RIN: 0991-AB57
Modifications to the HIPAA Privacy, Security, and Enforcement Rules
under the Health Information Technology for Economic and Clinical Health Act

September 13, 2010

Georgina Verdugo
Director
Office for Civil Rights
United States Department of Health and Human Services

Dear Ms. Verdugo:

The Center for Democracy and Technology (CDT), through its Health Privacy Project, promotes comprehensive privacy and security policies to protect health data as information technology is increasingly used to support the exchange of health information. CDT, along with those listed at the end of this letter, submits these comments in response to the July 7, 2010 notice of proposed rulemaking (NPRM) issued by the Dept. of Health and Human Services (HHS) Office of Civil Rights.[1]

Health information technology (health IT) is poised to transform patient-provider interaction and the delivery of health care, but will also exacerbate privacy risks if comprehensive regulatory safeguards are not in place. A comprehensive framework of privacy and security protections, including greater transparency regarding uses and disclosures of personal health data, is crucial to consumer trust in health information technology and health information exchange.

The privacy provisions in the HITECH portion of the American Recovery and Reinvestment Act of 2009[2] took significant steps toward establishing this comprehensive framework. We are encouraged that many of the provisions in the NPRM would further strengthen patient privacy, data security and enforcement of the law. However, several other proposals need clarification and other proposals should be reconsidered. In brief, our recommendations are the following:

- Marketing
  - Treat all subsidized communications as marketing that require patient authorization. A less desirable alternative is a strong opt out system.
  - Include generic equivalents in the marketing exemption for drugs or biologics the patient is currently taking.
  - Eliminate the exemption for communications subsidized through nonprofits.
  - Preserve the current marketing exemption for face-to-face communications.

[1] 75 Fed. Reg. 40867-40924 (Jul. 14, 2010).
[2] P.L. 111-5 (2009).

- Business associates
  - Require business associate agreements to limit uses and disclosures of PHI only to those necessary to perform specific services listed in the agreement.
  - Issue guidance on which factors determine when PHR vendors operate as business associates.

- Research
  - Develop a comprehensive approach to privacy for research based on more than individual authorizations.
  - Issue guidance on ways providers can maximize patient understanding of compound authorizations.
  - Require authorizations for future research to detail the purposes of future research.

- Decedents' information
  - Rescind the proposal to remove patient information from the definition of PHI fifty years after death.

- Enforcement
  - Apply HITECH's enforcement tools vigorously.
  - Develop penalty factors related to whether data was actually used for an unauthorized purpose.

- Fundraising
  - Establish an opt in standard for fundraising communications to patients that use PHI beyond demographics and dates of service.
  - Require that patients have the choice of opting out of single campaigns or all fundraising communications.

- Minimum necessary
  - Work with industry and consumer groups to establish a safe harbor detailing how covered entities can apply minimum necessary requirements.

- Individual access
  - Establish a timeframe of three business days for covered entities to respond to patient record requests.
  - Encourage industry to provide patients with the ability to download their health information.

- Patient record restrictions
  - Work with providers to ensure patients understand their responsibilities when requesting disclosure restrictions.

I. Marketing

a. Treat all subsidized communications as marketing

According to surveys commissioned by the Markle Foundation, most Americans support the movement toward electronic medical records but a significant portion is very concerned about privacy. Specifically, 89 percent said they were concerned about marketing firms getting access to their personal health information online, with 77 percent describing themselves as "very concerned."[3] Consequently, protections against the unauthorized use of personal health information for marketing purposes are critical to building public trust in new e-health systems. CDT has previously expressed concerns that the HIPAA Privacy Rule provides inadequate protections against the unauthorized use of patient information for marketing.[4]

Currently, covered entities are not required to obtain patient authorization before using protected health information (PHI) to send communications that fall under the Privacy Rule's exceptions to the definition of marketing. These exceptions include communications about treatment and those that direct or recommend alternative therapies, health care providers, or settings of care to the individual patient.[5] HHS established these exceptions to avoid obstructing educational communications related to a patient's health care or health benefits.

This rationale falls short, however, when the covered entity is being paid by the manufacturer or service provider to make the communication. Without a doubt, communications paid for by product manufacturers or suppliers that urge patients to buy, use or ask their physicians about the manufacturers' or suppliers' products are *marketing*. The fact that the communications are sent by the covered entity on a manufacturer's behalf does not make them any less so.

In HITECH, Congress responded to consumer concerns and defined marketing to include circumstances where a covered entity receives "direct or indirect remuneration" from an outside company (such as a product manufacturer or service provider) to make a communication that encourages an individual to buy or use that company's product or service.[6] Unfortunately, the actual language of this HITECH marketing provision is poorly

---

[3] Study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006), http://www.markle.org/downloadable_assets/research_doc_120706.pdf.

[4] Center for Democracy & Technology, *Policy Framework for Protecting the Privacy and Security of Electronic Health Information*, Pgs. 11-12, May 14, 2008, http://cdt.org/paper/policy-framework-protecting-privacy-and-security-electronic-health-information. *See also* McGraw et. al., *Privacy As An Enabler, Not An Impediment: Building Trust Into Health Information Exchange*, Health Affairs, Vol. 28, No. 2 (2009): 416-427, http://content.healthaffairs.org/cgi/content/abstract/28/2/416. *See also* Promoting the Adoption and Use of Health Information Technology, Statement of Deven McGraw, Director of the Health Privacy Project at the Center for Democracy & Technology, before the House Subcommittee on Health to the Committee on Ways & Means, Jul. 24, 2008, http://www.cdt.org/files/pdfs/20080724mcgraw.pdf.

[5] 45 CFR 164.501.

[6] Section 13406(a).

drafted. Specifically, HITECH declared that marketing communications paid for (directly or indirectly) by outside entities "would not count as a *health care operation*" (emphasis added).

In the NPRM, HHS declares that this language creates uncertainty as to Congress' intent: "Specifically, it is unclear whether Congress intended to restrict only those subsidized communications about products or services that are less essential to an individual's health care (*i.e.,* those classified as health care operations communications) or all subsidized communications about products or services, including treatment communications."[7] On one point, however, Congress was crystal clear – patient consent or authorization would not be required to use PHI to send subsidized communications about a drug or biologic that the patient is currently taking, as long as the payment for the communication was reasonable in amount.[8]

Unfortunately, in an attempt to resolve this perceived uncertainty, HHS in the NPRM establishes a confusing distinction between subsidized communications that are treatment and those that are health care operations. The feature distinguishing communications for treatment versus operations is whether the communication is made on an individual or population basis.[9] Under the NPRM, prior patient authorization would be required to send subsidized communications that are population-based and therefore qualify as health care operations. However, prior authorization would <u>not</u> be required to send subsidized communications for *treatment*, as long as the communications are tailored to an individual's health condition. Instead, subsidized treatment communications are subject to other requirements: the provider must notify the patient of its intent to send the patient subsidized treatment communications; the notice must inform the patient that she may opt out of receiving such communications; and the treatment communication itself must reiterate the patient's ability to opt out and disclose the fact of that someone paid the provider to send the communication.[10]

Although we appreciate HHS' efforts to resolve perceived ambiguities in the HITECH language, we are concerned that the distinction between population health and treatment is not as obvious as HHS proposes. If providers are left to determine which subsidized communications are for population health and which are for treatment, the influence of the subsidy is likely to result in PHI being used more frequently for marketing without an individual's authorization. For example, the NPRM arguably would not require prior authorization for covered entities to send their patients letters from drug companies encouraging them to switch from their current drug to another brand. Congress may not have enacted crystal clear language on this issue, but Congress clearly expressed an intent to enact greater protections around the use of individual information for marketing purposes.

In the NPRM, HHS offers two examples of the distinction between these two types of communication. Communications about a specific birthing center "suited to the patient's particular needs" is recommending a setting of care specific to the individual's condition,

[7] 75 Fed. Reg. 40885-40886.
[8] Section 13406(a)(X).
[9] 75 Fed. Reg. 40886.
[10] Id. at 40885-40887.

which constitutes treatment of the individual.[11] However, a blanket mailing to all patients with information about a new affiliated physical therapy practice is a population communication, presumably because it is sent to all patients.[12] The distinction is easy in these two examples because they represent two ends of a spectrum. But a communication need not be sent to all patients to be a population communication. In the former example about the birthing center, if the communication had been sent to all pregnant patients regardless of type of pregnancy (high vs. low risk, for example), the communication is still a population communication because it is sent to a population of patients without any determination of the particular or specific needs of the patients receiving the communication. Similarly, communications that encourage "all patients with diabetes" to purchase or ask their doctor about a particular therapy are population-based, because the provider is not making a judgment call to recommend the therapy based on the patient's particular needs and circumstances.

HHS' attempt to distinguish between individualized treatment and population-based care does not reflect the considerable overlap and nuance in these concepts. Chronic disease has overtaken communicable disease as the leading cause of death in the United States, and chronic disease treatments or interventions (including medications prescribed by physicians) are primarily medical.[13] Consequently, medical providers caring for patients are both acting on a treatment and population basis. Publications on the website of the Center for Disease Control, the federal agency charged with overseeing population health initiatives, include recommended medical interventions for individuals with chronic conditions like diabetes and heart disease.[14] In recent testimony before the Meaningful Use Subcommittee of the Health IT Policy Committee, several providers noted the importance of considering population health as function of health care that is as primary as individual treatment.[15]

Congress also didn't seem to understand the distinction. The new marketing provision expressly applies to "operations" communications - yet policymakers created an express exemption for communications about drugs and biologics that the patient is already taking, which would seem to be treatment communications. If the distinction is not easily made by materials from the CDC or by Congress, it is hard to see how it could be objectively and fairly made on a consistent basis by providers who also may be influenced by the receipt of the subsidy.

---

[11] Id. at 40886.
[12] Id.
[13] Mariner, Wendy K., *Medicine and Public Health: Crossing Legal Boundaries,* Journal of Health Care Law and Policy, vol. 10, at 144 (2007) (see in particular section III, "Medicalization of Public Health or Public Healthification of Medicine").
[14] Center for Disease Control, *Chronic Disease Prevention and Health Promotion*, http://www.cdc.gov/chronicdisease/resources/reports.htm (last updated Dec. 17, 2009).
[15] Health IT Policy Committee Meaningful Use Workgroup, *Public Hearing on Population Health*, Jul. 29, 2010, http://healthit.hhs.gov/portal/server.pt?open=512&objID=1472&&PageID=17094&mode=2&in_hi_userid=11673&cached=true#072910. See, in particular, the testimonies of Ross, Cheatham, and Parsons.

We urge HHS to instead consider all subsidized communications[16] to be marketing requiring prior individual authorization. From the patients' perspective, the distinction between individual- and population-based communications does not matter; patients experience the communication as marketing. Even a well-constructed opt-out provides individuals with far less protection for their information than a requirement for prior authorization. Given individuals' high degree of concern over the use of their electronic health information for marketing purposes, as well as the urgent need to build a strong trust foundation for more widespread electronic health information exchange, HHS should pursue an option that is more protective rather than less.[17]

We do not believe such an approach is contrary to HITECH, and it is consistent with Congressional intent. The language in HITECH requires HHS to make subsidized health care operations communications subject to prior authorization; but the remaining provisions in the HIPAA marketing rules are all contained in regulation and within HHS' discretion to modify to advance public policy goals. Further, Congress clearly was concerned about subsidized treatment communications and intended for them to be considered marketing – otherwise, there would have been no need to create an express exemption for reasonably subsidized communications about drugs and biologics that the individual is already taking. We submit that the reference to "health care operations" in the HITECH language instead represents rushed drafting that reflects confusion about the distinction between operations and treatment in the Privacy Rule. We note that the definition of health care operations includes activities that some would consider to also qualify as treatment, including recommending alternative therapies or settings of care, care coordination and case management.[18] In contrast, the definition of treatment is fairly broad and does not enumerate any of these particular activities.[19]

Although there is support for HHS' interpretation in the text of the Privacy Rule "operations" definition, that definition also supports an interpretation that care coordination, care management and providing information about treatment alternatives are not exclusively "population" activities.[20] In addition, because the Privacy Rule largely imposes the same set of rules for treatment and operations, there has been little need from a policy standpoint to distinguish between the two. If the distinction has not been

[16] Except, of course, those covered by the exception for communications about drugs or biologics that the patient is currently taking.

[17] In addition, the HIPAA Privacy Rule should not exacerbate the ethical conflicts that arise when physicians and other providers are paid by drug manufacturers to send communications to patients. See, for example, Brezis, M., *Big pharma and health care: unsolvable conflicts of interest between private enterprise and public health*, Isr J Psychiatry Relat Sci 2008; 45(2): 83-9; Jane E. Henney, *Safeguarding Patient Welfare: Who's in Charge*, Annals of Internal Medicine, vol. 145, no. 4, 305-07; Landefeld, CS & Steinman, MA, *The Neurontin legacy – marketing through misinformation and manipulation*, N. Engl J. Med. 2009, Jan.8: 360(2); 103-06.

[18] 45 CFR 164.501.

[19] Id.

[20] The term "population-based" could be read as modifying or describing only those activities that immediately follow the use of the term, prior to the comma – those after the comma are separate and distinct. Had OCR wanted to be more clear that all activities described in that particular section of subpart (1) of the definition of operations, the provision could read "population-based activities relating to improving health… such as" (emphasis added).

historically clear or relevant in the past, Congress likely did not intend to distinguish between subsidized treatment and operations communications.

b. In the alternative, provide more clarity on the distinction between communications for treatment and population health

If HHS seeks to maintain its distinction between treatment and operations communications, we urge the Department to provide more clarity on the distinction in order to ensure that only those communications that are for treatment are exempted from the requirement to obtain prior authorization for subsidized communications. We recommend HHS more clearly adopt the following distinction:

- Treatment communications are those that are based on a specific evaluation by the treating provider of a patient's particular unique needs and circumstances.

- Population communications are those sent by providers to classes of patients, such as all patients with a certain diagnosis, or taking a certain drug (in the latter case, the communications are to suggest alternative or adjunctive therapies), where there is no individualized determination of need.

The former communications, tailored to a patient's particular needs, are treatment (and patients could opt-out of receiving them); the latter, aimed at the health of patients in population groups, are population-based and therefore operations (and patients must provide prior authorization to receive them).

Under such an interpretation, HHS could maintain its distinction between treatment and operations communications, while providing the strongest protection against patients' PHI being used for marketing purposes without authorization. If HHS continues to maintain this distinction in the final rule, we urge HHS to be more clear about the distinction and to provide more examples regarding how it would be applied.

c. Maximize effectiveness of opt-out for individuals

We agree with HHS that "the opt out method provided to an individual for subsidized treatment communications may not cause the individual to incur an undue burden or more than a nominal cost."[21] HHS states that it "encourages entities" to consider using toll-free phone numbers, an opt out e-mail address, or similar mechanisms. For many providers, the sending of the subsidized communications is core to their business operations, thus some may have a strong incentive to have as few patients opting out as possible. To ensure that individuals are indeed provided with a range of easy-to-use mechanisms for opting out, HHS should strengthen this language in the final rule and *require* covered entities to use reasonable efforts to provide individuals with a range of simple, quick and inexpensive ways to opt-out.

Merely including notice in the treatment communication or burying it in the HIPAA notice of privacy practices is <u>not</u> sufficient. Patients should receive separate notice of their right to opt out before any subsidized communications are sent. Patients should be further

[21] 75 Fed. Reg. 40886.

notified of their right to opt out whenever a material change to the notice is made, and ideally once per year after the initial notice.

In addition, patients should also be notified in each subsidized treatment communication. The notice that the communication is paid for by a third party should appear close or next to the statement that the patient may opt out of the communication. HHS should consider requiring an additional statement, also near the opt out statement, informing patients that their personal health information was used to individualize the communication. Taken together, these statements should be no more than one paragraph long, be in a prominent position on the notice (such as in a box or other highlighted area), and appear in typeface no smaller than the body text. Patients should be provided with an opportunity to opt-out of *all* subsidized communications in each communication.[22]

The proposed opt out for treatment communications is complicated by increased data sharing that is the goal of the federal efforts to encourage the use of health IT to improve individual health and reform the health care system. If patient data is shared with multiple entities, patients should not have to make separate requests to each entity in order to fully opt out. For example, if a provider opts out with a covered entity, he or she should not have to further opt-out with that covered entity's business associates, with separate establishments that are part of the same chain or under common control, and other partners who may use a common system of records. HHS also should further explore ways to apply one opt out to all subsidized treatment communications, such as a universal do-not-market system similar to the do-not-call list for telemarketers.

d. Interpret marketing exemption to include generics but not new formulations

Congress specifically exempted subsidized communications about drugs or biologics that an individual is currently taking, as long as the subsidy is reasonable, to ensure patients receive communications that further their health care. Consistent with the goal of improving the cost and efficiency of health care, we support extending this exemption to the generic (or follow-on) form of the drug or biologic as an alternative therapy communication. HHS should explicitly exempt communications about cheaper generic equivalents from the definition of marketing. The larger goal of reducing patients' health care costs offsets the privacy issues in this limited circumstance.

However, we do not think this exemption should be extended to new formulations of the drug. Often manufacturers seek to subsidize communications about new drug formulations in order to maximize revenue during the phase of patent protection (which is often extended by pursuing patents on new formulations of drugs whose patents are due to expire or have expired). Physicians prescribe more expensive drugs when manufacturers focus their sales efforts and subsidize communications on newer, branded drugs instead of less expensive generic alternatives.[23] Higher prescription rates

[22] Providing an opportunity to opt out of a specific subsidized campaign is acceptable, as as long as it is accompanied by an opportunity to opt-out of all subsidized communications.
[23] See Amicus Brief of AARP et al. in support of defendant in *IMS Health Inc. v. Ayotte, 490 F.Supp.2d 163 (D.N.H. 2007)*, at 14-15, http://epic.org/privacy/imshealth/aarp_amic.pdf.

of costly drugs drive up the cost of health care overall and contribute to underuse of medication by those with limited resources.[24] HHS should not extend the marketing exemption to communications about newer, more expensive formulations of the branded drugs the patient is already taking. In this circumstance, the more compelling goal is to protect individuals from having their personal information used for marketing purposes without their authorization.

e. Eliminate potential loophole for indirect subsidies

Finally, we note that Congress was concerned about both direct and indirect subsidies for marketing communications. In the NPRM, HHS notes that if the communication is sponsored by a nonprofit entity or foundation, that does not qualify as a subsidized communication requiring patient authorization.[25] We caution that this language could result in drug and medical product manufacturers establishing nonprofits, or channeling marketing funds through existing nonprofits, in order to avoid triggering the rule. It would be difficult and perilous for HHS to determine on a large scale whether the nonprofits sending communications are truly independent enough that they should be considered to be exempt from the rule. HHS should eliminate the distinction between marketing communications sent by companies or subsidized through nonprofits, and instead require patient authorization for this type of marketing communication.

f. Retain current exemption for face-to-face communications

Finally, CDT supports HHS' decision to keep intact the current exemption of face-to-face communication from the definition of marketing. The communications that take place in a pharmacy or in a doctor's office, or in a hospital, are for patient education purposes (and in the case of the pharmacy, part of mandatory patient counseling). It is true that in some cases there may an external subsidy for these communications and the promotion of certain products and services. However, patients can easily and readily refuse to accept the sponsored communication in a face-to-face encounter, and such encounters do not involve the use of patient information in a way that is not immediately known to the patient.

II. Business Associates

a. Clarification on accountability for subcontractors is an excellent step forward

We strongly support the clarification that the accountability of business associates under HITECH extends to subcontractors.[26] Prior to the enactment of HITECH, the reach of the HIPAA Privacy Rule was limited in its scope of protection and accountability as data flowed from the covered entity to business associates to subcontractors. The break in the chain of public accountability once information was disclosed downstream breached the public's trust and was an obstacle to encouraging greater information flows to

[24] Id. at 12-13.
[25] 75 Fed. Reg. 40885.
[26] Id. at 40873.

improve individual and population health. Congress clearly intended to close this loophole by enacting the business associate provisions in HITECH. The clarifications made in the NPRM regarding subcontractor accountability, including the proposed language regarding business' associate liability for failure to take steps to cure material breaches of subcontractor agreements, realize Congress' intent and take positive steps toward maintaining a more consistent level of accountability for privacy protection as personal health data moves downstream.

b. HHS must strengthen Business Associate Agreements

In its NPRM, HHS restates some key provisions of the Privacy Rule regarding the role of business associate agreements (BAAs). In particular, proposed section 164.504(e)(2) states that BAAs must establish the permitted and required uses and disclosures of protected health information (PHI) by the business associate… [and] may not authorize the business associate to use or further disclose the information in a manner" that would violate HIPAA. The BAA also must bind the business associate to not using or disclosing information other than as permitted or required by the contract or as required by law.[27]

These provisions indicate that the BAA should be a tool for limiting a business associate's use and disclosure of PHI received from a covered entity. Unfortunately, the NPRM retains other BAA provisions from the Privacy Rule that have historically been viewed by consumer and privacy advocates as providing business associates with too much discretion with respect to uses and disclosures of PHI. For example, BAs are still permitted to use *and disclose* PHI for the "proper management and administration of the business associate" and to "perform data aggregation services."[28] BAAs also are still allowed to permit business associates to use PHI "to carry out the legal responsibilities of the business associate."[29]

The result of these overly broad provisions has, at a minimum, created a perception that business associates have not been sufficiently limited in what they can do with patient data. There is at least anecdotal evidence that questionable use of PHI is occurring.[30] Sweeping contractual language can enable business associates to indulge in creative expansion of their mandate and permit them to chase additional revenue streams with patient data. Given the increasingly important role that business associates will play in facilitating the exchange of PHI to improve individual and population health, the failure to use BAAs as a tool to more clearly limit how business associates can use and disclose PHI weakens the trust foundation for electronic health information exchange.

Now that the law holds BAs directly accountable for HIPAA compliance, HHS should make clear that the single most important function for BAAs is appropriately limiting access, use and disclosure of PHI. Business associates are service providers to covered health care entities, and patient privacy protection would be weak if the HIPAA Rules

[27] Proposed 164.504(e)(2)(ii)(B).
[28] Proposed 164.504(e)(2)(i).
[29] Proposed 164.504(e)(4)(i)(B).
[30] See, e.g., Change to win, *CVS Caremark: An alarming prescription*, Pgs. 15-21, Nov. 2008, http://www.alarmedaboutcvscaremark.org/index.php?id=37.

were the only real limitation on their uses and disclosures of PHI.[31] The BAA should be a crucial protection against business associates using patient PHI to profit in ways that are not related to performing the particular services for which covered entities contracted.

To make BAAs an effective privacy protection, HHS should revise the BAA provisions in the Privacy Rule to require those contracts to clearly spell out the services the covered entity is hiring the business associate to carry out. HHS should also require BAAs to limit uses and disclosures of PHI only to those reasonably needed to complete and administer those specific services. These limitations should also be expressly required to be carried forward in subcontractor agreements and further limited if the scope of services to be provided by the subcontractor is narrower than the scope of the initial BAA.

We urge HHS to consider the recent recommendations of the Privacy and Security Tiger Team of the Health IT Policy Committee.[32] The recommendations applied Fair Information Practice principles to third party service organizations, like business associates, to promote trust in health information exchange. The Tiger Team recommended that third party service organizations be permitted to collect, use, disclose, reuse or retain patient information only to the extent necessary to perform the functions specified in their service agreement or BAA (and any administrative activities necessary to support those contracted functions).[33] These recommendations were unanimously endorsed by the Health IT Policy Committee on August 19, 2010.

c. HHS should offer consistent rules and guidance for PHRs, and in the interim, clarify when PHRs are required to be business associates

Personal health records (PHRs) hold significant potential for consumers and patients to become key, informed decision-makers in their own health care. By providing individuals with options for electronically storing and sharing copies of their health records, as well as options for recording, storing, and sharing other information that is relevant to health care but is often absent from official medical records (such as pain thresholds in performing various activities of daily living, details on side effects of medication, and daily nutrition and exercise logs), personal health records can be drivers of needed change in our health care system.

HITECH provides that a PHR that contracts with a covered entity to offer a PHR as part of the covered entity's electronic health record shall be treated as a business associate.[34] Promptly upon passage of HITECH this provision was commonly interpreted

[31] For example, the Privacy Rule gives covered entities broad discretion to use and disclose PHI for treatment, payment and operation purposes without patient consent. 45 CFR 164.501. It would be inappropriate for business associates to operate under such an open-ended mandate.
[32] HIT Policy Committee letter to Dr. David Blumenthal, National Coordinator for Health IT, Pgs. 2-3, Aug. 19, 2010, http://healthit.hhs.gov/portal/server.pt/document/947492/tigerteamrecommendationletter8-17_2_pdf_%282%29.
[33] Id. at 6.
[34] Section 13408.

to render all PHRs covered by HIPAA.[35] Unfortunately, the NPRM did nothing to settle this controversy, resulting in considerable uncertainty for consumer and patients, as well as for industry.

CDT has called for consistent baseline privacy and security protections for all PHRs, regardless of who is offering them.[36] If such consistent protections were in place, there would be little need to determine whether or not a particular PHR was or was not covered as a business associate.

In June 2008, Markle Connecting for Health released the Common Framework for Networked Health Information outlining a uniform set of meaningful privacy and security policies for PHRs (which may include copies of health data generated by a covered entity as well as data the individual inputs him or herself).[37] This framework was developed and supported by a diverse and broad group of more than 55 organizations including technology companies, consumer organizations (including CDT) and entities covered by HIPAA.[38] The framework was designed to meet the dual challenges of making personal health information more readily available to consumers, while also protecting it from unfair or harmful practices. The framework is based on the principle that PHRs and other consumer access services are tools for consumers' use, and are controlled and managed by consumers.[39] This paradigm has two central policy implications: 1) That a consistent and consumer-oriented set of rules apply to PHRs regardless of the entity offering them; and 2) That the consumer's preferences with respect to sharing the copy of information in their PHR be recognized and implemented. CDT in 2010 issued a report with further guidance to regulators on how the provisions of the Common Framework could be implemented in law.[40] We hope that the study being conducted by HHS and the Federal Trade Commission (FTC) adopts these recommendations. [41]

---

[35] *See, e.g.,* Vince Kuraitis, *Privacy Law Showdown? Setting the Stage*, e-CareManagement, Apr. 20, 2009, http://e-caremanagement.com/privacy-law-showdown-setting-the-stage.

[36] Center for Democracy & Technology, *Building a Strong privacy & Security Framework for PHRs*, Pgs. 20-21, Jul. 21, 2010, http://cdt.org/files/pdfs/Building_Strong_Privacy_Security_Policy_Framework_PHRs.pdf. See also CDT and the Markle Foundation, Joint comments to HHS Interim Final Rule on *HITECH Breach Notification for Unsecured Protected Health Information Rulemaking*, Pgs. 13-15, Oct. 23, 2009, http://www.cdt.org/files/pdfs/CDT&MarkleComments.pdf. See also, Statement of Deven McGraw, Director of CDT's Health Privacy Project, at the Hearing on Personal Health Records before the National Committee on Vital and Health Statistics Subcommittee on Privacy, Confidentiality & Security on Jun. 9, 2009, http://www.ncvhs.hhs.gov/090609p6.pdf.

[37] See http://www.connectingforhealth.org/phti/#guide.

[38] See list of endorsers of the Markle Connecting for Health Common Framework for Networked Personal Health Information at: http://www.connectingforhealth.org/resources/CCEndorser.pdf.

[39] With such services, consumers may keep electronic copies of personal health information and health-related transactions generated through their interactions with health entities, collected by health-monitoring devices, or contributed by themselves.

[40] Center for Democracy & Technology, *Building a Strong privacy & Security Framework for PHRs*, Jul. 21, 2010, http://cdt.org/files/pdfs/Building_Strong_Privacy_Security_Policy_Framework_PHRs.pdf.

[41] Sec. 13424(b)(1).

Notwithstanding these recommendations, it could be some time before the PHR study is completed and its recommendations actually implemented. As long as there is a difference in regulation between PHRs covered by HIPAA and those that are not, it is critical that HHS provide further guidance in the final rule on the factors that trigger a business associate relationship between a PHR vendor and a covered entity.

In a July 2010 public meeting of the Health Information Technology Privacy & Security Tiger Team, Adam Greene of the HHS Office of Civil Rights answered questions about the PHR business associate provisions, and his answers provided important clues to the circumstances that would trigger the need for a business associate relationship between a PHR vendor and a covered entity: [42]

- "We also include personal health record vendors that are acting on behalf of covered entities, so this should not be seen as all personal health record vendors, but rather, just ones that are basically offering a PHR for a covered entity."

- With respect to "untethered PHRs," "to the extent that they're providing services directly to individuals rather than on behalf of a covered entity, they are neither covered entities nor business associates." Whether or not they are "tethered" does not answer the question – what is relevant is "their overall relationship with the covered entity." He also noted that PHR vendors often have different lines of business and could be a business associate in some respects but not in others.

- If the circumstance is just that patients are offered the capability of uploading their PHI into a PHR, the business associate relationship is not triggered – such a relationship would be triggered if the PHR was actually offering to create the PHR solution for the covered entity.

- Mr. Greene also reiterated that when PHR vendors merely provide covered entities with an interface to upload the information – to establish the necessary connectivity - this would not trigger a business associate relationship. "If it's simply ensuring that there's connectivity, but the PHR is really offering the services directly to the individual outside of the particular covered entity then that probably would not" trigger a business associate relationship.

Mr. Greene noted that he was relying on guidance that OCR had issued in 2008 on HIPAA and PHRs[43] – but this guidance was issued prior to the enactment of the HITECH provision and does not address this issue directly or with any degree of clarity.

---

[42] Privacy and Security Tiger Team, Draft Transcript of Jul. 9 Meeting, Pgs. 7-9, http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_12083_913626_0_0_18/2010-07-09-tiger-transcript.pdf.

[43] U.S. Dept. of Health and Human Services, *Personal Health Records and the HIPAA Privacy Rule*, Pg. 4, http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf (accessed Aug. 9, 2010).

We urge OCR to include more clear official guidance in the final rule on when a PHR vendor is required to enter into a business associate agreement. A summary of the factors initially sketched out by Mr. Greene, as well as those CDT has expressed previously,[44] include:

- Is the PHR offered independently to individuals?
    - Do individuals control the sharing of information into and out of the PHR?
    - Can individuals use their PHR accounts to download information from multiple providers at their discretion?
    - Do individuals have full discretion to open, move or close their PHR accounts?
- What is the nature of the relationship between the covered entity and PHR vendor?
- Is there a direct relationship between the PHR vendor and the individual account holder or is that relationship exclusively or largely between the covered entity and the individual?

HHS should enumerate these factors, and provide helpful examples, when finalizing this rule.

III. Research

In response to concerns expressed by researchers and some patient advocacy groups, HHS has proposed revisions to how individual authorization for research is obtained under the Privacy Rule. The establishment of a trust framework for the use of health information for research purposes is critical to building a learning health care system and to capitalizing on the federal government's significant investment in the meaningful use of health information technology to improve individual and population health.

Unfortunately, the HIPAA Privacy Rule focuses largely on using individual consent or authorization to build trust in research – and the focus of this NPRM perpetuates this flaw. A privacy approach that rests solely on obtaining consumer consent can provide weak protections for consumers and patients.[45] Consent alone cannot be a substitute for a comprehensive approach to privacy that protects consumers and builds trust.[46] Instead, we need a package of privacy and security protections rooted in fair information practices and bolstered by the application of technology solutions. It is critical that HHS establish a framework for research that builds public trust in and support for the use of electronic health information. Focusing too heavily on making consent easier for researchers to obtain risks exacerbating the issues and undermining trust.

[44] Deven McGraw, *Privacy Law Showdown? Legal and Policy Analysis*, e-CareManagement, Apr. 21, 2009, http://e-caremanagement.com/privacy-law-showdown-legal-and-policy-analysis.
[45] Center for Democracy & Technology, *Rethinking the Role of Consent in Protecting Health Information Privacy*, Jan. 2009, http://cdt.org/healthprivacy/200910126Consent.pdf. Markle Foundation, *Beyond Consumer Consent*, Mar. 10, 2008, http://www.connectingforhealth.org/resources/20080221_consent_brief.pdf.
[46] Markle Foundation, *Beyond Consumer Consent*.

We offer below some comments on HHS' proposed changes to the research authorization provisions of the Privacy Rule in order to take advantage of this opportunity. However, we believe these changes will have little impact on improving the availability of patient data for research and could potentially impair patient privacy and confidentiality in the absence of a comprehensive framework of protections for research that do not rely so substantially on the role of individual consent. We urge HHS to reject a piecemeal approach to dealing with privacy and research. HHS should consider the issues raised below as part of a broader, multi-stakeholder effort to more comprehensively address improving access to data for research.

a. HHS should proceed with caution in establishing its cost-based fee for selling patient data to researchers

Under HITECH, covered entities do not require patient consent to transmit PHI to researchers and, so long as any remuneration the covered entity receives is a reasonable fee based on the cost of preparing and sending the data.[47] HHS sought public comment on what types of costs should be included in the data provisioning fee, but this question belies the complexity the fee system introduces.[48] It remains to be seen whether the cap on fees will boost researchers' appetite for patient data in a way that is detrimental to privacy.[49] Supreme Court decisions on cost-based pricing in other industries constrain HHS' discretion in determining what costs should be included.[50] HHS faces the task of developing, administering and overseeing the pricing scheme, with limited personnel capacity to do so.[51]

HHS should consider establishing an interim fee structure as it carefully reviews its options and takes advantage of cost-setting expertise in other industries.[52] HHS should consider this review to be one component of re-evaluating health research policies with an eye towards improving the regulatory framework and relying less heavily on consent.

b. Compound authorizations must be understandable to patients

The HIPAA Privacy Rule prohibits health care providers from conditioning a patient's treatment, payment, or enrollment in a health plan or eligibility for benefits on obtaining an authorization from the patient.[53] There is an exception to this general rule that permits conditioning research-related treatment on an authorization for the research itself, but the current privacy rule prohibits covered entities from "compound authorizations": combining a conditioned authorization with an authorization that is not conditioned. The proposed rule would allow covered entities to combine conditioned and unconditioned

[47] 75 Fed. Reg. 40891.
[48] HHS should review a recent paper by Barbara Evans from the University of Houston, paying particular attention to Sections II-IV. See Barbara J. Evans, *Waiving Your Privacy Goodbye: Privacy Waivers and the HITECH Act's Regulated Price for Sale of Health Data to Researchers*, University of Houston/Health Law & Policy Institute Working Paper No. 2010-A-22, http://ssrn.com/abstract=1660582.
[49] Id. at 14-16.
[50] Id. at 16-25.
[51] Id. at 25-32.
[52] Id. at 32.
[53] 45 CFR 164.508(b)(4).

authorizations for research. However, the authorization must distinguish clearly between the conditioned and unconditioned components and allows patients to opt out of the latter.[54]

This proposal is not unreasonable; by producing less paperwork and offering a simpler format, compound authorizations may make the decision about whether to give authorization easier for patients to understand. However, educating patients on how to distinguish between the conditioned and unconditioned components is a crucial challenge.

The NPRM notes the importance of patient awareness by requiring clear differentiation of the two components and seeking public comment on ways to make this possible. We agree that redundant language should be avoided as much as possible and support separate discussions and check-boxes or signature lines for unconditioned and conditioned authorizations. For example, the check boxes should be designated in a simple but bold manner, such as "OPTIONAL (You can deny authorization and receive treatment)" and "NOT OPTIONAL (You cannot receive treatment if you deny authorization)". We hope to see guidance from HHS on methods providers can use to maximize patient understanding of compound authorizations, ideally based on objective testing of real patients in clinical settings.

c. Authorizations for future research should detail the purposes of future research, should not be conditioned on treatment, and should include means to revoke years after the fact

The NPRM interprets the current Privacy Rule to require that patient authorizations (when not waived) to use or disclose health information for research be specific to each study – one authorization per study.[55] However, the NPRM states that HHS is contemplating whether to modify this rule to avoid having to re-contact the patient for multiple authorizations for future research. More specifically, HHS is considering whether

- To permit an authorization for uses and disclosures of PHI for future research purposes if the future research is described in sufficient detail in the authorization that the patient can make an informed decision,

- To permit an authorization for future research to the extent that the description of the future research contained statements specified by the Privacy Rule, and what those statements should be, or

- To permit the first option as a general rule, but require disclosure statements on authorizations for certain types of sensitive research activities.

We generally believe the third option is the best of the three. We do not believe that all future uses of research are per se nonspecific and therefore inappropriate for HIPAA authorizations. However, blanket authorizations permitting indefinite and undefined use

[54] 75 Fed. Reg. 40893.
[55] Id.

of patient data for research purposes would violate Fair Information Practice principles. A crucial factor is the level of detail regarding the future research that the authorization must provide. The authorization should go beyond general descriptions of the future uses of PHI and should, at minimum, meet the requirements of informed consent for human subjects protection.[56] HHS should consider issuing guidance regarding the sufficient level of detail necessary for patient descriptions of future research.

Treatment of the individual should not be conditioned on an authorization for unspecified future research, and compound forms should highlight when the authorization for future research is optional. Authorizations for sensitive research activities should include still more specific descriptions of the purpose of the future research, and – where applicable – a statement that PHI disclosed under the authorization may be re-disclosed by the recipient and no longer protected under HIPAA.

In addition, authorizations for future research should include statements informing the individual of how to prospectively revoke the authorization. HHS should seek input from covered entities regarding their internal mechanisms that enable patients to revoke authorizations many years after issuance. It may be considerably difficult for patients to track down researchers after years of no contact in order to revoke an authorization.

IV. HHS should rescind the proposed modification to the PHI definition that would exclude sensitive information of patients fifty years after death

The NPRM proposes to exclude from the definition of *protected health information* the health information of individuals who have been dead for fifty years or more.[57] HHS argues that this modification would relieve health care entities from the burden of obtaining authorizations from the decedent's representatives, while the time period would protect the privacy of the decedent's living relatives and direct descendents. We urge HHS not to make this modification in the Final Rule and instead take additional time to review the potential consequences.

Data minimization is a core Fair Information Practice principle, under which entities are advised to retain data only long enough to fulfill a specified purpose.[58] Yet HHS' proposed modification would make it difficult to recommend any limit on data retention. The modification will likely encourage health care entities to alter their data retention practices, keeping patient data far longer than they otherwise might in order to monetize such data after the fifty-year period. The security and privacy risks such a move may introduce have not yet been thoroughly evaluated.

HHS has stated numerous times that the health care system – especially as we transition to greater use of health IT – depends on patient trust in the privacy of health

[56] 45 CFR 46.116(a)-(b).
[57] 75 Fed. Reg. 40895.
[58] U.S. Dept. of Homeland Security, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security,* Pg. 4, Dec. 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

data.[59] HHS makes no reference to any evaluation regarding the extent to which that trust in privacy may be undermined if decedents' health data becomes unprotected, even several decades after the fact. It is imprudent to assume that patients will be comfortable knowing information about embarrassing conditions – which may affect their legacies and sense of dignity – will be made available for unforeseeable purposes. It is also unknown how many patients may engage in privacy-protective behaviors to avoid such disclosure.[60]

In addition, it is imprudent to assume that the decedents' information will have negligible bearing on the privacy of the decedents' relatives. In coming years, science is likely to become much more skilled at predicting individuals' health based on family history. It is unknown whether exposing a long family history of a particular disorder would have adverse consequences on an individual in such matters as employment and insurability, even two generations removed.

If one purpose of the change proposed in the NPRM is to make it easier for relatives to access information that may be needed for their own health, HHS should propose a change (such as to Section 164.510(b)) that can address that specific circumstance. For example, if such information is needed in order to diagnose or treat a blood relative, and it is not possible to efficiently obtain the information from another source, information from a deceased individual's record in the possession of the covered entity can be released as long as the entity is not aware that the individual who is the subject of the information would have objected. In such a case, only the minimum amount of information that is needed to treat the relative should be released.

The unknown consequences and potential loss of trust in the privacy of the healthcare system outweigh the benefits of the modification if, as the NPRM suggests, the primary advantage is merely to avoid the trouble of contacting decedents' representatives for authorizations. Achieving this contact may become increasingly easy to do as communications technology makes the world more interconnected.
HHS should withdraw its proposed change and, at minimum, more closely examine the broad consequences of removing privacy protection from the health data of the dead.

---

[59] See, e.g., U.S. Dept. of Health and Human Services, *Statement on Privacy and Security*, Jul. 8, 2010, http://healthit.hhs.gov/portal/server.pt?CommunityID=2994&spaceID=11&parentname=CommunityEditor&control=SetCommunity&parentid=9&in_hi_userid=11673&PageID=0&space=CommunityPage.

[60] See California HealthCare Foundation, *Americans Have Acute Concerns about the Privacy of Personal Health Information*, Nov. 9, 2005, http://www.chcf.org/media/press-releases/2005/americans-have-acute-concerns-about-the-privacy-of-personal-health-information. Note that patients concerns were focused on employers and insurance, but patients were likely never asked their opinion on the effect of disclosure after death on, for example, their reputations or those of their relatives.

V. Enforcement

a. HHS should maintain vigilant stewardship of HIPAA

Through HITECH and the proposed rule, HHS now has considerably more leverage to enforce HIPAA. Prior to HITECH, HHS had an obligation to try solving compliance issues with covered entities through informal means. HITECH requires HHS to investigate any complaint of a violation if the facts indicate that an organization was willfully neglecting HIPAA rules. HITECH also requires HHS to pursue a civil penalty in cases of willful neglect.[61] The proposed rule implements these provisions and also proposes a modification stating that HHS will conduct a compliance review when a preliminary review indicates willful neglect.[62] We support this modification and are glad to see HHS take initiative in strengthening compliance investigations rather than just those based on patient complaints.

It remains an open question, however, whether HHS will use its new enforcement tools effectively and consistently. HHS has yet to pursue a single civil monetary penalty, although there have been a handful of monetary settlements. For example, in the past two years HHS has extracted two large monetary settlements from drug store chains caught dumping records with sensitive patient data in public trash.[63] Although it is encouraging that HHS took strong action in response to such egregious behavior, HHS started the investigations that led to these penalties because an enterprising television news station exposed the drug stores' violations in 2006.[64] It would be more encouraging if HHS were conducting such investigations on its own, and if it did not take four years before official punitive action was taken – especially when the evidence of a violation is as plain as video footage. We urge HHS to take additional internal steps to maintain a proactive role in HIPAA privacy stewardship.

HHS maintains its discretion regarding whether or not it will conduct a compliance review or a formal investigation in cases where willful neglect is not suspected. We urge HHS to promptly conduct audits, compliance reviews and investigations at a lower threshold than willful neglect, especially in cases involving knowledge of the violation, repeat offenders or particularly sensitive data.

---

[61] Section 13410.
[62] 75 Fed. Reg. 40876-7.
[63] U.S. Dept. of Health and Human Services, *Rite Aid Agrees to Pay $1 Million to Settle HIPAA Privacy Case*, Jul. 27, 2010, http://www.hhs.gov/news/press/2010pres/07/20100727a.html. See also, U.S. Dept. of Health and Human Services, *CVS Pays $2.25 Million & Toughens Disposal Practices to Settle HIPAA Privacy Case*, Jan. 16, 2009, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cvsresolutionagreement.html.
[64] WTHR Eyewitness News, *Prescription Privacy*, http://www.wthr.com/global/Category.asp?c=83157 (accessed Aug. 9, 2010).

b. In addition to harm factors, HHS should focus on what happens to data in determining penalties

We support the inclusion of reputational harm as one of the factors in determining the level of penalty sought for a HIPAA violation. Reputational harm addresses the dignity interest in privacy that is independent of financial loss. We do not believe that regulations should consider harm to individuals to be the determining factor regarding whether a privacy violation has occurred, and we argued against a "harm standard" in comments to HHS on data breach notification rules.[65] But the issue here is the degree of penalty to be imposed, where issues of harm are relevant. Consequently, and consistent with the standards for harm in breach notification, we urge HHS to include "other" harm in the penalty factors in addition to reputational harm.

The penalty factors also should incorporate consideration of what actually happens to the data involved – i.e., whether an unauthorized party accesses the data. This is consistent with HITECH's requirement that HHS consider the extent of the violation, as the gravity of the violation is increased if the data falls into unauthorized hands.[66] In addition, consideration of whether data was accessed by unauthorized parties will achieve greater consistency with breach notification rules. The Federal Trade Commission issued breach notification rules that gave significant weight to unauthorized access to the breached data.[67] A focus on whether data was compromised – not harm to individuals – was also Congress' intent with regard to the breach notification provisions in HITECH that formed the basis of HHS' breach notification rule.[68]

We urge HHS to resist calls to define reputational or other harm with great specificity. As we argued in our comments on breach notification, patients' reputational interest in health information is highly subjective. Patients should only be required to reasonably show reputational or other harm in order for this particular factor to apply.

VI. HHS should establish an opt in standard for fundraising that uses PHI beyond demographics and dates of service

We support the NPRM's proposed prohibition on conditioning treatment or payment on an individual's choice to receive fundraising communications.[69] Although we believe that an opt in standard for fundraising communications that use patient demographic data would have been more appropriate, CDT supports the NPRM's proposals to strengthen the opt out standard established in HITECH – namely, requiring that each fundraising

---

[65] CDT and the Markle Foundation, *Joint comments to HHS Interim Final Rule on HITECH Breach Notification for Unsecured Protected Health Information Rulemaking*, Oct. 23, 2009, http://www.cdt.org/files/pdfs/CDT&MarkleComments.pdf.
[66] Section 13410(d).
[67] FTC Final Rule, 74 Fed. Reg. at 42966.
[68] See Letter from Rep. Henry Waxman et. al. to Sec. Kathleen Sebelius, Oct. 1, 2009, http://energycommerce.house.gov/Press_111/20091001/sebelius_letter.pdf.
[69] 75 Fed. Reg. 40896-7.

communication clearly provide an opportunity for the individual to opt out, and prohibiting a covered entity from sending communications to an individual who has opted out.[70]

HHS seeks public comment on whether to open categories of PHI for use and disclosure for fundraising, or whether to leave intact the current limit of demographic data and dates of service only.[71] In the NPRM, HHS explained that a major impetus behind this inquiry was helping health care target solicitations to patients who received favorable outcomes from their treatment while avoiding soliciting patients who had bad treatment outcomes.[72]

When outside fundraising entities are used (including those who have executed BAAs), we believe the current limit on use of data for fundraising should remain intact and oppose an opt out standard for the use of additional categories of PHI beyond demographics and dates of service. Although the NPRM suggests using broad designations (such as oncology) rather than more specific designations (such as the treating physician), this is still revealing information that patients should have the right to keep private. Health care providers who are unsure of a patient's treatment outcome could ask the treating physician rather than send information to an outside fundraising entity. The arguments HHS lists in favor of reducing patients' privacy in this information appear to be borne out of convenience for health care fundraisers, rather than to provide any benefit to patients. An opt in standard for allowing outside fundraising entities to access such information would be more appropriate.

HHS also sought comment on whether a patient's decision to opt out of fundraising should apply to a single campaign or to all fundraising efforts from the entity sending the communication.[73] We believe individuals should have a choice of both. At a minimum, patients must be provided with the ability to opt out of all fundraising communications – so that if patients are given the choice to opt out by campaign, they must also have a clear choice to opt out of all such communications. Continuing to send fundraising communications to patients who may believe they have opted out of all fundraising risks giving those patients the impression that their privacy choices are not respected. Moreover, it is unnecessarily burdensome to require patients to opt out of every fundraising campaign.

VII. HHS should work with industry to establish a safe harbor detailing what constitutes minimum necessary in different use cases

The HIPAA "minimum necessary" provision requires covered entities to disclose the minimum amount of information as necessary to accomplish specified purposes.[74] We support HHS' proposal to extend the minimum necessary requirement to business associates.[75] The minimum necessary requirement implements the fundamental Fair Information Practice of data minimization, as well as collection and use limitations, and is

[70] Id.
[71] Id. at 40897.
[72] Id.
[73] Id.
[74] Id. at 40896.
[75] Id. at 40887-8.

key to effective health information privacy. Articulating the requirement with specificity can be challenging, however, because of the diversity of data needs for different health care transactions and use cases.

HITECH requires HHS to issue guidance on what constitutes "minimum necessary".[76] In the NPRM, HHS seeks public comment on what aspects of the minimum necessary standard would be most helpful for the guidance to address.[77] At a minimum, HHS should make clear in its guidance that minimum necessary applies to the identifiability of data in addition to the amount of clinical content needed for a particular purpose. For many routine uses under HIPAA (for example, health care operations and public health), fully identifiable data may be used when it is typically not needed or required. Congress clearly understood this concept, as the HITECH provisions on minimum necessary begin with an interim provision declaring a limited data set to satisfy the minimum necessary standard.[78]

We also urge HHS to consider encouraging a safe harbor regime that addresses the core issues the public raises in response to the NPRM. A safe harbor strategy recognizes differences in performance by treating actors who qualify for safe harbor more favorably than those who do not.[79] One advantage of a safe harbor in the minimum necessary context is that the requirements needed to qualify for the safe harbor could be tailored to different sectors of the health care system. The safe harbor requirements could act as a set of industry best practices, adherence to which qualifies as de facto compliance with the minimum necessary requirement. Other favorable treatment for companies meeting safe harbor requirements could include exemption from certain liabilities or penalties.[80] The purpose of the safe harbor is not to encourage mere compliance with legal requirements, nor is it a pathway for entities to self-regulate based on weak standards. Rather, entities seeking to qualify for safe harbor would have to demonstrate that their privacy practices are more protective than those that the letter of the law requires.[81]

Safe harbors are most effective when the requirements are developed through a collaborative process involving industry stakeholders, government representatives and consumer groups. The safe harbor regime must have independent approval and oversight components to ensure companies applying for safe harbor actually meet the standards and maintain compliance over time. No health care entity should be deemed to qualify for safe harbor without first undergoing a comprehensive audit to ensure compliance with the requirements.

---

[76] Section 13405(b)(1)(B).
[77] 75 Fed. Reg. 40896.
[78] Id.
[79] There is recent precedent for safe harbors in the health IT privacy and security arena. HHS established a safe harbor in its interim final rule on breach notification for health information. See U.S. Dept. of Health and Human Services, Interim Final Rule on Breach Notification for Unsecured Protected Health Information, 45 CFR 164.402 (2010).
[80] Letter to Chairman Rick Boucher from Professor Ira Rubenstein, Jun. 1, 2010.
[81] Ira Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, Public Law & Legal Theory Research Paper Series, Working Paper No. 10-16, New York University School of Law (Mar. 2010), http://ssrn.com/abstract=1510275. Note: Professor Rubinstein serves on the CDT Board of Directors.

In addition to considering a safe harbor for industry, HHS should develop guidance for government agencies. The guidance should provide details on how to incorporate the minimum necessary requirement in agencies' funding and procurement activities, and also with respect to how they collect and disclose patient data.

VIII. Individual Access

a. HHS should establish a timeframe of three business days for covered entities to respond to patient record requests

The proposed rule would modify the timeliness requirement for fulfilling patient requests for access or copies of PHI. Currently it is at thirty days, with the possibility for a thirty-day extension.[82] In the NPRM, HHS states that it wants to reduce this timeframe for electronic records, and prefers a single standard that applies to electronic records generally. HHS seeks public comment on the appropriateness of a single time standard for providing access to or copies of electronic health information to individuals upon their request.[83]

HHS deserves praise for its initiative to reduce the time it takes for patients to get a copy of their records. Patient activists have often criticized the present timeframe and attendant costs as burdens to effective self-care.[84] It is impossible for patients to take an active role in managing their health if they have to wait weeks or even a month (much less two months) to obtain copies of their information. As we enter the age of electronic health records, the technology to provide quick access and digital copies is widely available and the thirty-day timeframe for electronic records is not justified.

We believe that three business days is an appropriate turnaround time for providers to respond to record requests from their patients. In comments to proposed rules on meaningful use for electronic health records, consumer groups argued for a standard of 48 hours for patients to receive copies of health information.[85] The meaningful use rule ultimately settled on a timeframe of three business days, which is still significantly better than thirty days.[86] Early adopters of the incentive program must hit this timeframe for 50% of their patients, so clearly HHS believes this is an obtainable goal. Applying the same three-day standard to HIPAA has the advantage of establishing consistency among providers who are meaningful users and those who are not, reducing confusion among patients who may be dealing with multiple providers.

---

[82] 45 CFR 164.524.
[83] 75 Fed. Reg. 40903.
[84] Elizabeth Cohen, *Patients demand: 'Give us our damned data'*, CNN Health, Jan. 14, 2010, http://www.cnn.com/2010/HEALTH/01/14/medical.records/index.html.
[85] See, e.g., Markle Foundation, Center for American Progress, and Brookings Institute, *Collaborative Comments on the Centers for Medicare and Medicaid Notice of Proposed Rulemaking for the Electronic Health Record Incentive Program*, Pg. 13, Mar. 15, 2010, www.markle.org/downloadable_assets/20100315_ehrincent_cms0033p.pdf.
[86] 75 Fed. Reg. 44330.

b. HHS should encourage covered entities to adopt patient download capabilities

HHS invites public comment on whether CEs have the capability to provide an electronic copy of electronic PHI through secure web-based portals, emails, on portable electronic media, or other methods.[87] We urge HHS to explore setting standards and incentives that encourage the industry to develop and support the capability to download PHI. HHS should deem a download button to an acceptable way for covered entities that use web-based portals to provide patients with electronic copies and access to their records. If the data the patient seeks is not available through the covered entity's download service, the covered entity should still provide other means to the patient to obtain the data.

There is precedent for the download capability in the federal health architecture. In late August 2010, working with the Markle Foundation and the Department of Defense, the Department of Veterans Affairs launched a download feature on its electronic patient portal.[88] The Centers for Medicare and Medicaid Services is developing a download capability for beneficiary claims data, slated to launch sometime this fall.[89] With significant patient populations – namely veterans and Medicare beneficiaries – poised to enjoy the benefits of a download capability, the time is right for HHS to examine how a download capability can enhance patient care in the health industry as a whole.

A download capability has several advantages. A download capability can put patients' data literally in their own hands, breaking down barriers to access. It would help providers and data sources by alleviating the need for a user interface, which would be especially beneficial to those who do not have the resources to offer a secure portal.[90] A download capability would also separate data from applications, giving patients more choices regarding which programs and applications analyze and use their data.[91] This increase in data portability and consumer choice should drive interoperability standards and industry innovation.

Entities providing download capabilities will need to inform to patients of the policies and risks of using the download function, have a means to confirm the individual's consent to download PHI at the point of decision, use immutable audit logs, and include timestamps in the data indicating when it was downloaded.[92] The Markle Foundation has developed a set of policies that apply the widely endorsed Common Framework for Networked Personal Health Information specifically to download capability.[93] HHS should use these model policies to establish a framework with respect to covered entities' use of the

---

[87] Id. at 40901.
[88] Dept. of Veterans Affairs, *Blue Button Home*, http://www4.va.gov/bluebutton (updated Aug. 31, 2010).
[89] Centers for Medicare and Medicaid Services, *Blue Button Initiative*, https://www.cms.gov/NonIdentifiableDataFiles/12_BlueButtonInitiative.asp (last modified Sept. 1, 2010).
[90] Markle Foundation, *Policies in Practice: The Download Capability – Vision & Overview*, Pg. 3, Aug. 2010, http://www.markle.org/downloadable_assets/20100831_dlcapability.pdf.
[91] Id. at 4.
[92] Id. at 6.
[93] Id.

download capability. HHS should also work with NIST to develop guidance on identity proofing and authentication of individuals and automated services.[94]

IX. Providers should ensure patients are aware of their responsibilities when requesting disclosure restrictions

The Privacy Rule allows patients to request restrictions of PHI for treatment, payment and operations purposes, and covered entities who choose to honor the request must document the restriction in writing and abide by it.[95] HITECH requires covered entities to agree to patient requests for the restriction of uses and disclosures of PHI to a health plan for payment or health care operations purposes, provided the patient pays out of pocket in full for the underlying health care service.[96] We commend HHS for underscoring this legal requirement and encouraging open dialogue between providers and patients.

We support HHS' proposal to permit additional parties other than the individual patient to pay out of pocket and trigger the right to request a disclosure restriction.[97] We also agree with HHS' interpretation of Congress' intent to allow patients to restrict disclosures of particularized health issues, rather than requiring patients to restrict all or nothing.[98] We support HHS' clarification that a provider may not unilaterally terminate the restriction.[99] Regarding the obligation of providers to notify downstream entities of a patient's disclosure restriction, we support encouraging the development of electronic means of notification so that when a patient's record is sent from one provider to another, the restriction is clearly visible to the downstream provider. In the absence of this technical capability, providers should maintain alternatives, such as calling ahead to notify the pharmacy of the requested restriction.

HHS should work with providers to ensure patients seeking disclosure restrictions are aware of these complications. For example, providers referring patients who have requested a disclosure restriction to another provider should inform the patient that the downstream provider must be made aware of the patient's request. Likewise, providers should also inform patients that they must request a restriction on follow up visits for the same health issue in order to continue restricting disclosure to the health plan. Providers should also notify patients that their disclosure request may depend on whether the patient has adequate funds to pay for treatment out of pocket. If the patient's payment is returned to the provider for lack of adequate funds, the provider should make a reasonable effort to contact the patient (i.e., a phone call to the patient's contact number, as well as a letter or an email if the patient has offered email as a point of contact) and secure the funds within a reasonable time period before submitting the invoice to the patient's payment plan.

---

[94] Id. at 10-11.
[95] 45 CFR 164.522(a).
[96] Section 13405(a).
[97] 75 Fed. Reg. 40899.
[98] Id.
[99] Id. at 40900.

X. Conclusion

In sum, our recommendations are the following:

- Marketing
  - Treat all subsidized communications as marketing that require patient authorization. A less desirable alternative is a strong opt out system.
  - Include generic equivalents in the marketing exemption for drugs or biologics the patient is currently taking.
  - Eliminate the exemption for communications subsidized through nonprofits.
  - Preserve the current marketing exemption for face-to-face communications.

- Business associates
  - Require business associate agreements to limit uses and disclosures of PHI only to those necessary to perform specific services listed in the agreement.
  - Issue guidance on which factors determine when PHR vendors operate as business associates.

- Research
  - Develop a comprehensive approach to privacy for research based on more than individual authorizations.
  - Issue guidance on ways providers can maximize patient understanding of compound authorizations.
  - Require authorizations for future research to detail the purposes of future research.

- Decedents' information
  - Rescind the proposal to remove patient information from the definition of PHI fifty years after death.

- Enforcement
  - Apply HITECH's enforcement tools vigorously.
  - Develop penalty factors related to whether data was actually used for an unauthorized purpose.

- Fundraising
  - Establish an opt in standard for fundraising communications to patients that use PHI beyond demographics and dates of service.
  - Require that patients have the choice of opting out of single campaigns or all fundraising communications.

- Minimum necessary
  - Work with industry and consumer groups to establish a safe harbor detailing how covered entities can apply minimum necessary requirements.

- Individual access
    - Establish a timeframe of three business days for covered entities to respond to patient record requests.
    - Encourage industry to provide patients with the ability to download their health information.

- Patient record restrictions
    - Work with providers to ensure patients understand their responsibilities when requesting disclosure restrictions.

We thank you for the opportunity to submit these comments.

These comments are submitted by the Center for Democracy & Technology (CDT) and the following additional supporters:

AARP
Childbirth Connection
Consumers Union
National Partnership for Women & Families
The Society for Participatory Medicine