COALITION FOR PATIENT PRIVACY

March 15, 2010

Office of the National Coordinator for Health Information Technology,
Attention: HITECH Initial Set Interim Final Rule
U. S. Department of Health and Human Services
Hubert H. Humphrey Building, Room 729D
200 Independence Avenue, SW
Washington, DC 20201

Re: RIN 0991-AB58; Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology

To whom it may concern:

The Coalition for Patient Privacy is the leading voice of consumer organizations for privacy and health IT. We are a diverse, multi-partisan group united by our efforts to prevent discrimination in employment and other key opportunities based on health information. Patients will only trust the healthcare system if privacy and the right of consent is assured.

We appreciate this opportunity to provide public comment on the interim final rule (IFR) establishing the initial set of standards, implementation specifications, and certification criteria for Electronic Health Record (EHR) Technology.

We envision an ethical health system that reaps the benefits of technology while simultaneously protecting our children and grandchildren from generations of discrimination based on their protected health information. Individuals are best positioned to ensure that personal data goes *only* to the 'right' places at the 'right' times. With control over PHI (Personal Health Information), consumers can prevent the most egregious violations of privacy and most destructive uses of our health information, including rampant electronic fraud and identity theft by limiting who can access our records.

If we begin with what is easy (or easier) for industry rather than what is essential for patients' trust in electronic systems, we will not realize the ultimate vision for HIT. While ensuring privacy may be seen by some as challenging, it has been a core concept

of our systems of laws and ethical practice of medicine and doable and more importantly, it is absolutely essential for quality health care.

In the current IFR, the Coalition sees four critical missing pieces.

1) HIT effectively creates valuable personal information. Patients have long expected to enjoy legal and ethical rights to control how their information is used. The status quo and the IFR appear to ignore these rights. It appears that the IFR grants industry broad regulatory discretion to use personal health care information without the patient's permission. Failure to address this issue in a timely way and to engage the patient from start to finish will leave HIT 'dead on arrival' and will waste the stimulus billions on defective EHRs.

2) The term "privacy" is frequently used, yet HHS has not defined what it means. This leaves much of the IFR that relates to privacy subject to varying interpretations that will erode the public's confidence that their health information privacy will be protected.

3) The IFR notes that nothing in it supersedes existing stronger state and Federal laws; therefore, HHS needs to incorporate the more robust existing requirements into IFR functionalities and standards.

4) No one and no industry likes to be regulated. However, HHS needs to set a high bar for patient privacy in HIT, not promote and fund the use of products that will not be trusted. It will be more difficult politically to try to add privacy protections after health IT systems and products have been designed, built and sold.

1) Patient Control is Foundational for HIT

We certainly appreciate the need for gradual implementation. However, there are key technology features essential for earning and maintaining the public's trust: items such as logical information segmentation, consent management and audit trails need to be addressed now.

- P 14--- None of the 3 stages in the CMS EHR Incentive Programs deal with privacy (defined in the law as an individual's right of control over personal information).

In every EHR, the CRITICAL FUNCTION needed is the ability for patients to control the uses and disclosures of their health information (PHI) for all "routine" uses. We recommend adoption of the open source National Data Information Infrastructure Consortium consent technology. It enables detailed control over disclosures as a functional baseline model or 'floor' for consent technologies. The millions of members in our organizations want granular control over disclosures of their electronic health

records. The standard they are looking to replicate is analogous to the protections in state law and the ethical principles that have long governed our control over disclosures of our paper health records. If that control is not provided, patients will engage increasingly in self-preservation tactics of keeping sensitive health information out of any health record.

We believe that patients are only willing to participate in the healthcare system and trust doctors with their most sensitive concerns when they know that their PHI is being protected. Patients will disclose complete and accurate information when the trust factor is high; the results will contribute to achieving measurable and reliable outcomes, to improving quality, to discovering which treatments are most cost effective, to enabling breakthrough research, and finally to lowering costs in the long term.

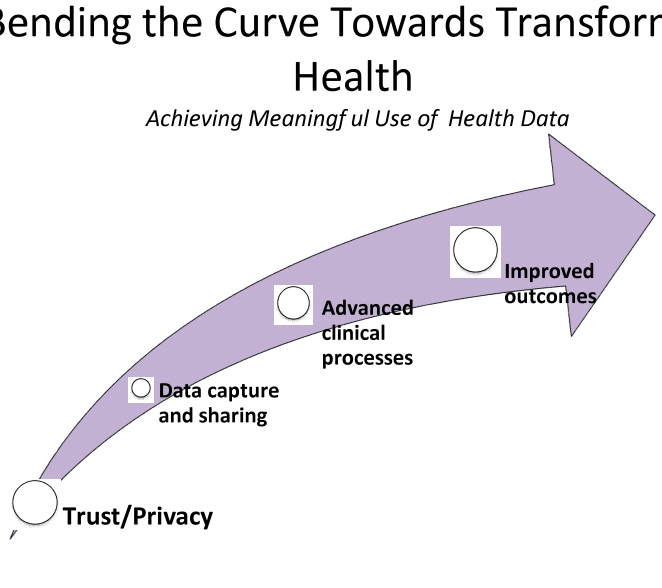
Accurate and complete information cannot be obtained by force. We know from the California HealthCare Foundation's National Consumer Health Privacy Survey of November 9, 2005 (prior to current efforts to implement an interoperable national electronic health system) that 12.5% of the population avoids seeing their regular doctor; they ask their doctors to alter diagnoses; they pay privately for a test or avoid tests altogether. Without restoration of patients' rights to control disclosures of PHI, we can expect electronic health data to have error and omission rates of far more than 12.5 percent. The breakthroughs and benefits possible with technology-enhanced research will never be attained with such a high rate of errors and omissions.

- Absent or Erroneous Data = Garbage In
- Garbage In = Garbage Out
- Garbage Out = Faulty Research
- **Research using bad or unreliable data will not produce dependable outcomes, measures or generate "comparative effectiveness" answers. When so many patients get treatment off-the grid or avoid treatment altogether, no data is produced. And, the data that is produced is skewed.**

See CHCF survey at: http://www.chcf.org/topics/view.cfm?itemID=115694

HHS under the Clinton Administration found unequivocally that quality healthcare depends on privacy[1]. Developing and maintaining TRUST is essential before patients are willing to give providers any data to capture. Trust and privacy (and security) need to be the starting point:

[1] "The **entire health delivery system** is based upon the willingness of the individual to trust a health care practitioner sufficiently to disclose to the practitioner the most intimate details of his or her life." "An assurance of privacy of health information is **necessary to secure effective, high quality health care.**" 65 Fed. Reg. at 82,467



- Page 16—Exception to "safe harbor".—Donating EHRs to physicians and health professionals under 'safe harbor' is a bad idea unless consent tools are built into EHRs. There is NO way patients can stop the donor entity or their physicians from allowing data mining and misuse of their sensitive PHI. The IFR MU certification criteria do not address the problem of data mining of PHI from donated EHRs. The IFR should prohibit donated EHRs from participating in data mining for secondary uses without informed, contemporaneous consent by patients.

- Page 37--EHR modules.--To the extent that modules house or store PHI and demographic, identifiable or re-identifiable data, no uses or disclosures should be made without informed, contemporaneous consent.

- Page 38--The definition of "complete EHR" does not include a functional requirement for addressing patients' rights of consent or for patients to have the ability to segment sensitive data; there are legal and ethical requirements in existing law and standards of practice that must be sustained.

- The definition for Certified EHR technology has the same flaws as the definition of "complete EHRs".

- Page 50— The requirements for state programs to set up electronic immunization registries are positioned ahead of Americans' expectations about

control of their PHI. State registries of sensitive data are already being attacked and are involved in litigation. For example, the Texas NBS program and ASU were sued over the misuse of bloodspots and the exploitation of Havasupai Indians' blood. The state registries collections of data and specimens will never be trusted unless the public knows and understands the uses for which the data or specimen is collected. Further, the public must be convinced that the records and specimens will ONLY be used for the original agreed purposes. Further, people want to make certain that if the items are to be used for other purposes, the secondary use will only happen with informed consent (except as required by law for specific legal uses).

- Page 72 –E-prescribing.--Prescriptions must not include additional information such as diagnoses. Sharing diagnoses through today's HIT systems enables the misuse of the nation's prescription data; going forward this will only compound the problem by enabling the misuse of sensitive identifiable diagnostic information. Prescription data mining, that is, the theft and trading of sensitive personal prescription records, convinced Congress of the need to ban the sale of PHI in HITECH. HHS previously found that even the disclosure of the drug regimen for treating HIV/AIDS would inhibit the willingness of individuals to be tested and treated. [FN-65-Fed.Reg. at 82,778.] According to HHS: "Strengthening privacy protections beyond this disease could increase confidence in privacy regarding HIV as well.

2) Adopt a Meaningful Definition of Privacy

The word "privacy" is used throughout the IFR; it is used without a definition. This lack of definition results in confusion and lack of specificity regarding Americans' EXISTING privacy rights under Federal and state law, Constitutional law and court decisions, and ethical codes of health professionals. We urge adoption of the NCVHS definition of health information privacy: "*. . . individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data."*

- Page 45-46—The IFR asserts that the certification criteria for MU based on the recommendations of the HIT Policy Committee are "logical", but are they logical for the general public? The public expects to control personal health information in EHRs. See quotes below from the AHRQ Publication No. 09-0081-EF "Final Report: Consumer Engagement in Developing Electronic Health Information Systems" Prepared by: Westat, (July 2009), See:

- http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_1248_888520_0_0_18/09-0081-EF.pdf

    - According to the AHRQ, A majority of participants in the 20 focus groups want to "own" their health data, and to decide what goes into and who has access to their medical records (AHRQ p. 6).
    - A majority believes their medical data is "no one else's business" and should not be shared without their permission. This belief was expressed not necessarily because they want to prevent some specific use of data but as a matter of principle. (AHRQ p. 18)

  The IFR asserts that certification will "be leveraged to improve security, privacy, and interoperability", but without a definition how can "privacy" be insured and improved?

- Page 46—Middle paragraph: the policy priorities in CMS Medicare and Medicaid EHR Incentive Program are to "ensure adequate privacy and security protections for PHI"--but under the existing common law definition of "privacy", the EHR Incentive Program does not ensure privacy. In fact, it assures that patients have no privacy of PHI. Statements such as this mislead both vendors and the public.

- Page 49—The IFR supports adopting standards qualified by "at a minimum" to accommodate current "industry practice." Industry is being 'accommodated' but not the real constituents, the public. The IFR should lead industry forward by requiring robust consent management, segmentation, and audit trail functionalities in certified EHRs.

1) Strong Privacy Requirements in state and Federal Laws Should Be Incorporated in the Certification Criteria for Electronic Health Record Technology

No taxpayer dollars should be spent on systems that cannot comply with existing state and Federal privacy laws.

- Page 59—The "Capability to exchange key clinical information" among "authorized" users conflicts with Americans' rights to health privacy. Existing Federal and state laws, ethics and standards of practice do not allow the millions of HIPAA "authorized users" to use and access PHI without informed consent. This Stage 1 Objective appears to violate existing law and violates Americans' rights to health privacy.

- Page 79—The "Adopted Content Exchange and Vocabulary Standards" for EHRs does not require the ability to segment sensitive PHI. Data exchange without the ability to segment sensitive data violates the strong protections in state law for sensitive genetic, mental health, and other personal information.

- Page 84—Middle paragraph. The IFR clarifies that the use of certified EHRs "does not change existing HIPAA Privacy Rule or Security Rule requirements, guarantee compliance with those requirements, or absolve an eligible professional, eligible hospital or other healthcare provider" from "having to comply with any applicable provision of the HIPAA Privacy or Security Rules". But we are concerned that industry and providers will rely on the IFR certification criteria despite this disclaimer. Vendors and providers will assume that the rest of the privacy requirements in HIPAA and in existing law and ethics will not be enforced; this causes us great angst. Through the IFR certification criteria, it seems to us that HHS sends the wrong signal. Instead of setting a high bar to ensure Americans' privacy rights, it looks as if it encourages vendors and providers to ignore the critical consumer protections the public wants in electronic systems. Vendors that have denied or ignored patients' privacy rights for decades will be able to continue to sell obsolete EHR systems and products. HHS and CMS certification criteria will squander taxpayers' money and build systems that violate state and Federal law.

- Page 88 --Quote. "Nothing required by this interim final rule should be construed as affecting existing legal requirements under Federal laws." Further, Certified EHR Technology "may not provide, from a technical perspective, all the capabilities necessary to comply with these regulations." The IFR cites 42 CFR Part 2 as one example of a law with which Certified EHR Technology will not comply. Why open the opportunity window to vendors and providers to sell Certified EHR Technology that cannot meet requirements in existing Federal and state law? HHS and CMS set IFR certification criteria that are out of compliance with existing Federal and state law and then make vendors and providers accountable for the lack of compliance in Certified EHR Technology.

- Page 109--- Federalism: "Nothing in the interim final rule imposes substantial direct requirement costs on State and local governments, preempts State law or otherwise has federalism implications." Certification criteria are not supposed to

preempt state laws. So, why are HHS and CMS certifying criteria for EHR technologies that will conflict with or preempt state laws?

4) HHS Needs To Set High Standards to Engender Patient Trust

Too often, the interests of the HIT, research, insurance, pharmaceutical and data mining industries are in direct conflict with Americans' longstanding legal and ethical rights to control personal health information. Without additional meaningful consumer and patient engagement, expecting the rulemaking process to protect consumers is like expecting foxes to design coops that chickens will trust. Similar to the auto, banking, and securities industries, the HIT, pharmaceutical, insurance, and healthcare industries will not add consumer protections willingly. *They will always claim consumers' privacy rights are impossibly complex, too expensive, or even unnecessary.* However, we believe these claims are spurious and that existing privacy-enhancing technologies and Federal privacy policy precedents should be used as minimum functionalities and policies for EHR certification criteria and quality matrices.

Acknowledging the time needed for implementation, we urge the Committee to recommend policies that will require no less than the use of existing privacy-enhancing technologies and to plan to continually raise the privacy bar. Audit trails are critically important. Likewise, early attention is needed for the successful implementation of segmentation and consent management features. If these protections remain on the backburner untended, EHRs will be purchased and used over the next four years without these critical features. Leaving out these essential items will make retrofitting for privacy a much more expensive burden.

- Page 34---"Functional" standards. We recommend that functional standards be implemented. We are concerned that even the requirements for the use of "specific languages" could prevent better language systems and ways of communicating electronically because the evolution of more efficient technologies will be stymied.

- Page 40—Last paragraph. We do not agree that the definition of Certified EHR Technology is "flexible enough to account for innovations in an industry that continues to rapidly evolve." We believe that the definition adopted in the IFR will smother innovation in the areas most critically needed: privacy and security technologies.

- Page 43—The definition of "disclosure" is new and is flawed in our view. Many large entities can disclose data inappropriately INSIDE enterprise systems to people who should never see/use PHI. The question of which disclosures are breaches was carefully articulated in HITECH. Congress concluded that there could be inappropriate breaches inside organizations. We recommend deleting this new definition.

- Page 56-57 --Copies of health information. The certification criteria and objectives are out of sync with reality. Americans are entitled to exact copies of their health records, i.e. all health records, not summaries. It is useful to offer different views or summaries of PHI to make it easier for people to understand and use PHI, but everyone is entitled to exact copies of their entire records with rare exceptions under the law (for example, in Texas mental health records can be summarized, instead of providing the copies of the entire chart).

- Page 57—There is no reason for patients to wait up to 96 hours for access to electronic records; records should be available whenever providers enter them electronically. Patients can certainly see paper records in less than 96 hours, and health IT should make the system more, not less, efficient.

- Page 58--"Provide clinical summaries for patients for each office visit". Office visit summaries can be provided, but we must note that patients are legally entitled to copies of the entire record of each office visit.

- Page 63--- "Privacy and Security Standards". The list of examples does not include basic consent management tools.

- Page 82—Encryption. Using ONLY encryption standards is a prime example of how requiring specific standards will block innovation and the use of new technologies to make data unreadable. Our concern is that certified EHRs will only use encryption unless the IFR designates encryption as a "minimum" functional standard to make data unreadable.

- Page 85---The first sentence states "nothing precludes the use or implementation of more protective privacy and security measures." But why would vendors build stronger privacy and security measures or providers ask for

them? The certification criteria HHS and CMS require in this IFR do not comply with existing state and Federal law or medical ethics. What inducement do vendors or providers have to implement more privacy protective measures when the HHS and CMS IFRs signal that compliance with stronger legal and ethical requirements for privacy will not be enforced?

- Page 90—The Secretary should not consider watering down the requirement for audit trails; they are critical to public trust. The IFR suggests that the administrative burden for entities should be taken into account. Effective technologies exist today that offer complete audit trails for EHR systems, building on transaction data for authenticating employee access to PHI. Authentication software can produce audit trails of all accesses to all software programs used by hospitals and providers that move/create/disclose data. See Imprivata's "Privacy Alert" technology--many vendors offer similar products that generate audit trails and are currently being used.

- Page 92—The IFR states: "We do not propose additional requirements at this time." It is our understanding that the entire purpose of the Administrative Procedures Act is to make certain that the public can make comments on the rulemaking process and that their concerns will be taken into account and that they will be addressed – which would mean listening to the public's concerns and adding new requirements, altering existing requirements and potentially making significant changes. This quote appears to dismiss critical public protections and input required by the rulemaking process and it appears to be inconsistent with the statement of ONC's Director of Office of Policy and Research who was quoted on February 24 by Healthcare IT News as saying that "ONC's ability to change the proposed rule will be limited to removing or tweaking aspects already there."

- Page 92—The Secretary has "discretion" to move the requirement for audit trails back to 2013. We urge her not to do so. The consumer protections required in HITECH and other Federal and state laws should be moved up to be the first requirements for EHR certification. Audit trail technologies exist and are in use now. The burden on industry is minimal because authentication is essential and the records of user authentication can be used to produce audit trails.

- Page 93--Second bullet. In the future, independent consent technologies located outside of all enterprises and data holders should be used to prevent fraud and abuse. Individuals will not allow providers or strangers to access or use their PHI unless they know, recognize, and approve the user and/or purpose of the request to access PHI. Individuals have the most at stake if their PHI is misused or accessed by people with malicious intent, whether to defraud the government, steal information for identity theft or medical identity theft, or track down victims of abuse. Requiring informed consent empowers individuals and their families to protect themselves from theft and misuse of sensitive PHI.

Conclusion

Ensuring ironclad privacy protections to prevent theft and misuse of PHI must be an obligation of doing business in health care. If a provider or entity cannot or will not protect our most sensitive data, they should not be trusted to be in the health care business. We currently have higher standards for protecting financial data than we have for protecting health data. With a breach of financial records, a consumer faces a significant headache, but ultimately credit and funds can be restored; this is simply not the case with health records. A stigmatizing diagnosis/condition or prescription in the wrong hands can cause irreversible damage and result in generations of discrimination. There is no perfect 'delete' or 'recover' button to restore the privacy of health information that has been used or disclosed without consent or lost via a breach. The burden on data holders to report breaches must not trump this important protection for consumers.

The Coalition urges HHS to revise the IFR so that it aligns more clearly with the public's expectations, with the intent of Congress, and with the paramount principles of privacy (control over personal information), transparency and accountability. Thank you for this opportunity to provide feedback. We look forward to working with you.

Sincerely,

The Coalition for Patient Privacy

Clinical Social Work Association
Consumer Action
Government Accountability Project
JustHealth
The Multiracial Activist
National Association of Social Workers

National Center for Transgender Equality
Patient Privacy Rights
Private Citizen, Inc.
Secure ID Coalition
Tolven Health