Archived Policy Statement

Comments to HHS HITECH Privacy and Security Modifications

U.S. Department of Health and Human Services
Office for Civil Rights
Hubert H. Humphrey Building
Room 509 F
200 Independence Avenue, SW
Washington, DC 20201

Attention: HITECH Privacy and Security Modifications, RIN 0991-AB57

Dear Secretary Sebelius:

Genetic Alliance is pleased to have this opportunity to respond to the Notice of Proposed Rulemaking (NPRM) published by the Office of Civil Rights (OCR) on July 14, 2010, to implement the Health Information Technology for Economic and Clinical Health Act (the HITECH Act). Founded in 1986 as the Alliance for Genetic Support Groups, Genetic Alliance has become the world's leading nonprofit health advocacy organization committed to transforming health through genetics. Our open network of over 10,000 organizations connects members of parent and family groups, community organizations, disease-specific advocacy organizations, professional societies, educational institutions, corporations, and government agencies to create novel partnerships. We actively engage in improving access to information for individuals, families, and communities, while supporting the translation of research into services and care.

We recognize the promise of modernized health information technology (HIT) to lower healthcare costs, improve quality and coordination of care, and reduce medical errors, and we are committed to HIT advancements accompanied by privacy protections. To that end, Sharon Terry, Genetic Alliance President & CEO, serves on the Health IT Standards Committee, a federal advisory body established by law to provide recommendations to the National Coordinator for Health Information Technology on the advancement of health IT as an integral component of health reform. She also has personal knowledge of how genetic conditions and the resulting disease issues can disrupt families. Because her children have a genetic condition called pseudoxanthoma elasticum (PXE), she worked intensely to identify and patent the associated gene and serves as CEO of PXE International, a nonprofit advocacy group she founded, which seeks to accelerate tests and treatments for the condition. Her own experience, magnified many thousands of times over by the experiences of individuals and families served by Genetic Alliance, helps fuel our organization's passion to seek medical advances through research. We are also passionate about seeking reforms to health care

systems as a whole, opposing wasteful, ill-advised practices and requirements and advancing broad, collaborative sharing of information, technology, and resources in ways that accelerate progress.

Privacy is a common thread through our work in genetics and healthcare systems: it affects interventional and information-based research, genetic testing and services, newborn screening, biobanks and registries, and informed consent. We strive to harmonize individualized privacy needs with appropriate transfer and use of health information. The guiding principle for our work is to support meaningful, efficacious protections for health information privacy, while maximizing consumer engagement in healthcare, broader dissemination of knowledge, improved efficiency of health care systems, better health outcomes, and research breakthroughs to ease suffering and improve health.

Background

That our current health care system is "broken" is widely lamented. The United States pays vastly more for health care than any other nation, with sadly disproportionate outcomes. We need not explain the basis of the oft-stated litany of complaints here – that the system is expensive, wasteful, uneven and unfair in distributing access to care, bureaucratic, over-regulated, litigious, siloed and antiquated in information technology, and ultimately irrational. Overall costs are becoming, and promise to further become, well beyond the ability of patients, payers, employers, and taxpayers to bear. And, sadly, from the patient perspective, despite remarkable progress, far too many diseases and conditions remain intractable. Some 40% of all treatments fail, and for complex diseases like certain cancers, that figure approaches 90%. For many rare or genetic diseases, no treatment is available at all.

Research, broadly construed, accompanied by better application of knowledge gained through research, is indispensable if society is to successfully address these shortcomings. Both interventional research involving participation of human beings in clinical trials, as well as information-based research using sophisticated analytics performed on huge data sets derived from health care records, are crucial. The Administration's commitment to achieving the goals of health reform -- achieving superior health outcomes, increasing access to care, reducing treatment disparities, improving safety and quality, increasing patient engagement, using comparative effectiveness studies to improve treatment efficacy and value, while bending the cost curve to lessen the crushing financial burdens of the status quo – all rest on more and better research.

The value of informational research was recently stressed by the Institute of Medicine:[1]
Today . . . an increasingly large portion of health research is information based. More and more research entails the analysis of data and biological samples that were initially collected for one purpose and are now being used for another purpose such as research. . . Like privacy, all these health-related activities provide high value to society. Collectively, these activities can provide important information about disease trends and risk factors, outcomes of treatment or public health interventions, functional abilities, patterns of care, and health care costs and utilization. They have led to significant discoveries, the development of new therapies, and

remarkable improvement in health care and public health. Thus, they provide a sense of hope for people with chronic, life-threatening, or fatal conditions. If the health research enterprise is impeded, or if it is less robust, important society interests are adversely affected.

We should see research as a source of hope and benefit. We need to cultivate a deep appreciation for the place of interventional and information-based research in strengthening an evidence-based, value-driven health care system, and be sure that our laws and public policies reflect a high prioritization of research unimpeded by ineffective and expensive barriers. Our comments, therefore, will focus on the anticipated effects of the NPRM and the HITECH statute on research. We will also comment briefly on other provisions that we think enhance – or set back – the overall goals of health care efficiency and value creation.

Provisions in the Proposed Rule affecting Research

- **Ban on Sale of Protected Health Information (PHI), § 164.508(a)(4)**

Genetic Alliance, along with numerous other organizations and governmental entities, actively supports a wide range of research collaborations involving data sharing. At a policy and at a practical level, we work strenuously to remove data silos and barriers to data sharing, knowing that the deployment of data analytics on an unprecedented scale will be necessary to achieve breakthrough medical advances. For example, PXE International, which holds the patent on the PXE gene test and is also led by Genetic Alliance's CEO, only licenses the clinical test to qualified labs who contractually agree to make de-identified test results publicly available for research. Genetic Alliance is a vocal advocate for and provides assistance to the NIH Genetic Testing Registry. Ms. Terry also served on the Genetic Association Information Network as an advisor to develop the data-sharing policies that allowed that very successful NIH project to be created. We also support, participate in, and often help to found innovative collaborations and novel partnerships advancing research and health care system improvements. Many of these collaborations, as well as countless others that we are not involved in, require the sharing of large quantities of health data in order to accomplish their mission. Sometimes these collaborations involve governments, nonprofits, and academia, but they often also involve for-profit technology and health care businesses. The synergy that results from numerous players pursuing aligned goals is vital. We will not receive the return that is possible on our major investments (both public and private), unless data is shared, and genotypes and other biomarkers are correlated with phenotypes.

In this increasingly collaborative health care research world, data liquidity is key. Of course, HIPAA and the research Common Rule already impose authorization and consent requirements for PHI to be used in research, which we do not propose to change and will not lay out here.

However, we are greatly concerned that HITECH, and correspondingly the NPRM, impose new barriers to data liquidity in research through the inappropriate application of the ban on the sale of PHI.

Data transfers are by no means free. Agreements to share must be reached; terms must be negotiated; data sets must be often be isolated, purged, analyzed, and otherwise processed; for Limited Data Sets (LDSs), fully identifiable data must be converted, sometimes painstakingly, into LDSs conforming to HIPAA requirements; electronic or physical transfer or access must be accomplished with corresponding data procedures and controls; and IT security safeguards must be negotiated and applied. These measures do not even address the threshold costs of the data being accumulated, maintained, and protected in the first place, before the sharing request was initiated. **It is utterly unrealistic to think that all the data transfers needed as the basis for accelerated research will take place without corresponding financial payments.**

Furthermore, it is unrealistic to think that data holders would be willing to share or transfer data if the most they can expect is to break even – *i.e.*, to have their marginal costs of preparation and transfer covered. Whether an entity will be able to expect to have all such costs fully covered is a very big if, given the likelihood of confusion, contention, and legal risk related to cost calculations. But even if marginal costs were believed to be fully covered, an entity is, frankly, unlikely to be enthusiastic about devoting its own IT staff to fulfilling the wishes and requests of an outside entity, when it could be using its IT staff to pursue its own goals. If we want data sharing for health research to occur --- and we very much do – then we need to be realistic about the role that compensation plays, and needs to play, in incentivizing needed data movements.

Again, to avoid any potential confusion, we are not advocating the removal of any existing consent mechanisms for research, whether under HIPAA or the Common Rule. **Instead, we are voicing our strong opposition to adding *yet another unrelated and onerous authorization requirement***, applicable whenever data transfers are accompanied by compensation incentives.

We therefore suggest the following changes regarding the ban on the sale of PHI:

- Exempt research from the ban on sale of PHI, without any cost conditions. Our reasons for encouraging the Secretary to use the discretionary authority Congress gave her under HITECH § 13405(d)(2)(G) to add additional exceptions "as similarly necessary and appropriate" and include research among the activities exempted under § 164.508(a)(4)(ii) are laid out above. Consistent with the policy of the Obama Administration, we strongly support the acceleration and expansion of research as necessary to fight disease and improve the value and performance of the beleaguered health care system. Because we recognize that compensation, including compensation above and beyond marginal costs, is necessary to facilitate the movement of the large data sets needed, we strongly urge that research be exempted entirely from the ban. Retaining the cost caps will cause confusion and complexity, which will benefit no one but lawyers. It is unquestionably foreseeable that the cost caps will act as a drag on data movements, which will be exceedingly unfortunate for patients who are waiting for research breakthroughs (as well as taxpayers and patients who would like some relief from the crushing financial costs of the status quo.)

- Exempt quality, safety, and efficiency improvement activities. The legal delineation between quality/safety activities and research is often murky and subject to differing interpretations, so it is thus important to exempt both types of activities explicitly under § 164.508(a)(4)(ii).

Congressional and Administration support for quality, safety, and efficiency improvements could not be clearer. Just a few examples:

- HHS itself is tasked by the Patient Protection and Affordable Care Act of 2010 (PPACA) with creating a national strategy to use health care data to improve quality, efficiency, and transparency of patient outcomes.

- PPACA encourages formation of Accountable Care Organizations, which will promote evidence-based medicine, report on quality and cost metrics, and coordinate care across entities, all of which will require sharing of PHI to coordinate quality improvements.

- The Patient Quality Reporting Initiative (PQRI) extends financial incentives to physicians for reporting quality data to the Centers for Medicare and Medicaid (CMS). CMS will then post aggregated quality and patient experience of care on a Physician Compare website, which will greatly enhance patients' abilities to select physicians based on objective outcomes metrics.

Like more traditional research, these quality-related functions will often involve payments – and sometimes incentive payments in excess of marginal costs – to facilitate data access. These data flows needed to realize vital Congressional and Administration goals could be jeopardized by inappropriate application of the ban on the sale of PHI. The NPRM does not currently contain an exemption for quality assurance or quality or safety improvement services, other than allowing remuneration if a Business Associate performs them on behalf of a Covered Entity. But because many quality activities will involve collaborations of many organizations, that provision will not be broad enough to remove the impediment imposed by the new ban. We thus urge you to use your authority to include quality, safety, and efficiency improvement activities among the "similarly necessary and appropriate" exemptions, which we think is entirely consistent with the health care reform statute's focus.

- We think an outright exemption for research, as stated in (a) above, is far and away the best approach to accelerate research and thus benefit patients. But in the alternative, we suggest the following:

- Exclude Limited Data Sets from the ban on the sale of PHI. In establishing the LDS as a tool to be used without an authorization for legitimate research and public health operations, the Department created a subset of PHI that is "almost-de-identified." The Department did so realizing that this type of data, which may include zip codes and dates but would otherwise meet the definition of de-identified data, is vitally needed for research. Mandatory protections for LDSs include a mandate that the recipient sign a Data Use Agreement agreeing to use the LDS only as permitted, to report any other use or disclosure to the Covered Entity, not to attempt to re-identify any individuals in the data set, and to require any agents or transferees to follow the same restrictions. Because of the reasons stated above regarding research in general, and particularly because of the additional privacy safeguards already applicable to LDSs, we strongly encourage the Secretary to include LDSs among the "similarly necessary and appropriate" exemptions.

- Harmonize the interpretation of "remuneration" and "sale." The title of the statutory exception regarding the ban is "Prohibition on the *Sale* of Electronic Health Records or Protected Health Information," while the statute refers to "*directly or indirectly receiv[ing] remuneration*." The catchall authority in HITECH for the Secretary to add other "similarly necessary and appropriate" exemptions was wisely inserted by Congress – in the midst of a highly rushed legislative setting - in response to concerns about potentially harmful unknown consequences that could arise from an overly broad ban.

With this background in mind, and with the opportunity now afforded to be deliberate and thoughtful in analyzing all potential consequences, particularly those potentially harmful to patients, we urge you to interpret this provision narrowly overall. In particular, we think that "sale" should strictly mean "sale," and "direct or indirect remuneration" refers to the type of payment that is associated with a sale. A sale is a transfer of ownership rights to property in exchange for consideration; a sale is not synonymous with a license or permission to access or use. If I sell you my horse or my data set (whether for direct or indirect remuneration), you own it and can do with it as you please, subject to any extrinsic legal restrictions. On the other hand, if I let you use (or access) my horse or my data set, subject to specified use and temporal restrictions and a mandate that you return it intact, then no sale has occurred. We would urge you to adopt and make clear that a similarly precise and narrow interpretation of "sale" of PHI applies in the context of this statutory ban. "Direct or indirect remuneration," in other words, should modify and expand upon the meaning of "sale," not open up other types of more limited legal arrangements to the proscription.

- Interpret "cost" broadly and clearly in the context of research. If the cost restrictions remain applicable to research, they have an unfortunate likelihood of creating confusion and argument, resulting in legal costs and serious obstacles to data liquidity. Many transactions simply won't occur where disputes about cost seem too complex or irreconcilable among the parties. We also think, as discussed above, it is unrealistic and unreasonable to expect transfers to occur where only marginal costs are recoverable, and this obstacle becomes even graver if recoverable costs are narrowly construed. Therefore, if a cost restriction does remain applicable to research (which we oppose), we think allowable costs must reflect an allowance for capital investment recovery for the electronic health record (EHR) or other data system that facilitated the original data collection plus a reasonable rate of return, plus all marginal costs incurred for negotiation and execution of the data sharing agreement, data extraction, quality control, metrics and analysis, data processing, data transmission, and security controls. The comments on this NPRM offered by the North Carolina Healthcare Information and Communications Alliance (NCHICA), which delineate factors to be included in PHI preparation and transmittal cost calculations, represent a good starting point; however, their list of factors demonstrates just how extraordinarily complex, expensive, and wasteful the cost calculation process is likely to become if cost caps remain applicable to research.

To prevent the highly foreseeable problem of research delays and bloated expenses arising from complicated cost allocation calculations (which could be exacerbated if Institutional Review Boards decide to participate in the calculation process), we encourage the Department to delay any implementation of cost restrictions until you can seek stakeholder input, including from the Institute of Medicine, on how to create a simple safe harbor method. Otherwise, large

amounts of legal, accounting, IT, and even IRB time and money could be wasted disputing about costs. Far better would be to avoid the entire fruitless cost-analyzing exercise by using your discretionary authority to exempt research and quality/safety activities entirely as "similarly necessary and appropriate."

- Remove the new and unnecessary requirement to modify authorizations regarding remuneration. The rule would require § 13405 authorizations – already an unnecessary and unfortunate addition in the research context – to state explicitly that the disclosure will result in remuneration to the Covered Entity. This is unnecessary. It would confuse patients, leading them to inappropriate conclusions, and would unquestionably further chill participation in socially beneficial and legally permissible uses of health data.

- Exempt the disclosure of research results to research funders and others. Covered Entities and research organizations paid for their services in conducting research, including clinical trials, are required to deliver their research results, which may include PHI, to the research funder or other collaborating entities. Of course, participants in research must already give their informed consent and privacy authorizations pursuant to the Common Rule and HIPAA, but § 13405 *adds yet another authorization requirement related to remuneration*. We strenuously oppose adding such a new level of burdensome, bureaucratic and confusing paperwork in the trial enrollment process. We urge you to use your discretionary authority to explicitly provide that disclosing research results in exchange for remuneration is a "similarly necessary and appropriate" exception to the ban.
- Modify the proposed exemption in § 164.508(a)(4)(ii)(E) to permit novel or alternative payment arrangements. This provision appropriately clarifies that payments for activities undertaken by Business Associates on behalf of Covered Entities are exempt from the ban, even if PHI transfers are involved, provided the only remuneration is "by the Covered Entity to the Business Associate." This proviso is too narrow for contemporary and future settings involving novel partnerships and complex HIT collaborations. As just one example, state and regional Health Information Exchanges (HIEs) are struggling to come up with sustainable governance and financing models, not only for the HIEs themselves but also for participating Covered Entities making data available for exchange. Financial models might involve the HIE (which is always a Business Associate, per HITECH) or a government body providing remuneration, direct or indirect, to Covered Entities to cover participation costs. We therefore urge you to strike the limiting phrase "by the Covered Entity to the Business Associate" from § 164.508(a)(4)(ii)(E).

- We cautiously support the new provision in section 164.508(a)(ii)(E) that would exempt from the ban all disclosures permitted by and in accordance with HIPAA, where the remuneration is cost-based, as specified. We are greatly concerned that, without such a provision, a number of legally permissible activities under HIPAA that are socially beneficial and important for health system improvement would become *de facto* banned because they would be subject to new, impossible-to-meet authorization requirements. We remain concerned, however, about the unknown consequences of the new cost restrictions on otherwise legally permissible functions.
- **Compound Authorizations, §164.508(b)(3)**

We support the new regulatory authority for compound authorizations permitting a conditioned activity, like participating in a clinical trial, and an unconditioned activity, like providing specimens for a biorepository or genetic analysis, in a single authorization form. The existing requirement for separate authorizations causes confusion and complaints among research participants and researchers.

To further reduce needless complexity in the trial enrollment process, we recommend that you allow organizations to decide whether an opt-in or opt-out process for unconditioned, ancillary functions, like biorepository participation, is most appropriate, provided the participant clearly understands that she is not required to participate in the unconditioned aspects. Participants are often confused when presented with opt-in boxes that require specific actions in addition to signing the consent documents. Sometimes patients even send in specimens for biorepositories, along with signed consents, but even though they took the trouble to collect and send in the specimens and clearly wanted them to be stored, they failed to notice the need to check a separate opt-in box for the storage. Additional expense and delay is thus needlessly required because they have to be recontacted and asked to check the box and resubmit the paperwork. We thus think organizations should be explicitly permitted to use an opt-out method for any unconditioned research activity, provided the informed consent form clearly differentiates between necessary and optional activities and clearly gives participants the opportunity to decline the latter. The one caveat we would add is that organizations must be aware of the needs of the cohort they work to enroll. For example, an opt-in method for optional activities or services may important with communities such as Native Americans if their general preferences are already known.

- **Authorizations for Future Research**

Currently, an authorization may not seek permission to use or disclose PHI for future unspecified research, but may only seek permission to store the PHI. This interpretation conflicts with the Common Rule, which permits a participant to consent to use of their information in future research as long as the future research is described in enough detail to allow informed consent. This disconnect between the content of the informed consent document and the HIPAA authorization causes confusion, delays, and wasted money in the enrollment process today. The Institute of Medicine has highlighted this problem and recommended that HHS change this rule.

The NPRM solicits comments on the best way to change this provision. We support the option you identify as (1) at 75 Fed. Reg. 40893-94, which is to permit authorizations to seek permission for future research, if adequately described, and we think that "adequate description" can appropriately be quite general. Many research repositories, including Genetic Alliance's biobank, are intended to make data and/or specimens available to support a wide array of research over a long period of time, and it would be impossible at the time of collection to describe future types of research in detail. We do not support the options you set forth as (2) or (3), which we think would unnecessarily hamstring future research by adding complexities to authorization forms and, even worse, paternalistically limiting participants' ability to agree to what they actually want to agree to. Many people faced with critical illness in themselves or their family have a fervent desire to have their data and specimens be used as

broadly as possible in order to advance treatments for anyone similarly suffering. We strongly believe that people are entitled to make those choices for themselves – and without any mandatory carve-outs for purportedly sensitive data like genetic information. To the contrary, many people correctly understand that it is their genetic information that will have its greatest utility in the future as science advances, and they adamantly want their genetic information to be used to its greatest potential to help people.

- **Making Consent Opportunities for Research Easy and Convenient**

Interventional research certainly requires a robust, personal enrollment process of informed consent, whereby individuals make informed decisions about risks. Information-based research, in contrast, involves a different nature and magnitude of risk. At the same time, information-based research has enormous potential as sophisticated techniques for analyzing vast data sets to uncover obscure insights become ever more readily available. The benefits to patients of expanded Comparative Effectiveness and other information-based research are well recognized today, as reflected by solid Congressional and Administration support through HITECH, PPACA, and other initiatives. Studies show a somewhat surprisingly high willingness among the general public to allow their information to be used in medical research, provided they have an opportunity to consent. For example, three-fourths of parents queried said they would be willing to have their child's leftover newborn blood screening samples used in research if they had an opportunity to consent.[2] Such altruism should be encouraged.

Therefore, for information-based research, where consent is legally required, as it is today, we strongly believe that it should be easier and more convenient for people to volunteer their medical information for research. Mechanisms for seeking and managing consents must become easier: patients could consent to information-based research when checking in with their provider and the EHR could record choices and transmit them through HIEs. In addition, they could actively manage their research preferences through a dynamic consumer-interactive consent management system. The Department should ensure that these consent mechanisms are clear and meaningful to patients, while avoiding authorization requirements that add length, confusion and complexity. What's most important is that opportunities for patients to consent to information-based research should become easy, convenient, and common.

- **Revisiting the Impact of the HIPAA Privacy Rule on Research**

We recommend that HHS take this opportunity to undertake a fresh look at the role of the HIPAA Privacy Rule on research overall. As you are aware, the Institute of Medicine concluded in *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research*, that HIPAA "does not protect privacy as well as it should, and that, as currently implemented, the HIPAA Privacy Rule impedes important health research."[3] We think a new regulatory framework to advance research while protecting privacy more effectively is needed. We urge you to fundamentally revisit the application of HIPAA to research through a thoughtful stakeholder approach to ensure that we, as a society, are doing all we can to accelerate medical treatment breakthroughs and system improvements in quality and efficiency, while simultaneously ensuring private health information is securely protected. We think both goals can and should be pursued together.

Non-Research Provisions in the Proposed Rule

- **Individual Access to PHI**

Genetic Alliance very strongly supports the expansion of patient access rights under HITECH and as you have developed them more fully in the NPRM. Patients' inability to access their health information is an unacceptable burden today, which lands most heavily on those with chronic and complex diseases. Patients can no more take more responsibility for managing their care and improving their health without access to their health information, than they could take responsibility for managing their finances if they were denied access to their bank account records. Sadly, that denial of ready, convenient, and quick access to one's health information on a practical level is far more often the norm than the exception today. We support most of the detailed provisions in the NPRM to implement the newly expanded access.

However, we do have one salient concern with the proposed regulation regarding the newly expanded access rights. HITECH § 13506(e)(1) provides that patients have a right to choose to direct a Covered Entity to transmit a copy of their PHI directly to a person or entity they designate, "provided that any such choice is clear, conspicuous, and specific." The NPRM's proposed narrowing of this right by adding a new, nonstatutory requirement that the choice be in writing and signed constitutes a troubling and inappropriate restriction of the right Congress gave individuals. Provided, of course, that the Covered Entity has appropriately authenticated the patient's identity, the patient should be able to instruct the Covered Entity to transmit her records to a particular recipient in any oral or written fashion she chooses. In fact, imposing a writing requirement in this setting would be a significant step backward in terms of technology and patient engagement; a writing and signature requirement would perpetuate the inefficiencies, delays, and blocked access resulting from paper and fax authorization processes today. In eliminating the proposed requirement for writing and a signature for patient access requests, we urge you to follow the approach you laid out with respect to parents' requests to have providers send immunization records to schools in § 164.512(b). In that setting, you quite appropriately enhance flexibility and convenience by having providers honor oral requests to send immunization records to schools, provided, of course, that the parent's identity is established.

In contrast, we would like to see EHRs evolve to the point where interfaces with major Personal Health Records (PHRs) are routinely built in and offered to patients. At check-out from a provider's office or during the visit itself, patients should be able to make a simple request that their records be sent to their PHR or email address. They should also be able to do so conveniently in other settings such as in a phone call, again, presuming the patient's identity has been properly authenticated. Although the NRPM states that the writing and signature requirements could be fulfilled in an electronic context "to the extent that the signature is valid under existing law," no more than a miniscule number of providers would be aware of what electronic signature legal requirements apply, so in practice they would be quick to use only what they do understand - paper and faxes! We thus strongly urge you to delete the unnecessary and inappropriate writing and signature requirement in §

164.524(c)(3)(ii), for it would undercut patients' statutory rights to access to their electronic information in a convenient, easy, and fast manner under their own direction.

We also do not want patient access to be blocked by providers refusing to exercise available options regarding electronic delivery methods. Of course, using an encrypted, secure transmission method to a known, authenticated electronic destination tied to the patient is ideal, and EHR designers need to be making rapid progress in building in this capacity. But where such methods are unavailable or impractical, the patient must be able to specify that she wants her information promptly using less secure means, including e-mail. If the patient is cautioned that e-mail is not a secure means, but she nonetheless insists that she wants to receive it that way in the interests of time or convenience, then she should be allowed to exercise that choice. Even under the pre-HITECH access rights, we are aware of situations where overly restrictive Covered Entities have refused to send patients their own medical records via U.S. mail on request, paternalistically claiming that U.S. mail was "not secure enough." We urge HHS to forestall similar electronic access barriers by offering guidance on the type of secure transmission methods Covered Entities should establish for routine access requests, but also specifically require that Covered Entities must send records via e-mail when specifically requested to do so.

Regarding the issue the NPRM raises about possibly shortening the time it takes under the existing HIPAA rule for patients to get a copy of their records (30 days, with another 30 day extension possible), we appreciate the effort HHS is making. We strongly agree with other consumer advocates that 30-60 days to get records is unacceptably burdensome and undermines proper medical care, especially since the fastest way to get records from one provider to another is still, unfortunately, for the patient to obtain and hand-deliver them. We would be enthusiastic about the two or three business day deadline that is being recommended by some advocacy groups. However, we understand that technology is still evolving, and we hesitate to impose mandates on Covered Entities that may be unrealistic or too burdensome. We thus do not have a specific recommendation regarding the turnaround deadline, other than to encourage the Department to continue its efforts to accelerate access, including the three-day access turnaround deadline to achieve Meaningful Use metrics for HIT incentive payments.

- **Preemption and Access Rights**

HIPAA § 160.203 provides, *inter alia*, that HIPAA preempts state laws that are contrary to HIPAA, unless the state law is more stringent than the applicable HIPAA provision. One of the ways a state law can be defined as "contrary" is that the state law provision "stands as an obstacle to the accomplishment and execution of the full purposes and objectives" of HIPAA. Access rights are unquestionably a key component of federal rights under the original HIPAA statute and rule and now even more so under HITECH. We would therefore urge you to explicitly clarify that the new HIPAA/HITECH rules preempt any state law that serves to diminish, block, or limit patients' ability to access their records. Examples of state laws that do, in fact, impede access rights at a practical level include (a) any state laws that allow the charging of fees to patients that are greater than that allowed under federal law, and (b) any state laws that impose access authorization requirements that go beyond federal authorization

requirements, such as requiring extra steps or special paperwork for "sensitive" information like genetic information. To the extent that any such state requirements serve as practical impediments to patients' access rights granted by federal law, they are preempted by HIPAA on the grounds that they "stand as an obstacle to the accomplishment and execution of the full purposes and objectives" of HIPAA. While making the other proposed clarifications to §160.202, HHS could provide a significant service to the public by reducing confusion on this key point, so providers don't impose state-based paperwork hassles or high state-based fees as impediments to patients getting copies of their own information. Such clarity would also be extremely helpful to those trying to design PHRs and other online health tools to be streamlined, efficient, and consumer-friendly.

- **Restricting Information Based on Self-payment**

HITECH requires a Covered Entity to honor an individual's request to restrict disclosure of information to a health plan for either payment or health care operations purposes if the individual pays in full for the service. The NPRM expands this requirement by providing that the Covered Entity must permit the individual to choose which health care items or services a restriction applies to and the Covered Entity may not require the individual to restrict disclosures (and self-pay) on an all-or-nothing basis.

We are troubled that the NPRM makes changes that would have the effect of expanding the statutory provisions. Aside from the extraordinarily negative policy implications of this legislatively-required restriction (which essentially encourages individuals to selectively 'buy privacy' by not using their insurance), we are concerned that there will be significant operational difficulties in trying to ensure that information systems segregate and restrict data flows to payers. The complexities of meeting this requirement are substantial, including: Covered Entity compliance with payer contractual provisions (which often preclude charging individuals for otherwise covered services or that dictate specific rates for covered services); state law reporting requirements; quality control and fraud and abuse monitoring; design of clinical record systems, which do not allow for (and could not readily allow for) segmenting or flagging data based on whether they were acquired through insurance or self-pay; and the like. Furthermore, we do not believe it is possible to develop a system in which self-pay restrictions will flow to downstream providers accurately and consistently. Error and inconsistency will thus grow in unpredictable ways throughout health record systems.

We are particularly concerned that, to comply with this rule requiring hiding information from insurers where patients self-pay, <u>all</u> providers will have to shoulder serious expense, technological complexity, bureaucratic hassle, and legal risk –even if none or a tiny number of their patients ever asks to self-pay and suppress information. We do not think it is fair or reasonable to impose these costs and legal risks on providers. Similarly, because providers must seek to pass their costs on, we do not think it is fair for patients or taxpayers to have to pay for technological complexities and dual record sets resulting from the choices of a tiny number of people who want to suppress certain information from their insurers. As one practical example, does it make sense to make it easy for a person to keep their insurer paying

for other prescriptions while hiding from the insurer their multiple Oxycontin prescriptions, so that the abuse cannot be detected by payer abuse detection safeguards?

We are also troubled at the prospect of creation of two versions of clinical records, one comprehensive and accurate, and the other missing items a patient deliberately chose to suppress. This problem will exist at both for clinicians and at a large-scale level. To the extent that patients do exercise this option, quality, safety, and efficiency studies involving insurer databases (which are often the best and most comprehensive data sets in existence) will become less accurate over time because of data inaccuracies, thus undermining important goals of health reform.

Because the statutory self-pay-and-suppress provision is fraught with potential for unexpected harmful consequences, we strongly urge you to interpret it narrowly in general in order to mitigate the harm. And at a minimum, we think providers should be allowed to adhere to a reasonable requirement that patients pay in full for all care or for none, for imposing the technological and administrative costs of selectively redacting and purging records before submission to insurers is excessive and unfair, and having two sets of clinical records for individual patients (one accurate, one not) at the provider level seems medically dangerous.

We would also urge the Department, in concert with the Food and Drug Administration and federal and state drug enforcement authorities, to undertake a study of the likely effects of the self-pay suppression option in practice. We are concerned about the likelihood that among those most motivated to exercise the suppression option would be individuals involved in prescription drug abuse or insurance fraud.

- **Notice of Privacy Practices**

Given that Notices of Privacy Practices (NPPs) are already exceedingly long and complicated, Genetic Alliance discourages any new additions to the privacy notice requirements, as we believe NPPs do not effectively convey information to the vast majority of patients and, in fact, are rarely read. We believe that lengthening a complex document unnecessarily will only increase the likelihood that patients will not read or understand any options they may have. In particular, we do not see the "pro-privacy" value of mandating inclusion in the NPP of disclosures that also will require a specific authorization. This requirement would expand the notices for all patients or members, with attendant legal and administrative costs, even where only a tiny minority will ever be asked for an authorization. We encourage the Department to remove the obligations to insert these new provisions into NPPs**.**

- **Decedents' Records and Disclosure about Decedents to Family Members**

We strongly support both of the changes regarding decedents in the proposed rule – (a) excluding records about decedents from the scope of HIPAA at fifty years after the date of death, and (b) the efforts you are making to permit disclosure of information about decedents to family members and others who were involved in the patient's care prior to death. The first provision will remove research obstacles involving old records, and the second is an

appropriate and compassionate accommodation to the needs of families and loved ones who today can get cut off from information about their loved one once death occurs.

- **Business Associates and Subcontractors**

Genetic Alliance is pleased with the steps taken in HITECH and the NPRM to extend federal privacy protections to PHI outside of the traditional health care setting governed by the original HIPAA rule. We support the idea of extending mandatory safeguards to subcontractors of Business Associates. In our view, entities that receive, transmit, disclose or use PHI should indeed follow the Privacy Rule requirements for use and disclosure and should have robust security measures in place in order to keep such information confidential.

While we believe that the bar for Privacy and Security Rule compliance should be set high for Business Associates and subcontractors, we want to note two concerns about the operational challenges of extending the chain of trust related to use and disclosure of PHI. First, the obligation to "perform a periodic, technical and non-technical evaluation . . . that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart" as called for at § 164.308(a)(8) may prove significantly more burdensome for Business Associates and subcontractors than for Covered Entities. In contrast to Covered Entities, many Business Associates and subcontractors may use or disclose PHI in the context of only a very small portion of their business and the costs of a full-scale (and ideally third-party) Security Rule compliance assessment may constitute a significant financial burden. Second, while requiring Business Associates to include appropriate contractual restrictions and information protection provisions in 'downstream' contracts is entirely appropriate, it is not appropriate to require that these contracts be constructed according to the specific and particularized requirements for Business Associate Agreements. In some cases, the subcontractors may be holding or processing information already regulated by different regulatory schemes, such as Gramm-Leach-Bliley. Inserting new Business Associate Agreement requirements*per se* and particularized Security Rule documentation would add new layers of legal complexity and expense to an already complex compliance setting. We also wonder whether HHS has jurisdiction to impose obligations on entities outside the health care environment on the sole basis of the entity being a subcontractor to a Business Associate. We suggest that HHS might at least partially address these operational challenges by including new model Business Associate Agreement language in the Final Rule. A model template could reduce the legal fees associated with the vast expansion of required Covered Entity-to-Business Associate and Business Associate-to-subcontractor contracts, and it could require Business Associates and subcontractors to have in place adequate administrative, physical, and technical security mechanisms without necessarily requiring the periodic assessment of § 164.208(a)(8). Another consideration might be to exempt any subcontractor from HIPAA-specific obligations if they have already completed security assessments and met security requirements of other regulatory frameworks.

Again, we strongly support the evolving concept of keeping legal obligations persistent with data as it moves outside the realm of traditional health care entities, although we have some concerns about these particular subcontractor requirements in practice. We look forward to

further discussions with the Department and other stakeholders regarding broadening and strengthening protections for health data outside the original HIPAA scope.

Genetic Alliance wishes to thank the Department for issuing this Notice of Proposed Rulemaking and appreciates this opportunity to offer our comments and suggestions. We would be delighted to participate in further discussions if you have any questions or comments about this letter. We appreciate your efforts and we look forward to working with you.

Sincerely,

Sharon Terry
CEO
Genetic Alliance
4301 Connecticut Avenue NW, Suite 404
Washington, DC 20008-2369

[1] Nass S, Levit L, Gostin L, editors; Institute of Medicine, Committee on Health Research and the Privacy of Health Information. Beyond the HIPAA Privacy Rule: enhancing privacy, improving health through research. Washington (DC): National Academies Press; 2009.
[2] Tarini B.A., Goldenberg A., Singer D., Clark S.J., Butchart A., Davis M.M. Not Without My Permission: Parents' Willingness to Permit Use of Newborn Screening Samples for Research. Public Health Genomics 2010; 13:125-130.
[3] Nass S, Levit L, Gostin L, editors; Institute of Medicine, Committee on Health Research and the Privacy of Health Information. Beyond the HIPAA Privacy Rule: enhancing privacy, improving health through research. Washington (DC): National Academies Press; 2009.