NCHICA
North Carolina Healthcare Information and Communications Alliance, Inc.

September 13, 2010

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

Response to "Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule," hereinafter "NPRM" (RIN 0991-AB57).

Submitted via Federal eRulemaking Portal

Dear Secretary Sebelius:

The North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) is a nationally-recognized nonprofit consortium that serves as an open, effective, and neutral forum for health information technology (HIT) initiatives that improve health and care. NCHICA is comprised of nearly 200 member organizations, representing the many sectors of the healthcare industry including providers, payers, government agencies, clearinghouses, business associates (BAs), research organizations, health care vendors, and attorneys.

NCHICA's role in advancing healthcare technology through the protection of individuals' privacy and security of individual data has been well established. NCHICA was actively involved in analyzing and providing support to its members regarding compliance with the provisions of the HIPAA privacy regulation, which became effective in 2003. NCHICA's comments on this Notice of Proposed Rulemaking (NPRM) is the result of a collaborative effort from NCHICA's various and diverse member

organizations, which, through its activities, have developed considerable expertise in the various aspects of the HIPAA Privacy and Security regulations.

NCHICA'S COMMENTS ON THE NPRM

NCHICA believes that the Department of Health and Human Services (the Department) should be commended for the intent behind these proposed implementing regulations as required by the Health Information Technology for Economic and Clinical Health Act (HITECH Act). It is NCHICA's view that the proposed clarifications to the NPRM continue to provide the strong protections afforded protected health information (PHI) by HIPAA. Our suggestions for clarification to the NPRM follow in the order in which the topics are discussed in the NPRM.

As follows, in response to the Department's request for comment to the NPRM, NCHICA is providing comment on the following topics:

1. **Penalty and Enforcement:** The Department's proposal for mandatory investigations and compliance reviews, elimination of 45 CFR § 160.402(c)'s exception to Covered Entity (CE) liability for BAs, and other penalty and enforcement changes;

2. **BAs and Subcontractors:** The workability of the Department's treatment of BAs and subcontractors;

3. **Marketing and Fundraising:** The restrictions on marketing and fundraising activities;

4. **Decedents:** The treatment of decedents' PHI;

5. **Research:** The changes affecting research and compound authorizations;

6. **Sale of PHI:** The restriction on the sale of PHI;

7. **Immunization Records:** The release of immunization records to schools;

8. **NPPs:** The timing for redistributing revised Notices of Privacy Practices (NPPs), as well as what must be included in revised NPPs;

9. **Self-Payment:** The requirement that CEs restrict disclosure of items or services to health plans when paid in full by individuals; and

10. **Access to PHI:** The increased access to electronic PHI (ePHI).

NCHICA believes clarifying these areas will provide a better basis for CEs and BAs to comply with HIPAA while maximizing the protections afforded to PHI and minimizing unintended consequences that chill or restrict the necessary flow of electronic information.

PENALTY AND ENFORCEMENT

The Department has proposed regulations to make several critical changes to the penalty and enforcement provisions of HIPAA. NCHICA supports enforcement efforts that focus on correcting noncompliance through voluntary corrective action and supports the actions of CEs to consistently work toward compliance. Several of the proposals of the Department in the area of penalty and enforcement raise concerns for NCHICA, including:

1. The requirement of a formal investigation (as to complaints and compliance reviews);

2. The elimination of an exception for CE's liability for BAs when contractual obligations are in place and the CE has no knowledge of violations.

In reading the multiple changes to the Enforcement Rule, NCHICA comments generally that the Department's primary focus on enforcement should remain on cooperation and overall compliance, as opposed to punishment.

Requiring Formal Investigations and Compliance Review under 45 CFR § 160.306(c) and 45 CFR § 160.308

NCHICA is concerned about the costs and potential disruption created by the proposed requirement that the Department formally investigate any complaint filed under 45 CFR § 160.306 or conduct a compliance review under 45 CFR § 160.308 "when a preliminary review of the facts indicates a possible violation due to willful neglect." The NPRM does not clarify how much the Department would endeavor to undertake to confirm (or dispute) facts asserted in a complaint to assess whether a "possible violation due to willful neglect" has occurred. NCHICA supports appropriate investigations by the Department where it appears more likely than not on demonstrated and confirmed facts, a violation due to willful neglect has occurred. NCHICA recommends reverting to the prior regulatory language that used "may" versus "will" removing the mandatory obligation to investigate formally or to conduct a compliance review under 45 CFR § 160.306(c)(1) and 45 CFR § 160.308(a).

To limit the likelihood of unnecessary formal investigations, NCHICA would draw a distinction between "possible" and "probable" violations and would recommend that the Department revise § 160.306(c)(1) to read,

> "The Secretary will investigate any complaint filed under this section when a preliminary review of the facts indicates a probable violation due to willful neglect."

And § 160.308(a) would read,

> "The Secretary will conduct a compliance review to determine whether a CE or BA is complying with the applicable administrative simplification provisions when a preliminary review of the facts indicates a probable violation due to willful neglect."

Furthermore, requiring the Department to conduct a mandatory compliance review when a review of the facts indicates "possible" incidents of "willful neglect" even if no complaint has been received places a heavy burden on the Department and CEs alike.

The creation of a mandatory compliance reviews and formal investigation in the proposed rules has real life significance. Not only could this result in numerous time-consuming and expensive formal investigations (affecting the Department, CEs, and BAs identified in the complaint), these provisions are overbroad and potentially fail to identify spurious or even vindictive complaints or unreliable "facts" giving rise to significant intrusion through a compliance review or a formal investigation. Undeniably, some complaints are based upon misunderstandings or fail to include an accurate and complete set of facts. Requiring a formal investigation or a compliance review — rather than initiating the investigation with a more informal approach by confirming or disputing alleged facts through, for example, questionnaires or requests for information — would be costly, inefficient, and disruptive to the operations and activities of CEs to undergo formal investigation on unsubstantiated complaints and full compliance reviews.

Elimination of § 160.402(c)'s Exception for a CE's Liability from BA Acts

NCHICA supports the Department's development of rules that strengthen privacy rights of individuals by rendering BAs directly liable for HIPAA violations. NCHICA is concerned, however, about the Department's proposal to eliminate the exception under 45 CFR § 160.402(c) that previously allowed CEs, who had exercised reasonable care, to avoid liability for the actions of BAs if the following were true:

- The relevant contract requirements had been met, and
- The CE did not know of a pattern or practice of the BA that violated the contract, and
- The CE did not fail to act with regard to those patterns or practices.

Removing this exception exposes CEs to unpreventable liability and potentially chills business relationships. The elimination of this exception is not necessary to further the goal of health information privacy and security. NCHICA respectfully requests that the Department reconsider its proposal to eliminate this exception.

Revisions to Enforcement Rule

NCHICA is appreciative of the Department's efforts to clarify a number of the previous revisions to the Enforcement Rule. Because the penalties are so substantial

for violating HIPAA, NCHICA believes these rules must be as clear as possible for CEs and BAs to comply with their requirements and effectively safeguard the privacy and security of health information. NCHICA believes that examples of how the Department will interpret the various tiers of liability and factors considered in assessing penalties—as in part have been provided in the NPRM, but more guidance would ensure compliance resources were appropriately allocated by CEs and BAs—are vital to understanding the Department's enforcement policy and perspective. As such, NCHICA respectfully requests further guidance either in the preamble to these rules when finalized or in a separate guidance.

BUSINESS ASSOCIATES AND SUBCONTRACTORS UNDER REVISED 45 CFR §§ 164.104, 164.504(e), AND 164.504

Application of Security Provisions to Business Associates (BAs)

The HITECH Act applies the security provisions, specifically 45 CFR §§ 164.308, 164.310, 164.312, and 164.316, to BAs. This change marks a significant expansion in responsibility and direction. The rationale behind this action is supported by data that suggest 42% of all data breach cases were causes by "third party mistakes" [Ponemon Institute: http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf]. The emphasis on the HIPAA Security Rule enforcement has driven positive behavior within the CE community, resulting in better controls. The result is that unauthorized individuals and professional hackers are turning to softer targets to steal sensitive data.

Prior to the signing of the HITECH Act, BAs had fewer incentives to implement a robust security management program. CEs were relying on contractual language to outline the security requirements. There were pressures on both sides to reduce the amount of contractual specificity so as to limit a CE's liability for directing a BA's specific actions. At the same time, CEs would expect the BAs to protect the sensitive information.

NCHICA supports the requirements in the HITECH Act to extend the Security Rule requirement to BAs. NCHICA requests additional guidance from the Secretary on how to address likely operational issues arising from this extension. As a result, NCHICA wishes to comment on the following five (5) issues relating to the application of security provisions to BAs:

1. Operational challenges promulgating contractual requirements to the multi-tier subcontractors within the proposed 180-day compliance deadline;

2. Operational challenges of CEs for monitoring compliance below the first tier BAs;

3. Timeline limitations for CEs to meet the 60-day breach reporting mandates when breaches are discovered by the multi-tier subcontract;

4. Operational challenges faced by BAs and subcontractors that support multiple CEs; and

5. Contractual challenges between small CEs and large BAs, e.g., Cloud vendors.

Operational Challenges Promulgating Contractual Requirements to the Multi-Tier Subcontractors Who Do Not Have an Existing HIPAA-Compliant Contract within the Proposed 180-Day Compliance Deadline.

The NPRM requires CEs, BAs, and all subcontractors who have access to ePHI on behalf of the covered entity to execute as appropriate HIPAA-compliant contracts within 180 days of the Final Rule unless a pre-existing HIPAA-compliant contract exists between the parties. When a HIPAA-compliant contract exists, the NPRM outlines exceptions up to one year plus 240 days from the date of publication of the Final Rule in the Federal Register. For subcontractors of BAs, NCHICA recognizes that this has inherent operational challenges in multi-tiered execution of unique contractual obligations. Since HITECH and now the NPRM for the first time extends the HIPAA requirements through the first tier of BAs downstream to supporting subcontractors, this group of supporting subcontractors are not as likely to have a HIPAA-compliant contract with their respective BAs. Each subsequent tier of supporting vendors would in turn have to follow the same requirements and ensure their downstream subcontractors are also HIPAA-compliant. NCHICA has concerns that many BAs may wait until they have contractual language from their covered entities to start the flow-down of HIPAA requirements. Since this may take up to, and even beyond the 180 day compliance period, NCHICA Is concerned that the downstream subcontractors may not be contractually obligated to comply with HIPAA by the deadline. Adding to the challenge is this group of supporting players will need education and training on HIPAA and its requirements, which may never have occurred before. In light of these challenges, NCHICA requests that the Department revise the proposed rules to allow for additional time to execute BAAs or similar required agreements through the multiple tiers of subcontractors.

Under the NPRM, the covered entity is ultimately responsible for the actions of non-compliant BAs. The tracking of downstream subcontractors could lead to each covered entity tracking thousands of subcontractor compliance activities and programs – something that is unduly burdensome and operationally unmanageable. Therefore, NCHICA also recommends that the Final Rule allow provisions for the BA to provide the CE with assurances that their respective second tiers of supporting vendors have been contractually bound in accordance with the services provided by the BA to the CE. NCHICA recommends that each subsequent tier of subcontractor be responsible for providing adequate assurances upstream.

Operational Challenges of CEs for Monitoring Compliance Below the First-Tier BAs

NCHICA recommends that the Department implement provisions under the Final Rule to recognize a first-tier BA's compliance with HIPAA requirements as to supporting vendors by the BA providing assurances to the CE that the HIPAA requirements are being followed by the BA and its subcontractors. To require that a CE monitor HIPAA compliance below the first-tier BAs creates numerous challenges for a CE. First, a CE may not be aware of all subcontractors used by a BA (or subsequent downstream BAs) and need not on a day-to-day basis be aware of these supporting vendors. Second, a BA may rely upon a myriad of subcontractors, including remote subcontractors, causing a CE required to monitor the activities of the subcontractor quite an administrative burden. Third, the working relationship with a subcontractor is between the BA and the subcontractor and not the CE and the subcontractor. Forcing the CE to interject itself into this working relationship has the unintended consequence of stifling business, exposing the CE to unnecessary liability, and potentially undermining the control or perception of the BA to its subcontractors. By relying on an assurance of compliance and creating liability on the BA to monitor its business partners, a CE can be assured that services will be provided in an environment that understands and safeguards privacy and security of PHI.

Operational Challenges Faced by BAs and Subcontractors that Support Multiple CEs.

Many CEs subcontract work to a few primary BAs. For example, the primary HIT vendors may have hundreds or thousands of customers. This results in BAs who have numerous unrelated CE clients being potentially subject to conflicting or, at a minimum, different BAA requirements. Being subject to differing requirements causes BAs to incur additional administrative and operational overhead to comply with these agreements and worse yet, risks non-compliance through confusion.

NCHICA recommends that the Department consider allowing a certification process for BAs and subcontractors to provide CEs with a "stamp of approval" that BAs and subcontractors have achieved HIPAA compliance. This process could be similar to the process in the financial sector, Banking Industry Technology Secretariat (BITS), or "shared assessments" process, that permits a third party's externally conducted assessment to be shared and accepted across dissimilar organizations.

Contractual Challenges between Small CEs and Large BAs, e.g., Cloud Vendors

NCHICA is concerned that the NPRM does not address compliance challenges inherent in the trend toward "Cloud Computing." Some CEs are moving ePHI into the Cloud, either through the use of Software as a Service (SaaS) vendors, Infrastructure as a Service (IaaS), or Platform as a Service (PaaS). It has been suggested that within the next decade, there will be less than a few dozen true SaaS vendor platforms, each with a national and/or international architecture. CEs desiring to take advantage of the

economies of scale offered by the Cloud are at a disadvantage in negotiating an enforceable BAA. Under the NPRM, individual CEs who use Cloud Vendors would be exposed to liability on the basis of the actions of the Cloud Vendor. This situation further supports NCHICA's request that the Department reconsider its proposal to eliminate section 160.402(c) exception for CE's liability from BA's acts, as discussed earlier.

MARKETING AND FUNDRAISING UNDER REVISED 45 CFR §§ 164.501 AND 164.514(f)

The Department's proposed changes to the marketing provisions clarify the definition of marketing; however, the changes will increase costs to the CE. The marketing definition was expanded to treatment communications in which the CE receives financial remuneration from a third party in exchange for making such communication. The NPRM permits subsidized treatment to be excluded from the marketing requirements of obtaining the individual's prior authorization if the CE notifies the individual of such communications in its NPPs and permits the individual from opting out of receiving such communications in the future. These requirements would increase the CE's costs without any true benefit to the individuals.

NCHICA recommends that the Department interpret "indirect" financial remuneration narrowly to avoid unnecessary costs and hampering open communication. Currently, CEs use third party communications, e.g., brochures, videos or posters, to provide informational materials to individuals. For example, CEs distribute informational/educational brochures or videos regarding services, such as post-acute facilities, alternative treatment or procedures concerning implants of devices. These materials clearly identify the sponsoring third party. These materials are produced and paid by the third party and distributed to the CE free of charge. These communications provide valuable information to the individuals and assist the individual in making choices of potential alternatives. Such materials — that conspicuously identify the sponsoring third party and are distributed without compensation to the CE — should not be included within the definition of indirect financial remuneration. Such activities should be considered non-subsidized communications as the financial remuneration is limited to in-kind costs related to the distribution of the materials and no additional payment is made to the CE.

NCHICA supports unrestricted communications to individuals regarding treatment. Third-party remuneration should not convert such a communication into "marketing" under the proposed rules. These third-party communications are a valuable tool of CEs to ensure individuals receive additional information about treatment without cost to the CE. The Department's proposal is likely to decrease such communications, since CEs, mindful of costs, are not likely to attempt to implement the opt-out provisions for such communications. The purpose of the communication is to provide information to individuals to allow the individual to make an educated choice about the individual's health care. A CE may continue to send non-subsidized materials related to services or products to an individual who has chosen not to receive subsidized material. NCHICA is concerned that the proposed rules have the unintended consequence of confusing

individuals about the difference between subsidized and non-subsidized communications.

It will be difficult for the CE to permit individuals to choose to opt out prior to receipt of any communications. First, a general statement within the NPP cannot clearly describe the types of subsidized communications; thus, an individual would not be able to make a reasonable decision. Second, the CE would need to track the individuals' choice without context of a specific communication.

If the individual has the right to opt out prior to any communication, the CE would need to remove the individual from all future communications since the individual would not be able to identify any specific communications since the individual has not received a communication. This would also create confusion for the individual. It would be more appropriate to limit the opt out to the specific communication; however, this option may be difficult to implement for all CEs in a compliant manner. The CE should have the discretion to determine if the entity removes the individual from all future subsidized communications or a specific communication.

NCHICA supports permitting a CE to conduct more targeted fundraising campaigns based upon general health care services. Permission of use of department or service information, pediatric vs. adult, or general service lines – hospice or obstetrics, would benefit to reach a grateful individual and not expose diagnostic information. Individuals would likely be more open to receiving fundraising solicitations regarding a service that they have experienced, rather than various general solicitations. NCHICA recommends that the Final Rule include an exclusion from disclosure for certain sensitive services, such as psychiatric services or substance abuse.

Currently, the NPP requires the notice of a CE's fundraising activity. The addition of the right to opt out within the NPP will create confusion to the individual. The placement of the opt out communication on a specific fundraising solicitation enables the individual to make a clear decision to refuse future solicitations. Creating the option for an individual to opt out of fundraising prior to the individual receiving the first mailing also places a large burden on the CE without substantial benefit to the individual. Disclosure of PHI is limited. Receipt of a fundraising solicitation does not disclose PHI to other parties. Receipt of such solicitations is commonplace.

To permit the individual to make direct choices, the individual's opt out should be limited to the current campaign where communication has occurred. The CE should have the discretion to determine if the entity removes the individual from future solicitation. The process to identify the individuals that have opted out and the specific associated solicitations may not be possible for all CEs. From an implementation perspective, an all or nothing approach may be easier, but loss of potential donors should increase. A CE should make the decision of implementation as to restricting to current campaign or all future campaigns. The ability to opt in to future solicitations should be the choice of the CE and not the individual, since the CE must implement such choices.

NCHICA supports clear and conspicuous opt out instructions on each piece of communication. CEs will continue to use due diligence through implementation of procedures and providing staff training to implement the individual's choice. However, the Department's proposal to create strict liability so that a single mistake causes the CE to be subject to the tiered enforcement is unnecessary.

TREATMENT OF DECEDENTS UNDER REVISED 45 CFR § 160.103 AND 45 CFR § 164.502(f)

The NPRM states that CEs must protect the PHI of individuals for 50 years after death and modifies the definition of "individually identifiable health information" to clarify that information regarding persons who have been deceased for more than 50 years is not PHI. NCHICA suggests that 50 years is excessive and unreasonable, from the perspective of both compliance and legal departments. For instance, NCHICA recognizes a weakness in this approach as it applies to past information in circulation prior to HIPAA's enactment. Much of this past information may already be shared or otherwise in the hands of non-CEs and non-BAs ranging from libraries and museums to schools and universities, who are not bound by the provisions of HIPAA, leaving this information neither private nor secure. For enforcement purposes, it may be difficult to determine from where information came and it would be unfair to penalize CEs and BAs for these problematic cases without clear indication that the CEs or BA was at fault.

Furthermore, most Statutes of Limitation with respect to health care run for three to four years. Having the Proposed Rule set a different timeframe provides significant confusion and complications for CEs. Accordingly, NCHICA suggests decedents' information be protected for four years following death.

RESEARCH UNDER REVISED 45 CFR § 164.508

Compound Research Authorizations

The NPRM includes a provision that would permit compound authorizations; that is, an authorization permitting a CE to use protected health information for more than one purpose, if both (or all) purposes relate to the same research project. Accordingly, a single authorization could be used for a clinical study, as well as for specimen collection for a central repository. Currently, compound authorizations are prohibited, which increases the burden on clinical trial sites when obtaining consent and authorization from subjects for the research project. Moreover, the Department has also requested comment on whether (and how) an authorization could be used to permit ***future*** unspecified research studies using the subject's PHI.

These changes to the Privacy Rule would greatly simplify the ability of sponsors and institutions to use collected information, data, and tissue in future studies. More importantly, this would reduce the need for sponsors and institutions to require individuals to review and sign multiple documents or for them to contact individuals, perhaps multiple times, about future use of their PHI. The individual can provide

consent and authorization, or not, in the first instance. Contacting individuals again and again seems disproportionate to the risk and a greater invasion of privacy.

The Proposed Rule provides a list of possible approaches to designing such compound forms, but requests comments on "additional methods that would clearly differentiate to the individual the conditioned and unconditioned research activities on the compound authorization." In fact, prior to the Privacy Rule, it was common for a research study's informed consent form to include check-boxes asking the potential subject to indicate whether the individual agreed to participate in certain optional study related activities. It was a much more convenient process both to the sponsor / institution and to the individuals. Individuals could elect in the first instance to participate in the main study, to participate in the separate related study activities, or for future unspecified studies. A reversion to this former, but very workable, process would be a simple solution.

SALE OF PHI UNDER REVISED 45 CFR § 164.508

As a preliminary matter, neither the HITECH Act nor the NPRM define the "sale of PHI." NCHICA suggests that the Final Rule include a definition of "sale of PHI." However, in drafting this definition, NCHICA strongly urges that the Department exclude from the definition of "sale of PHI" circumstances in which direct or indirect remuneration is provided to a CE in exchange for PHI where the CE is providing such information under an access agreement, license, or lease that limits uses and disclosures in accordance with 45 CFR §164.508.

The HITECH Act prohibits a CE from receiving remuneration in exchange for the disclosure of PHI unless the CE has obtained an authorization or an exception applies. One exception in the HITECH Act is for disclosure for research purposes permitted by the Privacy Rule, but only if the price charged for the information reflects the costs of preparation and transmittal of the data. The HITECH Act also instructed the Office of Civil Rights (OCR) to consider the impact of this cost-based payment condition on the exception for research when developing implementing regulations. The NPRM would revise the language of the research exception specifically to clarify that the cost-based payment condition applies to the exchange of a limited data set for remuneration for research purposes.

NCHICA applauds the Department for including specific references in the NPRM indicating that the use of limited data sets does not need "consent" from individuals – as a result, limited data sets can flow freely for "public health" purposes, including FDA-regulated activities. However, NCHICA is still concerned about the use of limited data sets for *research* purposes. The current provision would limit the exchange of compensation for such data, and thereby have a chilling effect on the ability to create large data sets important for a variety of research that could help save individuals' lives.

The NPRM also requests public comment on the types of costs that should be permitted under this provision. NCHICA notes that a CE has little, if any, incentive to expend time, money, and other resources on the preparation and transmittal of PHI or limited data sets without adequate remuneration. Accordingly, to avoid what would

otherwise have a chilling effect on the development of large databases so beneficial for research of many kinds, it is imperative that the final rule allow for a comprehensive cost-based payment assessment. The factors driving reasonable cost by the data sources for the preparation and transmittal of PHI for research purposes would include the following:

- Data source:
    - Contracting
        - Negotiating
        - Travel
    - Legal
    - System setup cost
        - Data transfer capabilities (WAN, encryption, connectivity)
        - Hardware and software licenses
        - Data translation and migration preparation
    - Data translation and preparation
        - Volume
        - Data complexity (including data collection, format translation and aggregation)
        - Frequency
- Transmission:
    - Direct connect (includes WAN, encryption, IT management)
    - Media
- Overhead:
    - IT and Facilities investment
    - Accounting of disclosures
    - Security and audit (internal and external)
    - Contracting and invoicing
    - Tax reconciliation
    - Legal
        - Risk mitigation, e.g., insurance, Business Continuity Plan/Disaster Recovery, etc.
        - Risk management, e.g., breach investigation and notification
    - Staff salaries and benefits
- Archival

NCHICA encourages the Department to factor in all costs related to aggregating and transmitting ePHI.

IMMUNIZATION RECORDS UNDER REVISED 45 CFR § 164.512(b)

The Department proposes to revise 45 CFR § 164.512(b)(1)(vi) to permit CEs to release immunization records to schools upon the oral request of a parent (or guardian) when state laws require proof of immunization for enrollment. NCHICA commends the Department for recognizing the importance of the prompt disclosure of immunization records to schools by CEs when enrollment is conditioned on this information. The proposed rules require an agreement between the CE and the parent seeking disclosure of the immunization records, which can now be oral instead of written, but still must be an "agreement." While the Department does not require that the CE document this agreement, as a practical matter, CEs are likely to continue to require an executed authorization to avoid concerns about miscommunication or withdrawal of consent. The burden of authorization remains; CEs likely will require authorization to eliminate potential liability concerns.

NCHICA recommends that the Department consider creating a new section – 45 CFR § 164.512(b)(1)(vi)(D) – to provide clear immunity for CEs who release immunization records in reasonable reliance upon reaching an oral agreement with a parent or guardian. Such a provision could read,

> "(D) The CE who obtains an agreement from an individual permitted under subsection (C) herein to the disclosure limited to proof of immunization shall be entitled to reasonably rely on such agreement and be immune from liability, penalty, or other enforcement action for such disclosure under these rules."

NCHICA believes that adding such a provision will provide the necessary comfort for CEs to achieve the Department's goal in relaxing the requirements as to the disclosure of immunization records to schools in states having laws conditioning enrollment on proof of immunization.

CHANGES TO NOTICE OF PRIVACY PRACTICES UNDER REVISED 45 CFR § 164.520

The NPRM obligates CEs to amend their NPP to conform to changes in individual rights and other provisions required by the HITECH Act, as well as requiring CEs to redistribute the newly revised NPP to individuals.

As discussed in these comments, the proposed rules require corresponding changes to NPPs for the following:

1. Uses and disclosures requiring an authorization still must be described in the notice, which will include authorizations to use or disclose PHI for marketing, to sell PHI, and to uses and disclosures of psychotherapy notes (*see* "*Marketing and Fundraising*" and "*Sale of PHI*");
2. Uses and disclosures of PHI for fundraising still must be described in the notice, but in addition the individual's right to opt out of such uses and disclosures must be described (*see* "*Marketing and Fundraising*");

3. If the CE intends to send treatment communications in exchange for financial remuneration, that fact and the individual's right to opt out of such communications must be described (*see* "*Use of PHI for Treatment Communications*"); and

4. A description of the individual's right to request restrictions of PHI made to health plans for payment or health care operations regarding services for which the individual has paid in full out of pocket (*see* "*Restriction of Disclosures to Payors for Items/Services Paid in Full by Individuals*").

The Department requires that the first three categories listed above be described in new and separate statements within the NPP. In addition, the Department solicits comments regarding whether breach notification requirements should be included in the NPP.

In the NPRM, the Department also states that the above-described changes to NPPs will constitute material changes to those notices, triggering the Privacy Rule's requirement to redistribute the revised notices. Section 164.520(c) of the Privacy Rule treats health plan CEs and non-health-plan CEs differently in terms of what is required for redistribution, prompt redistribution for non-health plans and redistribution within 60 days for health plans. While the Department comments in the NPRM that the obligation to redistribute the NPP is not "overly burdensome for providers," the Department solicits comments on this issue. The Department, however, notes that the redistribution requirements imposed on health plans may be overly burdensome and solicits comment on revising the redistribution requirements applicable to health plans.

NCHICA supports the need for clear communication regarding individual rights in health privacy and security. NCHICA commends the Department for advancing a number of options to address the redistribution of NPPs. NCHICA supports clarification by the Department that redistribution, both by health plans and non-health-plan CEs, be not overly burdensome and revise regulatory text to permit variation in the method and means of redistribution by all CEs, removing any explicit limitation such as the 60-day period currently applicable to health plans under 45 CFR § 520(c)(1)(i)(C). The costs and time associated with revising and redistributing the NPP of a CE in either paper or poster form can be significant regardless of whether the CE is a health plan or a provider, although admittedly the scale may differ. Not only does this process require staff time and effort in both creation and distribution of the NPP, it also frequently leads to additional costs, such as legal review, publication, and formatting, as well as other professional services. NCHICA also recognizes that CEs are business enterprises and the cost of revising NPPs multiple times, for example to add provisions later relating to breach notification after the compliance date for the finalized version of these rules, is wasteful and expensive.

NCHICA respectfully requests that the Department consider delaying any required revision to NPPs until the Department has determined all the provisions that need to be added as a result of the HITECH Act. Upon such determination, NCHICA encourages the Department to adopt a flexible approach to redistribution by replacing the 60-day notice period with clarifying regulatory text along the lines of "Within a

reasonable timeframe of a material revision to the notice. . . " in 45 CFR § 164.520(c)(1)(i)(C).

RESTRICTION OF DISCLOSURE TO PAYORS OF ITEMS/SERVICES PAID IN FULL BY INDIVIDUALS UNDER REVISED 45 CFR § 164.522(a)

The restriction of disclosure to payers for items/services that are paid in full by individuals places a significant burden on CEs to put in place systems to maintain compliance.

In response to the Department's request for comments on the types of treatment interactions that make implementing a restriction burdensome, NCHICA finds it nearly impossible to separate records within an encounter for billing documentation purposes, while keeping the encounter records together for clinical care purposes. A clinical visit dictates the need for a report of that encounter. That report has multiple uses, including clinical care, individual safety, and billing documentation, among others. To separate the record in substantiating individual billing, while retaining it for clinical care and safety, is untenable. To separate the encounter into the part submitted to the payer and the part paid by the individual raises the cost to both the CE and the individual (the CE has the overhead of multiple visits and the individual would need to pay for a second encounter). For example, individuals who obtain medications through self-pay may experience higher rates of adverse drug events (ADEs) because automated systems to detect ADEs will be bypassed. This also raises liability concerns for the CE. NCHICA recommends the Department provide relief from liability arising from these compromised records.

The Department requested comment on the obligation of a CE that knows of a restriction to inform other CEs downstream of such restriction. As clinical care is more and more a multiple provider activity, the ability to communicate the restriction across an array of providers, likely in multiple CEs, is fraught with difficulties. One CE may not even know who the downstream providers are. This will become exacerbated as the HITECH anticipated Health Information Exchanges (HIEs) will allow seamless communications among providers about an individual. NCHICA suggests that the individual, not the CE, have the responsibility to inform his other providers of the restriction.

The Department also requested comment on the extent to which a CE must make "reasonable efforts" to secure payment from the individual prior to submitting PHI to the health plan for payment. Section 13405(a)(2) of the HITECH Act clearly provides that the obligation of a CE to withhold the disclosure of PHI to a health plan upon the request of an individual only arises where the health care provider involved "*has been paid* out of pocket in full." Based on the language of this provision, if the CE has not actually received payment in full at the time the request for the restriction is made, the CE has no obligation to withhold the disclosure to the health plan. A mere promise to pay is not sufficient to obligate the CE to observe the restriction, and it would be unreasonable to require the CE to delay and possibly lose reimbursement from a health

plan as a result of delay by an individual to make payment in full at the time of the request. It is difficult to believe that Congress would have intended such a result. Therefore, NCHICA asks that the Department make clear that a CE is under no obligation to resolve any payment issue with the individual prior to sending the PHI to the health plan, and that payment must be made to the CE in full at the time the individual makes the request in order for the CE to be obligated to comply with the request.

NCHICA further supports that the CE may submit for payment for follow-up treatment without restriction if the individual does not wish to pay for the follow-up treatment. This situation, however, is likely to lead to confrontation with the individual who may not recognize the connections between the initial and follow-up treatments.

ACCESS TO ELECTRONIC PROTECTED HEALTH INFORMATION UNDER REVISED 45 CFR § 164.524(c)(2)

The HITECH Act seems to interpret the cost of labor to produce electronic copy is negligible. However, the cost to build the infrastructure to provide the data is substantial and will need to come from some place. Permissible expenses could be defined as listed above in the section regarding the sale of PHI.

NCHICA agrees that the provision of the ePHI should be without reasonable delay and not later than 30 days. CEs will still require the additional 30 days for off-site storage (typically paper).

In 45 CFR § 524(c)(ii), the proposed language states " or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual." However, there is no indication of how to address providing the information if the two parties cannot reach agreement. For instance, a large number of medical images are stored in a format called DICOM, which may not be readily translated to YouTube (an extreme example, but one that will probably appear at some point). NCHICA recommends that the Department specify that the time to provide the ePHI begins when agreement is reached.

SUMMARY

NCHICA appreciates that the Department issued this NPRM to implement protections of the HITECH Act. While NCHICA agrees that provisions of the Privacy and Security Rules must be revised to achieve the goals of the HITECH Act, NCHICA urges the Department to revise these rules when finalizing them to avoid unintended consequences of confusing communication to individuals, overburdening CEs and their BAs and chilling research with large databases, beyond the requirements of law.

The member organizations of NCHICA include CEs and BAs, research entities, and aggregators of health data, as well as other entities that support them every day. NCHICA is concerned that many of the proposed rules may have unintended and unanticipated consequences that may negatively affect health care treatment,

operations, payment, as well as research and other necessary activities by CEs and their BAs. NCHICA believes it is imperative that the Department revise these proposed rules before issuing final regulations.

Respectfully submitted,

W. Holt Anderson /s/
Executive Director