COALITION FOR PATIENT PRIVACY

September 13, 2010

The Honorable Kathleen Sebelius
Secretary, United States Department of Health and Human Services
Office of Civil Rights
Attention: HTIECH Privacy and Security Rule Modifications
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue, SW
Washington, DC 20201

Re: Comments on 45 CFR Parts 160 and 164
RIN: 0991-AB57; Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information technology for Economic and Clinical Health Act

Dear Secretary Sebelius:

The bipartisan Coalition for Patient Privacy is pleased to submit comments regarding the proposed rulemaking on 45 CFR Parts 160 and 164. We applaud the efforts of the Department of Health and Human Services (HHS). Ensuring Americans' health records are private is critical for health care and the success of health information technology (HIT).

The Coalition for Patient Privacy is the leading consumer voice for building ethical, trustworthy HIT systems. We represent 10 million Americans who seek to restore the right of consent and the right to health information privacy in electronic health systems. Consent and control are imperative for patients to be willing to participate in electronic health systems and data exchanges. The Coalition promotes privacy-enhancing technologies that ensure we can move the right information to the right person at the right time -- while preventing unwanted sale and misuse of protected health information (PHI) by strangers we have no relationship with.

As a voice for patients, the Coalition has no conflict of interest, financial or otherwise. We are deeply invested in this long term process and are eager to help HHS ensure both progress and privacy. The Coalition urged Congress to include historic new privacy and security rights in the Health Information Technology for Economic and Clinical Health (HITECH) Act.[1] These core protections are essential building blocks for privacy and HIT and must be fully implemented and enforced.

[1] See our letter to Congress at: http://patientprivacyrights.org/media/CoalitionPatPriv_Final01.14.09.pdf

The Coalition strongly supports the Administration's new commitment to personal control over sensitive health records. It was very gratifying to see HHS announce a new "Administration-wide commitment to make sure no one has access to your personal information unless you want them to" on July, 2010.[2] We appreciate the Secretary's leadership, along with that of the National Coordinator, Dr. David Blumenthal, who reinforced HHS' commitment to privacy when he stated "we want to make sure it is possible for patients to have maximal control over PHI (protected health information)."[3]

We are also grateful that Dr. Blumenthal agreed to hold the Consumer Choices Technology Hearing on June 29, 2010, at our request. The hearing video and records form a critical resource for consumers and state lawmakers to see seven privacy-enhancing technologies in live demonstrations, just as they begin to plan how best to use stimulus funds to promote the adoption of EHRs, design systems for data exchange, and prepare to link to the NHIN.[4]

GENERAL RECOMMENDATIONS & OBSERVATIONS

We agree with many of the proposed rules. We also note that the new rights and requirements of the HITECH Act necessitate robust electronic consent and segmentation tools. For example, electronic consents that enable segmentation empower consumers to:

- consent to the sale of PHI
- disclose the "minimum necessary" information from EHRs for a particular purpose
- segment PHI if the treatment cost was paid out-of-pocket so that information is not disclosed to a health plan
- segment sensitive PHI as required by state law
- give consent to disclose addiction treatment records as required in 42 CFR Part 2
- enable veterans to consent to disclose PHI as required by USC 7332, Title 38, Veteran's Benefits, Subchapter III—Protection of Patient Rights

We strongly recommend that HHS require the use of the consent and segmentation technologies showcased June 29th at the Consumer Choices Technology Hearing sponsored by HHS/ONC for all HIT systems, HIE, and the NHIN. The innovative, low-cost, effective privacy-enhancing technologies available that can empower patients to have "maximal control over PHI" should be viewed as what is possible now, not ten

---

[2] Press conference, July 8, 2010. See: http://www.hhs.gov/news/imagelibrary/video/2010-07-08_press.html

[3] Ibid

[4] Privacy and Security Tiger Team: Past Meetings, June 29, 2010, Consumer Choices Technology Hearing. See testimony at: http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=2833&PageID=19477#062910
See the video at: http://nmr.rampard.com/hit/20100629/default.html

years from now. We urge you to go farther and faster to make President Obama's commitment to building a truly patient-centric healthcare system a reality today. The key way to build trustworthy systems that ensure consumer control over health information is to require robust electronic consent and segmentation systems in all certified EHRs, all HIEs, and all NHIN models.

It is essential for public trust to require purpose specification and authorization for all new uses or disclosures of PHI. Moreover, these protections must be required now. Public distrust is already so high that the success of the massive stimulus investments we are making in HIT and HIE are at great risk.

The recent 2009 NPR/Kaiser/Harvard poll on "The Public and the Health Care Delivery System" found that 59% of Americans are NOT confident that their [online] medical records and PHI would remain confidential.[5] Seventy-six percent of Americans believe an unauthorized person would get access to their [online] medical records. Key findings from 20 consumer focus groups held across the nation are detailed in the AHRQ "Final Report: Consumer Engagement in Developing Electronic Health Information Systems" (July 2009). The report shows the public expects to control PHI in HIT systems and data exchanges:

- A majority want to "own" their health data, and to decide what goes into and who has access to their medical records
- Medical data is "no one else's business" and should not be shared without their permission… [as] a matter of principle
- There was no support for... general rules that apply to all health care consumers
- Consumers should be able to exert control over their own health information individually, rather than collectively. [6]

If HHS does not require strong privacy policies and the enforcement of patients' rights to control PHI now, the US will be destined to the waste of billions in HIT and HIE investments. Further, we will experience the same extreme public rejection of HIT and data exchange witnessed in the United Kingdom. When the UK decided to add PHI to the National Health data base without consent there was a public outcry.[7]

- The project triggered anger when it was revealed that information could have been logged on the system without patients' knowledge.

---

[5] See: *http://www.kff.org/kaiserpolls/upload/7888.pdf*

[6] AHRQ Publication No. 09-0081-EF "Final Report: Consumer Engagement in Developing Electronic Health Information Systems" Prepared by: Westat (July 2009) http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_1248_888520_0_0_18/09-0081-EF.pdf

[7] See: UK Telegraph, "Controversial medical records database suspended. A controversial scheme to upload confidential medical records to a national database has been suspended following public outcry." By Kate Devlin, Medical Correspondent, 17 Apr 2010 at: http://www.telegraph.co.uk/health/healthnews/7598520/Controversial-medical-records-database-suspended.html

- The British Medical Association (BMA) warned that many people were not even aware of the scheme, let alone the fact that they could 'opt out'.

Ending secondary uses, onward data transfers, and disclosures of PHI can be achieved very quickly if HHS requires the use of privacy-enhancing technologies, such as Private Access[8], Critical Management for Behavioral Health Sciences[9], or the Department of Veterans Affairs [10] consent systems for data use and/or exchange. Innovative technologies can enable robust electronic consent and segmentation functionalities. Consumers can be contacted automatically via computers or cell phones[11] for any exceptions to their standing consent 'rules' or directives, or when new consents or authorizations are sought when CEs (Covered Entities), BAs, and health data users want to use PHI for new purposes. An example of a cell phone contact system the VA uses to contact patients to obtain consent to access PHI is Anakam's Two Factor Authentication Platform. Anakam delivers authentication through the use of devices - such as cell phones, home phones, web-connected computers, office phones, voice biometrics, or OATH-compliant tokens.

Patient privacy can be assured with trustworthy systems using consent and segmentation systems. With meaningful enforcement of security and privacy we will be able to reap the benefits of HIT while preventing most harms. We stand with you to help this Administration carry out its new policy to put patients in control of who can access PHI.

DETAILED COMMENTS AND RECOMMENDATIONS

Part 160 --
Section 160.103, Definitions

2. Definition of "Business Associate"

We agree that the Business Associate (BA) definition should be expanded to include: Patient Safety Organizations, Health Information Organizations, E-prescribing Gateways, data transmission services, PHR vendors and subcontractors of Business Associates.

---

[8] See Privacy & Security Tiger Team: Past Meetings, 6.29.2010, Meeting Materials, Private Access [PDF - 308 KB] or http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=2833&PageID=19477#062910 .
[9] See Privacy & Security Tiger Team: Past Meetings, 6.29.2010, Meeting Materials, Critical Management for Behavioral Health Sciences [PDF - 33 KB] or http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=2833&PageID=19477#062910
[10] See: See Privacy & Security Tiger Team: Past Meetings, 6.29.2010, Meeting Materials, Department of Veterans Affairs [PDF - 60 KB] or http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=2833&PageID=19477#062910
[11] See: Anakam.TFA® Two Factor Authentication

- We recommend that data transmission organizations that do not access PHI "routinely" should ALSO be included in the definition of BAs.
- We recommend that any disclosure or breach of a data transmission organization's communications of PHI needs to be subject to the breach notice requirements and all the security requirements of the HIPAA and the HITECH Act.
- We recommend that every entity inside or outside the healthcare system that handles PHI should be required to comply at a minimum with the HIPAA and HITECH security protections, otherwise there will be breaches of PHI that are never known or reported.

2c. Inclusion of Subcontractors

We strongly agree that the definition of "Subcontractors" should be included in the definition of BAs and that they should be liable for their actions and report breaches to BAs. We also agree with widening the definition of "Disclosure" to include divulging information in any manner outside the entity holding the information.

4. Definition of "Electronic Media"

We recommend that the use of any electronic means to convey information should require compliance at a minimum with the HIPAA and HITECH security protections.

5. Definition of "Protected Health Information" (PHI)

We agree with the definition of "violation or violate".

- We recommend against changing the definition of PHI to permit access to PHI of persons who have been dead 50 years.

This section is a surprising and very privacy-destructive move. We urge you to reject the requests of curious historians to eliminate the privacy of the dead, because revelations about genetic and health information can be used to discriminate against their living descendents. It is extremely premature to propose a system that will determine disclosure of PHI of the deceased at this time.

Alternatively, we recommend requiring technologies that allow individuals to set their own robust and detailed advance consent directives.[12]

8. Definition of "Workforce"

[12] See the Consumer Choices Technology Hearing video at: http://nmr.rampard.com/hit/20100629/default.html. Read the testimony about 7 consent and privacy-enhancing technologies by scrolling down to June 29, 2010: http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=2833&PageID=19477.

We agree with the expansion of the Workforce definition to include volunteers, trainees, and other persons who work for BAs.

D. Subpart B—Preemption of State Law,
Section 160.201—Statutory Basis

We strongly recommend the preservation of this exception that ensures that the strong protections and rights to patient privacy that exist in the laws of all 50 states are preserved and not preempted by weaker provisions in HIPAA.

E. Subpart B-Preemptions of State Law,
Section 160.202-- Definitions

We strongly agree with amending the definition of "contrary" and "more stringent" to include Business Associates, so that they are subject to the same requirements as CEs.

Subparts C and D of Part 160
Section 160.300 -- Applicability

We agree that the Secretary, BAs, subcontractors, and others listed should comply with the enforcement provisions.

Subpart C—Compliance and Investigations,
Section 160.304(b)—Principles for Achieving Compliance

We recommend that the Secretary should be able to assess penalties and fines regardless of whether or not the Secretary provided technical compliance assistance to the organization. Even though the entities correct identified violations, depending on the size of the population affected, the severity of the violation(s) and consideration of other relevant factors, penalties may be imposed.

Section 160.304 (c) -- Investigation, Section 160.306(c) and Section 160.308 -- Compliance reviews

- We strongly recommend that the only category of violators that should not be penalized with fines are those who despite due diligence could not discover the violation, who reported the violation immediately when discovered, and fully corrected the problems within 30 days of discovery.

We believe that HHS's first duty is to protect the public and fully enforce the requirements of the HIPAA, the HITECH Act, and to require compliance with all other federal privacy statutes that require consent, including 42 CFR Part 2 and 38 USC 7332, Title 38, Veteran's Benefits, Subchapter III—Protection of Patient Rights. We urge HHS

to focus on ensuring enforcement and compliance with all federal rights to health privacy, not just on the HIPAA and the HITECH Act compliance. Again, HHS has no duty to protect the interests of CEs, BAs, subcontractors, etc.

Congress specifically increased penalties and enforcement in the HIPAA as a result of actual harm that has already occurred. Moreover, industry's attitudes toward protecting sensitive health information are lax at best after ten years without any meaningful enforcement. Millions of health record breaches have occurred; the number and frequency of breaches is increasing, not decreasing.

The systemic practice of health data mining theft, sale, and misuse of the nation's treasure trove of personal health information by countless numbers of CEs, BAs, subcontractors, and others prompted Congress to ban the sale of PHI without consent in HITECH. Huge under-the radar health data mining corporations are using PHI today in ways that no one would ever agree to. Congress intended to send a very strong signal to industry that trusted systems are essential for consumer participation in healthcare. Congress added historic new consumer privacy and security protections to HITECH. We urge HHS to ensure strong enforcement of security and privacy violations to protect and defend consumers' interests and rights.

Section 160.312—Secretarial Action Regarding Complaints & Compliance Reviews

We strongly recommend that the Secretary be required to impose a penalty in every case of noncompliance, even when resolution and compliance has been achieved by informal means. What is the point of having a penalty structure to motivate industry compliance if penalties will not be assessed for most violations? This is the wrong message to send the public and industry. Congress' intention in amending the HIPAA was to require strong, effective, and appropriate enforcement policies and procedures to ensure the healthcare system complies with all federal health privacy and security laws. The public must see that vigorous enforcement takes place in order to trust HIT and HIE systems and the NHIN.

Section 160.401 – Definitions

We agree with the definitions of "reasonable cause" and "willful neglect". However, we disagree that examples (1) and (2) on page 40878 of the Federal Register demonstrate reasonable diligence. The first example was a printing error where two pages were left off a Notice of Privacy Practices; but any reasonably diligent person would have checked the prints to be sure all the pages were present before distributing the notices. The second example was about terminating access privileges for the wrong employee with the same name as a former employee. Again, this is a situation where a reasonably diligent person would have checked to see which of the two people with the same name should have been terminated. There could be situations where reasonable diligence

would not be enough to prevent an error, but these examples do not illustrate "reasonable diligence".

Section 160.402—Basis for a Civil Money Penalty

We agree with this entire section, including that the Secretary should impose civil money penalties on CEs that violate an administrative simplification provision, that BAs should be liable for the actions of their workforce and subcontractors, and that CEs should be liable for workforce members or BAs actions.

Section 160.406 – Violations of an Identical Requirement or Prohibition

We agree that the Secretary should determine the number of violations and that a separate violation occurs each day the CE or BA is in violation of a provision.

Section 160.408 -- Factors Considered in Determining the Amount of a CMP

This section includes all the factors the Secretary should consider when determining the size of the fines imposed on violators. We recommend that (d)(1) and (d)(2) be deleted. We recommend that the financial condition and/or financial difficulties of the CE or BA should <u>not</u> be considered as mitigating factors in determining the amount of "civil money penalty". These provisions allow the Secretary to lessen penalties for violators who harm consumers. Again, the Secretary's goal should be protecting consumers, not shielding industry from penalties for wrongdoing.

Section 160.410 – Affirmative Defenses

This section imposes severe limits on the Secretary's authority to impose a "civil money penalty". We are very concerned that on or after February 18, 2009 the Secretary is prohibited from imposing penalties UNLESS the violation is due to willful neglect and is not corrected. We believe that using the lax scheme proposed in the NPRM will only encourage industry to continue to avoid obeying the law and avoid protecting the most sensitive personal information on Earth: our health information, from prescription records to DNA to diagnoses.

We recommend that all violations due to "reasonable cause" should require penalties, because if "reasonable diligence" had been exercised, the violator would have known of the violation and could have acted to report and remedy the problem(s). It is not too much to expect that those who are part of the healthcare system exercise "reasonable diligence".

PART 164—SECURITY AND PRIVACY

We recommend that HHS remove the "addressable" designation from the security rule. The continued use by HHS of a combination of risk evaluation, addressable and reasonable practice, establishes ambiguity in the industry around expectations for security. We recommend that HHS provide benchmarks by sector that will start to define a reasonable practice for the industry, remove ambiguity and finally achieve substantive improvements in controls for the industry. A good example for the Secretary is the Breach Notification Law. This law was clear and specific around encryption controls, and the net result is a significant increase in the adoption of these technologies across the industry. While the addressable nature of some requirements was intended to not unduly burden any organizations, the net result is broad ambiguity and insubstantial adoption of those controls in the industry.

Section 164.104 -- Applicability

We agree that the security and privacy standards, requirements, and implementation specifications should apply to BAs in the same manner as they apply to CEs.

Section 164.302 – Applicability

We agree that a CE or BA must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic PHI of a CE.

Section 164.304 – Definitions

We agree with definitions of "Administrative safeguards" and "physical safeguards".

Section 164.306 – Security Standards, General Rules

We agree that CEs and BAs "must" "ensure the confidentiality, integrity, and availability of all electronic PHI the CE or BA creates, receives, maintains, or transmits" and "must comply with applicable standards as provided in this section".

Section 164.308 – Administrative Safeguards

We strongly agree that CEs and BAs must conduct "accurate and thorough" risk analyses of the "vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by the BA or CE". We also agree with the required Sanction policy, the Termination procedures, the policies on Access establishment and modification, the Response and reporting requirement, and "periodic technical and nontechnical evaluation based initially on standards and subsequently in response to environmental and operational changes affecting security.

We agree with the language in (b)(1) regarding Business Associate contracts and other arrangements.

- We strongly recommend that HHS clarify the expectations of CEs to ensure that BAs and their subcontractors have appropriate controls in place and not simply rely on contractual arrangements. Patients entrust their CEs with their data, not BAs. CEs should exercise appropriate due diligence by auditing their BAs and subcontractors to ensure that patient information is protected when accessed and used by these entities.

- We strongly recommend that all BAs and CEs should be required to undergo meaningful and comprehensive security and privacy audits annually, to establish and prove that their methods of operation do in fact safeguard patient information.

"Assurances" are totally inadequate to guarantee that HIT and HIE systems are trustworthy. The strength of security and privacy functions must be proven annually. Section(b)(2) permits BAs to use subcontractors if the subcontractors provide the same kind of "assurances" that information will be safeguarded. Again this approach is totally inadequate to protect patients' privacy and security.

- We recommend that all subcontractors should be required to undergo meaningful and comprehensive annual security and privacy audits to establish and prove that their methods of operation do in fact safeguard patient information.

This is required in the HIPAA Security Rule 164.308(a)(8) Evaluation. HHS should reinforce the difference between the risk assessment and evaluation requirements, as confusion in the industry is resulting in one form assessment substituting for the other. It is important for HHS to emphasize that organizations must continuously assess or evaluate their control environment to ensure that information protections are operating effectively. Again, HHS job is to protect the public from the "gold rush" created by the massive stimulus funding for HIT and data exchange. The healthcare and HIT industries are flooded with new and unproven businesses and corporations that just want the money.

Section 164.501 – Definitions

The definition of "marketing" excludes actions that the average person would clearly call marketing and find offensive. The public would not agree that any of the listed exclusions should be permitted.

The Coalition, and the average person, would consider a doctor to be "marketing" if that doctor was paid to recommend a treatment, medication, or device, regardless of

whether or not his/her Notice of Privacy Practices states that the doctor is paid to sell the product or service and the patient is offered a clear opportunity to opt-out of such sales pitches. This exception is actually unethical. Physicians who sold medications to patients were the reason that the practices of Pharmacy and Medicine were legally separated early in the 20th century. Lawmakers realized that allowing doctors to sell their own nostrums to patients created a conflict of interest and coerced patients to buy dubious products. Sending patients medication refill reminders, describing health-related products or services included in a health plan or that "add value" to benefits, and care or case coordination information that does not fall under the definition of treatment are also not defined as "marketing". We disagree and believe this section to be far outside the bounds of Congressional intent.

- We strongly recommend that the exceptions to the definition of "marketing" in the NPRM be eliminated because *the average person <u>would</u> define them as marketing.* These exceptions should require authorizations prior to patients receiving "sales pitches" for all products or services, no matter who sells them.

Section 164.502 (a)(4)(i) Business Associates: Permitted Uses and Disclosures.

BAs may use or disclose information only as permitted by contract or as "required by law". We are concerned that the phrase "required by law" could be interpreted to grant BAs the same rights to use and disclose PHI for Treatment, Payment and Health Care Operations (TPO) without consent as CEs were granted by the Amended the HIPAA Privacy Rule. The intent of this NPRM is to make sure that BAs are required comply with the same privacy and security requirements CEs must follow to protect PHI, i.e., the requirements in the HIPAA. However, in 2002, HHS amended the HIPAA and the consent provisions were replaced, "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, and healthcare operations" (67 Fed. Reg. 53,183). It is critical that HHS clearly restrict BAs' access to PHI rather than grant BAs access to use, disclose, and sell PHI.

- We strongly recommend that BAs (including subcontractors) should be prohibited from using and disclosing PHI except as specified by the CE in the business associate contract.

- We strongly recommend that HHS state its intent to end the unbounded onward transfers, secondary uses, and disclosures of PHI without informed consent or authorization.

- We strongly recommend requiring all CEs and BAs to comply with the Code of Fair Information Practices and provide "a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent."

This means requiring robust electronic consent systems that enable CEs and BAs to automatically check patient directives about uses of PHI.

Section 164.502(b) – Uses and Disclosures of PHI

We agree that CEs and BAs should limit health information to the "minimum necessary" to accomplish the intended purpose.

- We strongly recommend that that HHS require the use of the consent and segmentation technologies showcased June 29th at the Consumer Choices technology Hearing sponsored by HHS/ONC for all HIT systems , HIE, and the NHIN.

Patients and providers must have an electronic way to send only the "minimum necessary" PHI, otherwise this requirement and important consumer protection is impossible to implement. Consent systems that enable patients to selectively share PHI are required to implement the "minimum necessary" provisions of HIPAA and HITECH.

Section 164.508 (a)(2) and (a)(3)(ii) Authorization Required: Psychotherapy Notes

We strongly agree with these sections.

Section 164.508 (a)(4) Authorization required: Sale of PHI (A) For public health purposes and (B) For research purposes

We strongly disagree with this section. The exceptions to the requirement to obtain patient authorization before the sale of PHI by CEs or BAs for public health or research purposes legalize two massive existing privacy "loopholes" in the HIPAA. These "loopholes" effectively eliminate consumer control over PHI and will eliminate privacy for generations of Americans if not addressed and remedied in this rulemaking process. It is essential that HHS close these loopholes in this rulemaking process.

<u>The HIPAA "Research" and "Public Health" Loopholes</u>
We recognize that the IOM and many respected scientific and research institutions believe that researchers should have open access to PHI without patient knowledge or consent and believe that the "research" and "public health" loopholes should remain in the HIPAA. They believe the loopholes are essential to deriving the greatest research benefits from health technology systems. Unfortunately, the public does not agree.

In fact, the public strongly opposes unfettered research access to PHI. Alan Westin's survey for the IOM on the effects of the HIPAA on research[13] found:

- Only 1% of the public agreed that researchers would be free to use personal medical and health information without consent
- Only 19% of the public agreed that personal medical and health information could be used as long as the study "never revealed my personal identity" and it was supervised by an Institutional Review Board.

Mark Rothstein[14] concluded that the IOM "missed the mark" when it recommended open access to PHI without consent for research purposes.

> "Clinicians, researchers, and their institutions do not have the moral authority to override the wishes of autonomous agents. Individuals seeking treatment at a medical facility are not expressly or impliedly waiving their right to be informed before their health information and biological specimens are used for research. The recommendation of the IOM Report would automatically convert all patients into research subjects without their knowledge or consent".

Even more troubling than the lack of concern about the public's attitudes toward research on PHI without consent is the fact that the legitimate clinical and academic research communities have not acknowledged the commercial exploitation of the "research" and "public health" loopholes by health "research" corporations, such as prescription data mining corporations, insurers, and technology and hardware vendors.

The existence of a large commercial "research" industry whose "research" does nothing to improve health or benefit patients could blacken the reputation of the entire legitimate research community. Commercial use and sale of PHI for corporate business analytics and data analyses could destroy patient trust in legitimate research. This difficult problem cannot be solved by denial or by re-defining "research" to exclude commercial "research" that benefits corporate bottom lines, not patients.

Public health access to medical records and PHI has always been granted by statutes that address specific diseases such as TB, HIV/AIDS, SARS, etc. The public has never debated or agreed to unlimited access to medical records or PHI without consent by public health agencies. This massive expansion of the mission and definition of public health has never been debated, much less endorsed by the public. The history of public health has been vigorously debated leading to consensus and lawmaking that addressed specific threats to all posed by deadly infectious diseases.

---

[13] Westin/Harris Survey for the Institute of Medicine, Results of a National Survey, on "Health Research and the Privacy of Health Information: The HIPAA Privacy Rule" by Dr. Alan F. Westin, See: http://patientprivacyrights.org/media/WestinIOMWkshp2-28-08.ppt

[14] "Improve Privacy in Research by Eliminating Informed Consent?" IOM Report Misses the Mark. In The Journal of Law, Medicine & Ethics, Volume 37, Issue 3 (p 507-512) by *Mark A. Rothstein.* See: http://patientprivacyrights.org/wpcontent/uploads/2010/02/Rothstein-ReIOM-Report.pdf

Unless informed consent is required for "research" and "public health" uses of PHI, as required by ethical codes for research[15] and by international treaty[16], the lack of health information privacy will result in patients avoiding treatment, out of fear that their health information will be used for research they do not support. The ethical codes of all health professions require informed consent before use or disclosures of personal health information[17].

> "The well- being of the human subject should take precedence over the needs and interests of society."[18]

- **We strongly recommend that HHS close the "research" and "public health" loopholes in HIPAA by requiring robust electronic consent** for all types of research, quality improvement, comparative effectiveness research, P4P, population health research, patient safety research, and all public health use and research UNLESS specified by statute.

The use of privacy-enhancing consent and segmentation technologies (see pages 2 and 10) will preserve the ethical basis of research and public health, while ensuring patient trust in health professionals, researchers, and HIT systems. Public health research shows that with consent, over 75% of parents would support the use of their newborn's bloodspot for research. Without consent, only 28% would support research on their newborn's bloodspots.[19]

Furthermore, Congress had no intention of promoting the kinds of business analytics "research" being done today on sensitive personal health information, which provides no direct benefits to patients and is done without patient knowledge or consent. The commercial "research" industry collects, sells and discloses data sets of longitudinal patient information that can easily be re-identified and used to destroy patients' privacy, reputations, and life opportunities, such as jobs and credit.

Today, countless health data mining and HIT corporations have changed their business models to take advantage of the massive "research" and "public health" loopholes in the HIPAA, transforming their businesses into for-profit "research" firms or by selling corporate "research" on public health issues such as drug interactions and

---

[15] NCVHS Report to HHS, (June 22, 2006)
[16] Ethical Principles for Medical Research Involving Human Subjects, World Medical Association Declaration of
Helsinki, June 1964
[17] NCVHS Report to HHS, (June 22, 2006)
[18] Ethical Principles for Medical Research Involving Human Subjects, World Medical Association Declaration of Helsinki, June 1964
[19] Dr. Aaron Goldenberg (Case Western Reserve), *Public Health Genomics*, July 9, 2009 (as reported at Genetic Alliance Conference on Newborn Screening, December 2009).

complications. This lucrative industry is premised on obtaining PHI without consent. A recent example is IBM Corporation which is now positioning itself as a "public health research" institution that is addressing the problem of childhood obesity.[20]

- 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."
- Today, many EHR/HIT vendors justify the sale PHI without consent as a permissible "research" use of Americans' health data; a few examples are GE Centricity[21], AthenaHealth EHRs[22], Greenway EHRs[23], Cerner EHRs[24], and Practice Fusion EHRs[25].

Many health data mining corporations, such as Thomson Reuters, obtain PHI without consent for business analytics and business research they sell to large employers and other customers without patient knowledge or consent.[26] See quote below from a

---

[20] See: Healthcare IT News, "IBM launches massive health data research project" by Diana Manos, Senior Editor, May 06, 2010 at: http://www.healthcareitnews.com/news/ibm-launches-massive-health-data-research-project

[21] GE Healthcare's Clinical Data Services Business provides access to de-identified ambulatory electronic medical record data. It is one of the largest anonymized clinical databases in the United States providing access to real-world longitudinal patient information. See: https://www2.gehealthcare.com/portal/site/usen/menuitem.b399d8492e44a6765c09cbd58c829330/?vgnextoid=ae0f4fb9efff5210VgnVCM100000382b3903RCRD&fromChannel=7e0f4fb9efff5210VgnVCM100000382b3903

[22] Xcomomy.com: "Athenahealth Paying Dearly to Take on Larger Rivals" by Ryan McBride, 5/6/10 See: http://www.xconomy.com/boston/2010/05/06/athenahealth-paying-dearly to-take-on-largerrivals/3/

[23] Prime*Research,* Our research solution provides access to a vast network of clinical trials, evidence-based medicine and pharmaceutical research, as well as clinical and financial benchmarking services. The result – increased practice revenues and access to patient care improvements. See: http://www.greenwaymedical.com/solutions/prime-research/

[24] Kansas City Business Journal, "Cerner finds a treasure in data mining" by Mike Sherry, May 29, 2009. See: http://www.bizjournals.com/kansascity/stories/2009/06/01/story5.html?b=1243828800^1835382

[25] Healthcare IT News, "Practice Fusion expands, shows signs of rapid growth" by Diana Manos, 12/31/07. See: http://www.healthcareitnews.com/news/practice-fusion-expands-shows-signs-rapid-growth

[26] WHITE PAPER, Health Research Data for the Real World: The MarketScan Databases by David M. Adamson, PhD, Stella Chang, MPH, Leigh G. Hansen, MS, MBA; Research and Pharmaceutical Division, Thomson Medstat, January 2006

white paper that states Thomson health **data is maintained at the individual patient level**:

- "Data from individual patients are integrated from all providers of care, maintaining all healthcare utilization and cost record connections at the patient level."

And today, Thomson Reuters is advising states to use "opt-out" consent for HIEs[27], a form of 'consent' that actually violates patients' rights to selectively share sensitive personal data about genetics, STDs, mental health, addiction, etc. Every state requires patient consent to use sensitive PHI. Quote from a press release:

- Say No to an Opt-in Consent Policy: While it is vital to protect patient privacy in the HIE, opt-in environments have been shown to impede patient participation. An opt-out environment, by contrast, preserves the rights of the patient without hindering adoption.

Finally, major insurers use and sell claims data and obtain PHI without consent for various purposes including business analytics and business "research". One example is BCBS' Blue Health Intelligence. See quotes from "What is BHI® (Blue Health Intelligence)?"[28]:

- share critical health information with employers
- premier health intelligence resource in the nation
- unmatched detail about healthcare trends and best practices while protecting individual privacy [no proof offered]
- BHI sets the new standard for healthcare data aggregation, reporting and analysis
- longitudinal data on 54 million BCBS members [used for this purpose without consent]
- 36 months of historical information
- reporting not only by MSA, industry and product type, and *Diagnosis Related Groups*
- code, *age group* and *gender* [allows re-identification]

Today's technology systems and architecture enable the health data mining industries to exploit the "research" and "public health" loopholes in the HIPAA, and eliminate

---

[27] Press Release, 29 Mar 201 0, Thomson Reuters Establishes Best Practices for Statewide Health Information Exchanges: Whitepaper Outlines Steps to Maximize Stimulus Funding. See: http://thomsonreuters.com/content/press_room/tsh/tr_establishes_best_practices_statewide_health

[28] http://www.bcbs.com/innovations/bhi/bhi-faqs-1-12-09.pdf

Americans' health privacy and right of control over PHI. HHS must address and remedy these loopholes in this rulemaking process.

Gayle Harrell, a member of the national HIT Policy Committee stated, "The fundamental right of privacy should determine the architecture of the system to be used and the policy that formulates it. Technology must be used to preserve values, and be determined by them - not the other way around". We urge HHS not to be distracted by industry naysayers, whose positions are based on self-interest.

- **We strongly recommend** that HHS require the use and implementation of robust electronic consent and segmentation tools in 2011 in all EHRs certified for "meaningful use", for HIE, and for the NHIN models (see examples cited above on page 2 and page 10), to ensure compliance with existing federal and state laws and patients' rights to health privacy (control over personal information).

Section 164.508 (b)(3)(i) Authorization Required: Sale of PHI, Compound Authorizations

We believe that the recommendations for compound authorizations for research will lead to confusion. The need to "clearly differentiate between the conditioned and the unconditioned components" is made more difficult by combining the components into one document.

HHS should require research communities to use robust electronic consents instead of preserving the "research" and "public health" loopholes in HIPAA. Electronic drop-down menus of consent choices and clicks to receive more information can actually improve the process of informed consent and end the use of advance, blanket 'consents'. Robust electronic consent systems are effective, easy to use, inexpensive ($5/patient/year[29]), and can contact thousands instantly and automatically, for contemporaneous consent, eliminating the need to use IRBs or Privacy Boards to authorize access to PHI. Electronic consent systems can actually promote research by enabling researchers to contact people with the conditions they want to study and enable patients to find research studies they want to participate in. Private Access' consents are being used now to obtain consent and protect patients' rights to control PHI for genetic research and by Pfizer[30] for clinical trials.

---

[29] See video of June 29, 2010 Consumer Choices Technology Hearing, 3:30-4:30 pm Panel Discussion, Dr. Deborah Peel's questions to Robert Shelton, CEO of Private Access at: http://nmr.rampard.com/hit/20100629/default.html

[30] Business Wire, Pfizer And Private Access Announce Plans To Develop Online Community To Accelerate Clinical Research, August 19, 2009. See: http://www.businesswire.com/news/home/20090819005806/en/Pfizer-Private-Access-Announce-Plans-Develop-Online

- We recommend that HHS eliminate section (i) on compound authorizations.

- We recommend that HHS fund and require the use and studies of robust electronic consent systems.

Section 164.510 – Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object

We agree with this section.

Section 164.512 (b)(1)(v)(A)(1) and (A)(2) – Uses and Disclosures for which an Authorization or Opportunity for the Individual to Agree or to Object is Not Required

We recommend eliminating these sections as employers should not have access to PHI without consent unless required by law.

Section 164.514 – Other Requirements Relating to Uses and Disclosures of PHI

We recommend that patients should have to **opt-in** to fundraising communications. The public prefers opt-in to opt-out use of sensitive health information.

Section 164.514 (d) -- Minimum Necessary

- We recommend that CEs and BAs determine the "minimum necessary" PHI to be used or disclosed for a particular purpose in consultation with the patient and/or using the patient's electronic consent directives to selectively share the "minimum necessary" information for a purpose. Technology can be developed to guide and inform patients about how to set their directives or "rules" to disclose only the "minimum necessary" information needed.
- We recommend that the NPRM require robust segmentation functionalities so that patients' consent directives and rules ensure that CEs and BAs exchange only the minimum necessary data for a particular purpose, with informed consent.

Section 164.514 (e)(2) – Other Requirements

We do not agree that limited data sets should qualify as the minimum necessary information in response to a request for PHI. The identifiers that are stripped out to create "limited data sets" actually make re-identification of the data very easy, because the following identifiers remain: admission, discharge, and service dates; dates of birth and, if applicable, death; age (including age 90 or over); and five-digit zip code or any other geographic subdivision.

For the same reasons we do not agree that IRBs or Privacy Boards should be able to waive authorization for any research use or disclosure of limited data sets.

- We strongly recommend that electronic authorization or consent be obtained before the release of a limited data set and that the NPRM should not permit the use of limited data sets to meet the minimum necessary requirements.
- We strongly recommend that the sections of the NPRM that enable research or public health use of limited data sets without consent be eliminated.

Section 164.520 (b)(1)(iv) -- Notice of Privacy Practices

- We strongly recommend that since these notices need to be modified to inform consumers of their new rights, the NPRM should also require all Notices of Privacy Practices to list the privacy rights patients have according to medical ethics and the laws of the state where they seek treatment, and how to exercise those rights.

We have never seen a Notice of Privacy Practices (NPP) that actually fully sets out consumers' privacy rights according to state law, common law, Constitutional law, or medical ethics and how to exercise those rights even though this was required by the Original HIPAA Privacy Rule. We believe that the NPRM should specify the inclusion of privacy rights in all federal law, state law, common law, Constitutional decisions or protections, privileges, medical ethics, licensing laws, etc in each NPP. Unless NPPs list and educate consumers about all their privacy rights and describe how to exercise them, the notices will fail to comply with the HIPAA and the HITECH Act. Worse, NPPs that violate federal law will prevent consumers from being able to protect themselves.

We agree that consumers must receive copies of new NPPs as quickly as possible. It is essential that the costs of informing patients not be used to justify any delay in informing the public about how to exercise their rights. Since older NPPs failed to inform patients about how to exercise their privacy rights according to all stronger state and federal laws and medical ethics, it is essential that new NPPs contain this critical information and be distributed as soon as possible.

Section 164.522 – Rights to Request Privacy Protection for PHI

We strongly support the changes to this section enabling those who pay cash for treatment to prevent PHI from being disclosed to health plans for payment and healthcare operations.

- We recommend that HMOs be required to build technology systems that are capable of data segmentation, since every state has strong laws requiring

segmentation and the HITECH Act requires the abilities to selectively share PHI for several purposes (when patients' pay privately, for minimum necessary, and for the sale of PHI). Since segmentation functionalities should be required for all EHRs and HIT systems, the systems in HMOs should enable patients to segment information about the treatment they do not want to be disclosed for payment or HCO to their insurer.

Section 164.524 – Access of Individuals to PHI

We strongly support HHS' intent to ensure patients can get electronic copies of all health information, wherever it is held, on demand. HIT systems should be required to automatically provide full and complete copies of all PHI. Other limited views of electronic health information may be offered, but patients are entitled to complete copies of all personal health information held in any data base.

- We recommend that HHS clarify that consumers are entitled to full and complete copies of PHI from all data holders instantly or within one day. HHS should clarify this right to full and complete access, because industry is already beginning to lobby to limit patient access to complete copies of PHI and delay when patients can acquire copies of PHI.
- We strongly recommend that individuals not be required to request copies of PHI in writing. For the convenience of patients, all data holders should be required to offer electronic requests and authentication, as well as written requests for copies of PHI. Again, in patient-centered healthcare systems, technology should be used to improve the ease and convenience of electronic requests.

Recommendations for Industry Audits

- We recommend that HHS/OCR take a proactive and rigorous approach to industry audits.

As stated in the NPRM, the HITECH Act Section 13411 requires the Secretary to provide for periodic audits to ensure covered entities and business associates comply with the applicable requirements of the HIPAA Privacy and Security Rules. A reason for this requirement is the healthcare industry's continued lack of attention to implementing adequate controls to secure PHI despite the passage of the HIPAA security compliance date over seven years ago. The rate of breaches, over 4 million records to date, also is a clear indicator of the abysmal state of information protection in the industry.

Congress recognized that HHS would have to establish a more proactive and forceful enforcement process to fundamentally change the current state. It is unclear in the NPRM how HHS/OCR plans to conduct audits, and the extent of reporting that Congress, the industry and patients can expect to receive based on enforcement activities. It is

important that HHS provide a clear and unambiguous message to the industry and patients about the level of enforcement to be expected. All too many healthcare organizations that are prepared to roll the dice with respect to regulatory action need to clearly be forewarned that it is long overdue and completely unacceptable not to invest in securing PHI.

We recommend that HHS/OCR consider the following approaches with respect to proactive enforcement efforts:

- Publicly disclose OCR's general audit strategy on an annual basis. Specifics about organizations and focus are not required and counterproductive, but this type of notice is useful in keeping privacy and security obligations as a priority for organizations. This was evidenced by the HIPAA assessments conducted by OIG in 2008. These audits created a renewed sense of focus and urgency for organizations to address HIPAA compliance requirements.

- Conduct audits based on risk and exposure in the industry. To date, regulatory audits are executed by OCR in reaction to a complaint or high profile breach, but proactive audits should focus on the issues that present the highest risk for security breaches. OCR should leverage the data collected about breaches in the industry to identify relevant sectors and associated issues that present a high risk to the industry. For example, audits should focus on these type of issues and provide important data about the results back to the industry and Congress:

    - Exposure of health insurance information to attacks from organized crime and Medicare related fraud
    - Exposure and good practices for small to medium sized provider organizations
    - Extent of vulnerability associated with fast moving trends, such as mobile or cloud computing
    - Extent of exposure of PHI managed by BA's and subcontractors in the US and abroad
    - Inconsistent practices and related vulnerabilities of health information networks and their related customers and affiliated organizations

Recommendations:

1. OCR should consistently promote the need for organizations to assess their security as required by the Evaluation requirement in the HIPAA Security Rule (164.308(a)(8) Evaluation) by using this as a risk factor for considering OCR's audit focus.
2. OCR should direct significant audit activities to organizations that do not assess their environments, but not ignore other organizations.

3. OCR should use the results of evaluations or assessments for gathering data that continues to help the office understand and direct audits towards high exposure areas for the industry.
4. OCR should publish an annual summary of the results of these audits with related recommendations for remediating findings. This type of reporting will shed light on the extent of the vulnerabilities in the industry and also provide direction to organizations looking to remediate similar issues in their environments.

Conclusion:
We urge HHS to recognize that now is the time to require technology companies and their development teams to support our privacy rights and build consent and segmentation functionalities into the next generation of HIT systems.

Not long ago providers, CEs, BAs, and industry cited technology challenges and cost as excuses for not encrypting PHI; but HHS was not distracted by those voices. HHS' requirements for breach notification and encryption fundamentally changed the market and raised the bar for critical consumer protections in electronic systems. What industry claimed was not practical or possible just 24 months ago, has quickly become standard practice.

Unless HHS makes similar clear and unambiguous recommendations to implement robust functionalities that support privacy, consent, and segmentation in HIT and HIE, HHS will set the nation on a privacy-destructive course that will take us well into the next decade to resolve and repair. During the next decade, if these privacy-enhancing requirements are not added to the meaningful use criteria, millions of health records will be endlessly disclosed, collected, misused, and sold, compromising people's lives and reputations for generations. If HHS does not impose meaningful and comprehensive consent and segmentation requirements, industry will never improve existing primitive HIT and HIE systems and technologies.

Now is the time for HHS to build upon the strong privacy protections in existing federal law (not just in the HIPAA and the HITECH Act) to ensure that the stimulus billions are not wasted and the public's trust in government, health technology, research, and the physician-patient relationship is not destroyed. Once trust is lost, it is very difficult to restore. Our best chance to build effective, efficient, high quality, useful HIT systems and data exchanges is to build in consumer control over PHI at the front end, as soon as possible.

Thank you for the opportunity to submit public comment for this critical regulation. We look forward to continuing our efforts together.

Sincerely,

The Coalition for Patient Privacy

American Association of People with Disabilities
American Civil Liberties Union
Consumer Action
Cyber Privacy Project
The Doctor Patient Medical Association
The Fund for Genetic Equity
Gun Owners of America
JustHealth
The Multiracial Activist
Patient Privacy Rights
Private Citizen, Inc.
U.S. Bill of Rights Foundation

Representative Nancy Barto (R-AZ), Chairman, Health & Human Services Committee
Christine L. Borgman, Professor & Presidential Chair of Information Studies, UCLA
Prof. Chip Pitts, Stanford Law School & Oxford University; President, Bill of Rights Defense Committee