope the results of this project will help individuals, governments and businesses actually understand exactly how the actions they take affect health - and then work together to make better decisions that make it easy to be healthy," Sepulveda said.

According to Sepulveda, in the U.S., chronic diseases such as diabetes, heart disease and obesity account for 70 percent of all deaths and more than $1.5 trillion of healthcare spending annually. Factors far beyond the traditional healthcare system – including finance, urban planning, individual behavior, disease transmission, clinical research, media and many others – influence human health. Understanding these interconnected factors is critical to developing effective programs that enhance health and well-being.

"Managing health, be it for a single patient or an entire population, is an overwhelmingly complex challenge," said Gary An, assistant professor of trauma and critical care at Northwestern University Feinberg School of Medicine. "Despite the critical influence of cultural, socio-economic and environmental factors, the doctor-patient relationship remains the mainstay of delivering healthcare: all these complex issues need to meld into a single thread of conversation as I talk to my patient. Therefore, any initiative – like the one IBM is launching – that can help bring together these disparate and often potentially contradictory forces and aid me in tailoring how I can help my patient improve his or her health, is both greatly needed, and greatly welcomed."

According to IBM, the research project could help pinpoint incentives governments and businesses might offer or what types of investments might be needed and how to prioritize them.

"In many cases, the data and models exist. They just need to be put together in a consumable way that shows the wider connections and potential actions that can enhance individual and community health," said Paul Maglio, an IBM researcher. "This is a huge challenge from both a social and technological perspective, but we believe our expertise in service science, computational modeling, math and large-scale analytics can help answer these important questions."

IBM researchers said they will partner with public policy and food experts, medical clinicians, economists, simulation experts, industry leaders, universities and others in this collaborative endeavor.

Last week IBM gathered many of the leading thinkers from these areas at the 10th annual Almaden Institute in San Jose, California to discuss the fundamental issues of the research project.

http://www.healthcareitnews.com/news/ibm-launches-massive-health-data-research-project