

**TESTIMONY BEFORE THE INTERIM HEALTH SERVICES  
COMMITTEE  
April 12, 2012**

Good afternoon Chairman Lee and Members of the Interim Health Services Committee. I Am Sheldon Wolf, the Health Information Technology Director. I am pleased to present testimony on whether any laws or regulations prohibit a health information exchange from selling individually identifiable health information. The short answer to your inquiry is: Yes, there are federal laws and regulations that generally prohibit a health information exchange ["HIE"], such as the North Dakota Health Information Network, from selling any individually identifiable health information the exchange stores or transmits.

We asked Mike Mullen who is a Special Assistant Attorney General to ITD and the Health Information Technology Advisory Committee to identify any laws and regulations that prohibit the sale of health information. His letter outlining those laws and regulations is attached to this testimony. I will now explain how these laws and regulations prohibit the North Dakota Health Information Network and its Participants and contractors from selling any individually identifiable health information.

Under the HIPAA Privacy Rule, a federal regulation issued under the Health Insurance Portability and Accountability Act of 1996, a covered entity may not use or disclose protected health information, “except as permitted or required by [the Privacy Rule].” So the general rule is: if the disclosure of individually identifiable health information is not permitted under the HIPAA Privacy Rule—the disclosure is prohibited.

Under the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”), which was part of the American Recovery and Reinvestment Act of 2009, the HIPAA Privacy Rule applies not only to hospitals, clinics, and other covered entities, but also to individuals and organizations that provide services “for or on behalf of” a covered entity that involve the use or disclosure of individually identifiable health information. An organization providing these services is designated as a “business associate” of the covered entity. The HITECH Act explicitly specifies that a Health Information Exchange Organization such as the North Dakota Health Information Network must be treated as a Business Associate of the health care providers and health plans for whom the Network transmits health information.

Each Participant in the North Dakota Health Information Network (“NDHIN”) has signed a business associate agreement designating NDHIN as its business associate and granting NDHIN the authority to facilitate the exchange of individually identifiable health information between Participants of the Network. However, the Agreement also requires the NDHIN to comply with all applicable provisions of the HIPAA Privacy and Security Rules—as well as other policies and contractual requirements.

Under the HITECH Act and the HIPAA Privacy Rule, a business associate such as the NDHIN may disclose protected health information to a business associate that is a “*subcontractor*.” But the business associate must “ensure that any subcontractors that create or receive protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information.”

We have engaged a technology company, Axolotl, (which is now OptumInsight), as a “subcontractor” of the North Dakota Health Information Network to provide technological services that will assist North Dakota health care providers and health plans in the efficient and secure exchange of health information. We have a business associate agreement with Axolotl under which Axolotl has agreed to

comply with all of the requirements for a business associate under the HIPAA Privacy and Security Rules including those requirements that prohibit both a covered entity and a business associate from disclosing health information for remuneration to any third party.

The HITECH Act generally prohibits the sale of individually identifiable health information so that neither a covered entity nor a business associate may “directly or indirectly receive remuneration in exchange for [disclosing] any protected health information of an individual” unless the covered entity obtains the individual’s authorization.

I will note that the HITECH Act contains a few exceptions that permit payment to a covered entity or business associate for the disclosure of health information. For example, the prohibition against remuneration does not apply to the disclosure of protected health information for public health purposes. The prohibition also does not apply to a disclosure by a business associate for activities that the business associate undertakes on behalf of a covered entity “[if] the only remuneration provided is by the covered entity to the business associate for the performance of such activities.” The justification for these exceptions is that it is not unreasonable to compensate a business associate for the work it must undertake to comply with

disclosures that are required by law or by the business associates' contract with the covered entity for whom it is providing technology services. But again, in general, the sale of health information to unaffiliated third parties is prohibited—and any such disclosure would be a violation of the HIPAA Privacy Rule subjecting the business associate or subcontractor to all applicable civil and criminal penalties.

Finally, it should be noted that one of the NDHIN policies that each hospital, clinic, pharmacy, health plan, etc., that participates in the Network must comply with explicitly prohibits the sale of health information without the authorization of the individual to whom the information pertains. (See Exhibit A, NDHIN Policy 11, Uses and Disclosures of Health Information, page 2.)

Chairman Lee, this completes my prepared testimony. I will be pleased to answer any questions the Committee may have regarding the prohibition on the sale of health information or any aspects of the North Dakota Health Information Network.

Phone 701.226.8334  
[mikemullen.nd61@gmail.com](mailto:mikemullen.nd61@gmail.com)

**Michael J. Mullen**  
**Attorney-at-Law**  
**P.O. Box 384**  
**Waterville Valley, NH 03215**

April 6, 2012

Sheldon Wolf, Health Information Technology Director  
ITD  
State Capitol  
600 E. Blvd. Ave., Dept. 112  
Bismarck, ND 58505-100

Re: Prohibition on the Sale of Protected Health Information

Dear Sheldon:

Thank you for asking whether there are any laws or regulations that prohibit a health information exchange from selling individually identifiable health health information (also frequently referred to as "protected health information"). There are several federal laws and regulations that generally prohibit a health information exchange ["HIE"], such as the North Dakota Health Information Network, from selling any individually identifiable health information the exchange "stores" or "transmits."

The basic federal law restricting the use and disclosure of health information is the Health Insurance Portability and Accountability Act of 1996—known as "HIPAA." Pub. L. No. 104–191. The Health Insurance Portability and Accountability Act authorized the federal Department of Health and Human Services to issue regulations regarding the privacy and security of health information.

Under the HIPAA Privacy Rule, "[a] covered entity may not use or disclose protected health information, except as permitted or required by [the Privacy Rule]." 45 C.F.R. § 164.502(a). So the general rule is: if the disclosure of individually identifiable health information is not permitted under the HIPAA Privacy Rule—the disclosure is prohibited.

"Covered entities" include health care providers such as hospitals, clinics, pharmacies, etc., that transmit health information in an electronic form, and government and private health plans such as Medicare and Medicaid, and Blue Cross Blue Shield, Aetna, and CIGNA, respectively. See 45 C.F.R. § 160.103 (definition of a covered entity). Thus,

Sheldon Wolf

April 6, 2012

Page 2

each health care provider and health plan that will exchange electronic health records through the North Dakota Health Information Network is a covered entity.

A covered entity is permitted to disclose individually identifiable health information for treatment or payment for health care services, and also for specified public purposes such as a disclosure to a public health authority as authorized by public health laws, or a disclosure required under a court order. See 45 C.F.R. §§ 164.502 and 164.512. Any disclosure not permitted by the HIPAA Privacy Rule requires the written authorization of the individual to whom the health information pertains. 45 C.F.R. § 164.508.

The Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), which was part of the American Recovery and Reinvestment Act of 2009 ("ARRA"), Pub. L. No. 111-5, significantly modifies the Health Insurance Portability and Accountability Act by adding new requirements concerning the privacy and security of health information. Under the HITECH Act, the HIPAA Privacy Rule (and the penalties that apply to violations of the Rule) apply not only to hospitals, clinics, and other covered entities, but also to individuals and organizations that provide services "for or on behalf of" a covered entity that involve the use or disclosure of "protected [individually identifiable] health information." An organization providing these services is designated as a "business associate" of the covered entity. See 45 C.F.R. §§ 160.103 (definition of a business associate) and 164.504(e) (business associate contracts). The HITECH Act explicitly specifies additional entities that must be treated as a business associate:

Each organization, with respect to a covered entity, that provides data transmission of protected health information to such entity (or its business associate) and that requires access on a routine basis to such protected health information, such as a Health Information Exchange Organization... is required to enter into a written contract (or other written arrangement) [i.e., a Business Associate Agreement], with such entity and shall be treated as a business associate of the covered entity for purposes of [the HIPAA Privacy and Security Rules].

HITECH Act § 13408; 42 U.S.C. § 17938 (emphasis added).

The North Dakota Health Information Network ("NDHIN") is a health information exchange organization and is, therefore, a business associate of each hospital, clinic, pharmacy, laboratory, health plan, etc., that is a Participant in the Network. Each Participant has signed a business associate agreement designating NDHIN as its business associate and granting NDHIN the authority to facilitate the exchange of individually identifiable health information between Participants of the Network; but also requiring the NDHIN to comply with all applicable provisions of the HIPAA Privacy and Security Rules—as well as other policies and contractual requirements.



Sheldon Wolf

April 6, 2012

Page 3

Under the HITECH Act and the HIPAA Privacy Rule, a business associate may disclose protected health information to a business associate that is a "subcontractor" and may allow the subcontractor to create or receive protected health information on its behalf, "if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i) [requirements for business associate contracts], that the subcontractor will appropriately safeguard the information." Proposed 45 C.F.R. § 164.502(e)(2)(ii). And, a business associate must "ensure that any subcontractors that create or receive protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information." Proposed 45 C.F.R. § 164.504(e)(2)(ii)(D). The Health Information Technology Office, with the Approval of the Health Information Technology Advisory Committee, has engaged a technology company as a "subcontractor" of the North Dakota Health Information Network to provide technological services that will assist North Dakota health care providers and health plans in the efficient and secure exchange of health information. That subcontractor, is Axolotl, which is now OptumInsight.™ The State, acting through the North Dakota Health Information Network, has a business associate agreement with Axolotl under which Axolotl has agreed to comply with all of the requirements for a business associate under the HIPAA Privacy and Security Rules including those requirements (discussed below) that prohibit both a covered entity and a business associate from disclosing health information for remuneration to any third party.

The HIPAA Privacy Rule generally prohibited the sale of individually identifiable health information, but the HITECH Act makes this prohibition more explicit by providing that "a covered entity or business associate shall not directly or indirectly receive remuneration in exchange for [disclosing] any protected health information of an individual" unless the covered entity obtains the individual's authorization. HITECH Act § 13405(d); 42 U.S.C. § 17935(d) (emphasis added). The HITECH Act further explicitly provides that it applies to the sale of protected health information in electronic health records. HITECH Act § 13405(d); 42 U.S.C. § 17935(d) (caption "(d) PROHIBITION ON SALE OF ELECTRONIC HEALTH RECORDS"). The HITECH Act will be implemented through amendments to the HIPAA Privacy Rule that will require a covered entity to obtain an authorization "for any disclosure of [individually identifiable health information] for which the disclosure is in exchange for direct or indirect remuneration from or on behalf of the recipient of the protected health information." See proposed 45 C.F.R. § 164.508(4).

Now it should be noted that there are a few exceptions that permit payment to a covered entity or business associate for the disclosure of health information. For example, the prohibition against remuneration does not apply to the disclosure of protected health information for public health purposes under 45 C.F.R. § 164.512(b) (the general rule on disclosures to public health authorities and for other public health purposes). HITECH Act § 13405(d)(2)(A); 42 U.S.C. § 17935(d)(2)(A). The prohibition against remuneration also does not apply to a disclosure "[t]o or by a business associate for activities that the business associate undertakes on behalf of a covered



Sheldon Wolf

April 6, 2012

Page 4

entity. . . [if] the only remuneration provided is by the covered entity to the business associate for the performance of such activities." HITECH Act § 13405(d)(2)(E); 42 U.S.C. § 17935(d)(2)(E) (emphasis added.) The justification for these exceptions is that it is not unreasonable to compensate a business associate for the work it must undertake to comply with disclosures that are required by law or by the business associates' contract with the covered entity for whom it is providing technology services. But again, in general, the sale of health information to unaffiliated third parties is prohibited—and any such disclosure would be a violation of the HIPAA Privacy Rule subjecting the business associate to all applicable civil and criminal penalties.

It also should be noted that under North Dakota law any individually identifiable health information "submitted to, stored in, or transmitted by the health information exchange [NDHIN]. . . and any such data or record in the possession of the health information technology office is confidential" and, therefore, not subject to disclosure under the open records law. N.D.C.C. § 54-59-29. Consequently, because state law prohibits the disclosure of confidential information except as specifically required or permitted, selling confidential health information, without an authorization, would be an impermissible disclosure of the information.

In addition, the NDHIN has created policies that have been approved by the Health Information Technology Advisory Committee. Each Participant agrees to comply with the NDHIN policies in its executed Participation Agreement with NDHIN. One of the policies addresses the allowed use and disclosure of health information, and specifically prohibits the sale of health information without authorization of the individual to whom the information pertains. (See Exhibit A, NDHIN Policy 11, USES AND DISCLOSURES OF HEALTH INFORMATION, page 2.)

So to summarize my conclusions: the HIPAA Privacy Rule and the HITECH Act prohibit the sale of individually identifiable health information by hospitals, clinics, other health care providers, and health plans, and also prohibit the sale of health information by business associates and subcontractors (except in the specific, narrow circumstances described above).

Let me know if you have any other questions regarding this issue.

Sincerely,

Michael J. Mullen

Michael J. Mullen

Special Assistant Attorney General for ITD

Enclosure: Exhibit A

CC: Pam Crawford, Assistant Attorney General

## **USES AND DISCLOSURES OF HEALTH INFORMATION**

**Policy Statement:** Individual Health information may be accessed only by Authorized Users through the North Dakota Health Information Network (NDHIN) for only the purposes consistent with this policy.

### **Compliance with Law**

All disclosures and uses of health information through the NDHIN must be consistent with all Applicable Laws and the NDHIN Policies, and may not be used for any unlawful or discriminatory purpose. If applicable law requires that certain documentation exist (such as an authorization) or that other conditions be met prior to using or disclosing health information for a particular purpose, the requesting Participant shall ensure that it has obtained the required documentation or met the requisite conditions and shall provide evidence of the documentation and conditions at the request of the disclosing Participant.

### **Participant Permitted Purposes**

A Participant may request and may disclose individual health information through the NDHIN only for purposes of treatment, payment, health care operations, to comply with public health reporting requirements, and as required by law.

Each Participant shall provide or request Individually Identifiable Health Information through the NDHIN only to the extent necessary for the permitted purpose.

Any other use of Individually Identifiable Health Information data is prohibited.

### **NDHIN Permitted Purposes**

NDHIN may use and disclose Protected Health Information (PHI) for the following purposes:

1. for the proper management and administration of the Business Associate, in accordance with 45 C.F.R. § 164.504(e)(4);
2. **subject to the Participation Agreement, NDHIN Policies and Procedures, and 45 C.F.R. §§ 164.504(e)(2)(i) and 164.504(e)(2)(i)(B), provide data aggregation services related to the health care operations of the covered entities with which NDHIN has a Participation Agreement;**
3. **manage authorized requests for, and disclosures of, PHI among Participants in the network;**
4. **create and maintain a master patient index;**
5. **provide a record locator or patient matching service;**
6. **standardize data formats;**
7. **implement business rules to assist in the automation of data exchange;**
8. **facilitate the identification and correction of errors in health information records; and**
9. **subject to the Participation Agreement and the NDHIN Policies and Procedures, aggregate data on behalf of multiple covered entities.**

**Prohibitions**

Except as permitted by the Health Insurance Portability and Accountability Act (HIPAA) privacy rule, Patient Data may not be used by a Participant or NDHIN for marketing, marketing related purposes, or sales without the authorization of the individual to whom the information pertains.

**Information Subject to Special Protection**

Certain health information may be subject to special protection under federal, state, or local laws and regulations (e.g., substance abuse). Each Participant shall identify any information that is subject to special protection under applicable law prior to disclosing any information through the NDHIN. Each Participant is responsible for complying with all applicable laws and regulations.

**Minimum Necessary**

Participants shall disclose and use only the amount of information reasonably necessary to achieve a particular purpose.

Each Participant may share health information obtained through the NDHIN with and allow access to the information by only those workforce members, agents, and contractors who need the information in connection with their job function or duties.

This minimum necessary policy does not apply to the disclosure of PHI to health care providers for treatment.

**Treatment and Insurance Denial Prohibition**

A health care practitioner may not deny a patient health care treatment and a health insurer may not deny a patient a health insurance benefit based solely on the provider's or patient's decision not to participate in the NDHIN.

**Participant Policies**

Each Participant shall have in place and shall comply with its own internal policies and procedures regarding the disclosure of health information and the conditions that shall be met and documentation that shall be obtained, if any, prior to making any such disclosure.