

To: RTI and VCU Project HealthDesign Team

cc: Patti Brennan and Gail Casper

From: Manatt, Phelps & Phillips, LLP

Date: August 2, 2010

Subject: Privacy and Security Law Analysis of Project HealthDesign Research Study

This memorandum is intended to provide staff members of the RTI International (“RTI”) and Virginia Commonwealth University (“VCU”) Project Health Design Research Study (the “Project”) with an overview of the privacy and security law issues that may affect the structure and implementation of the Project. Section I of the Memorandum provides a brief summary of our key findings. Section II describes the way in which health information is expected to be exchanged in connection with the Project. Section III summarizes applicable Virginia and federal privacy and security laws and regulations. Section IV contains an analysis of how these laws and regulations may be implicated by the Project.

**I. Summary of Key Findings**

- Neither the transmission of health information by patients to RTI through smart phones or sensors nor the transmission of such information by RTI to patients or VCU requires authorization under HIPAA or Virginia’s Health Care Privacy Law. However, for risk management purposes, it would be prudent to obtain each patient’s authorization for these transmissions as part of the informed consent process.
- Patients will not have any rights under HIPAA to request copies, amendments or an accounting of disclosures of health information maintained by RTI. As they do outside of the Project, patients will have such rights with respect to health information maintained by VCU.
- As is presumably its standard operating procedure, VCU will have to ensure that typical HIPAA compliant access controls, audit trails, authentication procedures and transmission security safeguards are in place with respect to health information maintained or transmitted by VCU. While HIPAA does not impose similar obligations on information maintained by RTI or on devices in patients’ homes, from a risk management standpoint, it would be prudent to adopt similar safeguards for these data.

## II. Overview of the Project

The Project is titled, “BreathEasy – A PHR for Adults Living with Asthma & Depression.” It focuses on low-income adult patients with asthma and depression treated at two ambulatory health care clinics owned by VCU Medical Center. Patients with psychiatric diagnoses other than depression (e.g. schizophrenia and bipolar disorder, among others), active suicidal ideation, or severe depression that renders the patient unable to participate in the study will be excluded.

Patients participating in the Project will be provided with password-protected smart phones, which they will use to report observations of daily living (“ODLs”), including peak-flow rates (a breathing measure), asthma medication adherence, level and types of physical activity, and subjective evaluation of symptoms. Passwords will probably be implemented at the device-level as opposed to the software application level. Patients will have the opportunity to disable the password function on their smartphones though doing so will be discouraged. Further, devices such as pedometers, portable spirometers, heart rate monitors, and portable flow meters, among others, may be used to collect and report additional information about patients to the Project. It is currently unclear how much information patients will be expected to input about their mental health status and medication adherence. Information could include how the patient feels each day, including his or her anxiety level, which the patient could communicate by clicking on an emoticon reflective of their mood. Patients may also provide information about adherence to mental health medications.

It is currently unclear how the devices (e.g. pedometers) collecting the ODLs will transmit the ODLs to the patients’ smart phones, as the Project has not yet identified which devices will be utilized. This may occur through some type of wireless upload.<sup>1</sup> All ODLs, including those collected via remote device, will be transmitted from patients’ smart phones to a database housed on RTI’s “enhanced security network (the “RTI Server”). The data will be protected during transmission from the smart phones to the RTI Server by SSL encryption. Patients’ smart phones will likely initiate data transmission to the RTI Server, either when manually instructed to do so by the patient (e.g., when the patient clicks on a button), or automatically at specified time periods (e.g., when a certain amount of data has been collected or when there is a sufficient connection for transmission). It is not expected that data transmitted from devices can be encrypted. RTI is a research organization and does not provide health care services.

Patients will enroll in the Project at one of the two participating VCU clinics, where a research coordinator will collect both demographic and health information in order to set up an

---

<sup>1</sup> The Project’s preliminary proposal summary indicated that these tools would report data to the patients’ smart phones “via serial or Bluetooth connection.” See page 7.

account for each patient. This information will be transmitted to the RTI Server along with the ODLs collected during the course of the Project. Patients will be prompted to provide consent for their participation in the Project, together with informed consent documents and other research-related forms required by RTI's and/or VCU's IRB.

Based on the ODLs reported by the patients or their remote monitoring devices, the Project will generate a web-based dashboard providing analysis and visualization tools that allow physicians and nurses to view their patients' data and evaluate their health status. The dashboard application will be accessible to participating physicians and nurses through a web-based portal. Physicians and nurses using electronic health records ("EHRs") could access the web-based portal by clicking on a hyper-link, which will take them outside of their EHR to the portal-site. It does not appear that the web-based portal will interact in any other way with the EHRs.

Physicians and nurses will likely participate in an initial enrollment session, at which time they will be provided unique user names and passwords to access the web-portal by Project staff. All physicians and nurses at the two VCU clinic sites participating in the Project will be authorized to access the ODLs of each patient participating in the Project at each clinic. Physicians and nurse access to the portal will be tracked.

RTI staff will have access to patient data through the portal for research purposes. They may also access data for system support and maintenance activities. While patients will not have access to the web-based portal, applications running on the RTI Server will generate messages to patients' smart phones. These messages may be texts, charts and graphs regarding the patient's condition. These messages may also provide reminders to take medications or contain positive reinforcement about healthy behaviors.

### III. Applicable Law

#### A. HIPAA

There are two regulations that have been issued under HIPAA that are relevant to the Project: the Privacy Rule (45 CFR §§ 160 and 164) and the Security Rule (45 CFR §§ 160 and 162). Both rules apply only to "covered entities," which include three types of organizations: health plans, health care providers conducting HIPAA transactions and health care clearinghouses. 45 C.F.R. § 160.103.

##### 1. *The Privacy Rule*

The HIPAA Privacy Rule restricts the use and disclosure of "protected health information" by covered entities. Protected health information is defined as "individually identifiable health information" maintained or transmitted in any form, except for certain

education and employment records. 45 C.F.R. § 160.103. Individually identifiable health information is information (including demographic data) created or received by a health care provider, health plan, employer or health care clearinghouse that relates to the health of an individual, the provision of health care or the payment for health care services, and that identifies or could reasonably be used to identify the individual. 45 C.F.R. § 160.103.

Covered entities may use and disclose protected health information without the individual's authorization for certain purposes such as treatment by a health care provider, payment and health care operations. 45 C.F.R. § 164.506(c). Protected health information may also be disclosed to the individual himself or herself without written authorization. 45 C.F.R. § 164.502(a)(1)(i). In addition, covered entities may use or disclose protected health information for research purposes in three different ways:

- Pursuant to the individual's written authorization;
- Pursuant to a waiver of the authorization requirement by an Institutional Review Board ("IRB") or Privacy Board in accordance with certain protocols; or
- Pursuant to a data use agreement between the covered entity and the researcher for the exchange of a "limited data set" that excludes facial identifiers.

45 C.F.R. § 164.512. A covered entity may share protected health information with a vendor acting on the entity's behalf (referred to as a "business associate") without patient authorization, but the business associate must adhere to the same restrictions on use and disclosure of the information as the covered entity. *See* 45 C.F.R. §§ 164.502(e) and 504(e).

If an authorization is required, it must contain the following elements: (i) a description in a "specific and meaningful fashion" of the information that will be used or disclosed, (ii) the name of the person or class of persons carrying out the use or disclosure, (iii) the name of the person or class of persons receiving the information, (iv) a description of the purpose of the disclosure, (v) an expiration date or event, (vi) the signature of the individual or his or her personal representative and (vii) required statements regarding the individual's right to revoke the authorization, the conditioning of treatment upon receipt of the authorization and the potential for re-disclosure. 45 C.F.R. § 164.508(c).

An authorization generally may not be combined with another document, but an authorization to disclose information for research purposes may be combined with an informed consent to participate in the research study. 45 C.F.R. § 164.508(b)(3)(i). Moreover, a covered entity may condition participation in a research study on the individual's willingness to sign an authorization permitting use and disclose of information generated through the research. 45 C.F.R. § 164.508(b)(4)(i).

The Privacy Rule also requires covered entities to afford individuals certain rights regarding their protected health information. These rights include, among others:

- The right to access to information contained in a “designated record set,” which is a group of records maintained by a covered entity that constitute medical, billing, enrollment, payment, claims or medical management records, or are records otherwise used to make decisions about an individual. 45 C.F.R. §§ 164.501 and 524.
- The right to request an amendment of records maintained in a designated record set. 45 C.F.R. § 164.526.
- The right to request an accounting of disclosures. Currently, the accounting does not have to include disclosures made: for treatment, payment or health care operations; to the individual; or pursuant to the individual’s authorization. 45 C.F.R. § 164.528. However, the Health Information Technology for Economic and Clinical Health Act (“HITECH”) requires the accounting to cover disclosures made through an electronic health record for treatment, payment or health care operations. This obligation becomes effective on the later of January 1, 2011 or the date on which the covered entity acquires a new electronic health record system. HITECH § 13405(c).

## 2. *The Security Rule*

The HIPAA Security Rule requires covered entities to employ certain administrative, physical and technical safeguards to protect the confidentiality and integrity of protected health information maintained or transmitted electronically. The Security Rule’s obligations are intended to be scalable: within the Security Rule’s parameters, a covered entity has discretion to adopt particular security measures based on the entity’s size, complexity, capabilities and resources. In addition, while certain security measures are required, others are “addressable,” which means that a covered entity has the flexibility, through a formal security risk analysis, to assess whether the measure is “reasonable and appropriate” in its particular environment and, if not, to adopt an alternative reasonable and appropriate measure. 45 CFR § 164.306(b).

The Security Rule’s administrative and physical safeguards generally apply across a covered entity’s entire enterprise.<sup>2</sup> See 45 C.F.R. § 160.308 and 310. Therefore, the Project is unlikely to trigger the need for new security policies or procedures to meet the administrative and physical safeguard standards. However, compliance with the Security Rule’s technical safeguard requirements often necessitates an activity-specific or data system-specific analysis.

---

<sup>2</sup> For example, the obligations to appoint a Chief Security Officer or configure workstations in a manner that minimizes incidental disclosures apply to all activities across the entire enterprise.

The Security Rule's technical safeguards that are most likely to be relevant to the Project are as follows:<sup>3</sup>

- Access controls to ensure that only authorized individuals are permitted to access protected health information. The controls include unique user identification, emergency access, automatic log-off (A) and encryption (A).
- Audit controls to record system activity.
- Authentication of system users.
- Transmission security measures covering protected health information sent over an electronic communications network. These measures include integrity controls (A) and encryption (A).

45 C.F.R. § 160.312.

## **B. State Law**

### *1. General Medical Information*

Virginia's Health Records Privacy Law is similar to HIPAA. The law restricts the disclosure of medical records by a "health care entity," which is defined to include any health care provider, health plan or healthcare clearinghouse. Va. Code Ann. § 32.1-127.1:03. A "health care provider" includes physicians, hospitals, podiatrists, chiropractors, physical therapists, physical therapy assistants, optometrists, clinical psychologists, clinical social workers, professional counselors, licensed dental hygienists and health maintenance organizations. Va. Code Ann. § 32.1-127.1:03(B) (quoting Va. Code Ann. § 8.01-581.1). A research organization that does not provide health care services is not a health care entity under the Health Records Privacy Law.

Individuals and entities subject to the statute may disclose a patient's medical information only pursuant to the patient's written authorization unless an exception applies. Va. Code Ann. § 32.1-127.1:03(D). There is an exception that covers disclosures "necessary in connection with the care of the individual," i.e., for treatment purposes. Va. Code Ann. § 32.1-127.1:03(D)(7). It is unclear whether there is an exception covering disclosures for research purposes, including the recruitment of patients to participate in research protocols. We were unable to obtain guidance from regulatory authorities on this issue.

---

<sup>3</sup> Those standards with an (A) next to them are addressable; the others are required.

If a patient's written authorization is required, it must contain all of the HIPAA-mandated elements referenced in Section III.A.1 above, such as a description of the purpose of the disclosure, the names of the parties disclosing and receiving the information, and an expiration date. Va. Code Ann. § 32.1-127.1:03(G). In addition, the authorization must contain the following (or substantially similar) language, which is similar to, but differs slightly from, the mandated HIPAA warning statements:

As the person signing this authorization, I understand that I am giving my permission to the above-named health care entity for disclosure of confidential health records. I understand that the health care entity may not condition treatment or payment on my willingness to sign this authorization unless the specific circumstances under which such conditioning is permitted by law are applicable and are set forth in this authorization. I also understand that I have the right to revoke this authorization at any time, but that my revocation is not effective until delivered in writing to the person who is in possession of my health records and is not effective as to health records already disclosed under this authorization. A copy of this authorization and a notation concerning the persons or agencies to whom disclosure was made shall be included with my original health records. I understand that health information disclosed under this authorization might be redisclosed by a recipient and may, as a result of such disclosure, no longer be protected to the same extent as such health information was protected by law while solely in the possession of the health care entity.

The Health Records Privacy Law prohibits re-disclosures of medical information beyond the purpose for which the disclosure was made unless a new authorization for re-disclosure is executed. However, this re-disclosure restriction does not prohibit a health care entity receiving health records from another health care entity from making subsequent disclosures permitted under the HIPAA Privacy Rule. The restriction also does not prohibit a health care entity from furnishing de-identified data to researchers. Va. Code Ann. § 32.1-127.1:03(A)(3).

## 2. *Mental Health Records*

Virginia law establishes special protections for the confidentiality of individually identifiable information for persons receiving services from a public or private provider of services operated, licensed or funded by the Department of Mental Health, Mental Retardation and Substance Abuse Services ("DMH"). 12 Va. Admin Code § 35-115-10(C). These protections, among other things, restrict re-disclosure of mental health information obtained from providers licensed or funded by DMH. Mental health information obtained from other sources is not subject to this statute.

## IV. Legal Analysis

### A. **Subject Authorization for Use and Disclosure of Information**

#### 1. *Transmission of Information From Phones and Devices to RTI*

ODLs relate to the health of an individual. Therefore, if ODLs are linked to identifiable information about an individual, they potentially constitute protected health information under HIPAA, even though they are created by subjects rather than providers. But both HIPAA and the Health Records Privacy Law restrict the use and disclosure of protected health information only by “covered entities” or “health care entities.” Neither statute regulates the disclosure of information by a patient of the patient’s own health information. As a result, neither HIPAA nor Virginia’s Health Records Privacy Law requires written authorization for the transmission of ODLs from smart phones and other devices to the RTI Server. Notwithstanding the foregoing, as discussed in Section IV.D below, for risk management purposes, it would be prudent for subjects to be educated about the security risks associated with their disclosure of ODLs and assume those risks as part of providing informed consent to participate in the Project.

#### 2. *Transmission of Information From RTI Server to VCU and Subjects*

RTI is a research institution that does not provide or bill third parties for health care services, and therefore, is not a covered entity under HIPAA. In addition, it is not acting as a data custodian or other type of vendor of VCU, but rather, receives information from VCU pursuant to each subject’s authorization. Therefore, RTI is not a business associate for HIPAA purposes. Accordingly, the disclosure of protected health information from the RTI Server to VCU (through a dashboard or other means) or to subjects (through messages to a subject’s smart phone) does not require written authorization under either statute. HIPAA imposes no restriction on the re-disclosure of protected health information obtained from a covered entity pursuant to an individual’s authorization. As a result, HIPAA does not regulate RTI’s disclosures under the Project even if a portion of the information being disclosed was obtained by RTI from VCU.

The Virginia Health Records Privacy Law, like HIPAA, does not apply directly to RTI. But, in contrast to HIPAA, the Virginia law prohibits parties receiving health information through a regulated health care entity from re-disclosing the information for any purpose inconsistent with the original authorization under which the party received the information unless the individual provides written authorization for the re-disclosure or the re-disclosure is otherwise permitted by law. Therefore, while the Virginia law does not restrict the re-disclosure of ODLs obtained by RTI from subjects, it does regulate RTI’s re-disclosure of information

obtained from VCU.<sup>4</sup> It is our understanding that RTI will not be re-disclosing identifiable data obtained from VCU to any third parties. But if it does, authorization under the Virginia Health Records Privacy Law would be required.

## **B. Subjects' Rights**

### *1. Access to Records by Subjects*

As indicated in Section III.A above, under HIPAA, individuals have the right to access records maintained in a designated record set. But designated record sets are maintained only by covered entities. RTI is not a covered entity. In addition, it receives information from subjects or from VCU pursuant to the subject's authorization; it does maintain records on VCU's behalf as VCU's business associate. Therefore, the records maintained in the RTI Server are not subject to the provisions of HIPAA granting individuals access to their records. Information received by VCU from RTI (such as the dashboards generated by applications running on the RTI Server) would not be automatically integrated into VCU's EHR, but if a VCU health care provider made notes in the EHR based on a dashboard, these notes would become part of the designated record set maintained by VCU. Under HIPAA, each subject would have the right to access this information from VCU upon request.

### *2. Amendments of Records by Subjects*

Section III.A indicates that individuals' amendment rights are also limited to information maintained by a covered entity in a designated record set. Accordingly, for the reasons described in Section IV.B.1 above, subjects will have no amendment rights with respect to information maintained in the RTI Server but they will have the right to request amendments to any information integrated into the VCU electronic medical record system.

### *3. Accountings of Disclosures*

Individuals are entitled to an accounting of disclosures made for certain purposes by covered entities. Because RTI is not a covered entity or a business associate acting on a covered entity's behalf, any disclosures made from the RTI Server will not be subject to the accounting requirement. VCU, while a covered entity, will not be transmitting protected health information to the RTI Server through the web-based portal under the Project. Therefore, none of the disclosures made in connection with the Project should require an accounting.

---

<sup>4</sup> The Health Records Privacy Law contains two exceptions to the re-disclosure prohibition: one covers disclosures between health care entities that are permitted under HIPAA and the other that permits disclosure of de-identified data by health care entities to researchers. But neither of these exceptions is applicable.

## **C. HIPAA Security Rule Requirements**

The Security Rule applies only to electronic protected health information maintained or transmitted by covered entities or their business associates. Therefore, the Security Rule's provisions on access controls, audit trails, authentication and transmission security do not apply to information maintained or transmitted by subjects or RTI. They apply only to information maintained by VCU, and they apply in the same manner as generally applicable to VCU's activities outside the Project. This Section IV.C discusses the application of the Security Rule to VCU under the Project. We discuss in Section IV.D below the extent to which RTI should employ similar safeguards for risk management purposes, even though it is not technically subject to the HIPAA Security Rule.

### *1. Access Controls*

VCU must have safeguards in place to ensure that only authorized VCU clinicians who are treating individuals participating in the Project have access to ODLs or other information integrated by VCU into its electronic medical record system. Access controls typically include procedures for issuing a unique user identification to each system user, granting and terminating access rights to the system in connection with employment, limiting access to records based on an individual's role in the organization and facilitating emergency "break the glass" access for medical emergencies. It is our understanding that all VCU clinicians will have access to any subject's records in the electronic medical record system, without regard to whether the clinician is actually treating the subject. This is not an uncommon arrangement among health care providers because restricting access based on preexisting treatment relationships can impede timely treatment when new referrals are made or practitioners are covering for one another. To address the potential for improper access by clinicians for purposes unrelated to treatment, health care providers typically monitor audit trails retrospectively to confirm that practitioners accessing a subject's records have a treatment relationship with the subject. Audit trail obligations are discussed in Section IV.C.2 below.

### *2. Auditing*

As it presumably already does, the VCU EHR must have the capacity to track each system user's access to ODLs or other data maintained in the system. The system must be able to produce audit trail reports covering uses and disclosures of information during the previous six-year period. Audit trails should be monitored periodically to detect improper access or disclosure of protected health information. As indicated in Section IV.C.1 above, monitoring audit trails is particularly important if the VCU electronic medical record system does not technically restrict access to ODLs to those clinicians with a preexisting treatment relationship with the patient.

### 3. *Authentication*

While the Security Rule does not mandate the nature of the authentication procedures implemented by covered entities, assigning unique identification numbers to each system user and requiring the entry of a user-specific password to access protected health information is assumed to be a minimum standard. The VCU EHR should, and presumably already does, have an effective password management system, which requires strong passwords, obligates users to change their passwords periodically and prohibits both group passwords and the sharing of passwords by users. More robust authentication measures such as biometric identification may be considered but are not generally deemed mandatory.

#### **D. Security Risk Management Considerations for RTI**

While the data maintained on and transmitted from the subjects' smart phones, the in-home sensors and the RTI Server are not subject to the Security Rule, it would be prudent from a risk management standpoint to establish reasonable security safeguards to protect these data. In the event of a security breach, the absence of such safeguards could lead to adverse publicity about RTI and the Project, and possibly trigger legal claims against RTI under state law negligence theories, especially since RTI is providing subjects with the technology that is being used to capture and transmit the ODLs. Moreover, RTI might fall within the definition of a "personal health record vendor" under HITECH.<sup>5</sup> If it does, RTI would have to provide subjects (and potentially the Federal Trade Commission and media outlets) with notice of any security breach involving information maintained on or transmitted from the RTI Server. *See* 42 U.S.C. § 17937. RTI might also be subject to breach notification obligations under Virginia law.

For all of these reasons, it is recommended that RTI employ security safeguards similar to those discussed above. This would include:

- Facilitating password protection for the application used on the smart phones to input ODLs and to send and receive ODL-related messages.
- Exploring whether it is feasible to encrypt data residing on the smart phones and sensors.
- Encrypting ODLs when transmitted between the smart phones and the RTI Server and from the RTI Server to the web-based portal where VCU clinicians may access them.

---

<sup>5</sup> A personal health record vendor" is an entity other than a covered entity that offers or maintains a personal health record. A personal health record is an electronic record of PHR identifiable health information (on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual. *See* 42 USC 17921 (11),(18).



manatt | phelps | phillips

RTI and VCU Project HealthDesign Team

August 2, 2010

Page 12

- Exploring whether it is technically feasible to encrypt data transmitted from sensor devices to the RTI Server.
- Establishing authentication and access controls for RTI personnel accessing ODLs and other health information maintained on the RTI Server.

\* \* \* \*

We hope the above fully addresses all of the privacy and security legal issues relevant to the Project. We look forward to continuing our work with you on this matter.

200014021.4