

To: Carnegie Mellon Project Health Design Team

cc: Patti Brennan and Gail Casper

From: Manatt, Phelps & Phillips, LLP

Date: July 23, 2010 File No. 43630-030

Subject: Privacy and Security Law Analysis of Project Health Design Research Study

This Memorandum is intended to provide staff members of the Carnegie Mellon University (“CMU”) Project Health Design 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 Pennsylvania 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

- The transmission of health information by Presbyterian Senior Care (“PSC”) and its clinicians to Microsoft HealthVault (“HealthVault”) will require patient authorization under HIPAA and Pennsylvania law. This authorization can be incorporated into the Project’s informed consent document. Neither the transmission of health information by patients from home laptop computers or sensors nor the transmission of such information by CMU to patients or healthcare providers requires authorization under HIPAA or Pennsylvania 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 contained in HealthVault. Patients will have such rights with respect to health information maintained by PSC.
- PSC will have to ensure that HIPAA-compliant access controls, audit trails, authentication procedures and transmission security safeguards (including possibly encryption) are in place with respect to health information maintained or transmitted by PSC. While HIPAA does not impose similar obligations on information maintained or

transmitted by CMU or patients, from a risk management standpoint, it will be prudent to adopt similar safeguards for these data.

II. Overview of the Project

The Project is titled “Embedded Assessment of Elder Activities (Cognitive Decline and Arthritis) for Augmenting Personal Health Records.” It focuses on older community-dwelling adults at the low-income senior residences managed by PSC in Pittsburgh, Pennsylvania. PSC is a long-term care facility licensed under Pennsylvania law. These residents are at risk for cognitive decline and have osteoarthritis.

Sensor technology will be added into the residences of the participants that record observations of daily living (“ODLs”) such as preparing meals, using the phone, taking medicine, getting in and out of bed and chairs, and walking up and down stairs. Sensors around the house will communicate electronic data to a laptop placed in the subject’s home. The data being transmitted from the sensors to the laptop will not be encrypted because encryption will consume battery life and adversely affect data collection by the sensors. However, the data will consist solely of a string of numbers that will be meaningless to anyone without a decoder.

The laptop is password protected. This data is automatically uploaded to HealthVault. In addition, subjects may self-report ODLs through an application on their laptops that will auto-upload to HealthVault. Caregivers (e.g. family and friends) may also provide data through a web survey that is uploaded to HealthVault. Existing information from PSC’s electronic health record (“EHR”) system will populate data in each subject’s HealthVault account. Finally, a PSC-affiliated occupational therapist will perform tests on the subjects and upload testing data to HealthVault. It is not yet clear whether the results will first be transmitted to the PSC EHR or go directly to the HealthVault account. Research staff do not expect to obtain HIV or mental health information through the sensor technology. But it is possible such information could be disclosed through subject self-reporting or the caregiver reports.

CMU research staff will set up a standard HealthVault account for each subject. However, Microsoft will not be maintaining any information on HealthVault as a data custodian of CMU. Instead, the data maintained in HealthVault will be controlled by the subjects and will be disclosed to CMU or others only with the subject’s written authorization. Caregivers do not have access to the subject’s account. Each account will have a unique user identification and password. All collected, summarized data and integrated data will be encrypted on the laptop and transmitted to HealthVault through SSL encryption. Once the ODL data resides in HealthVault, the subject and the CMU research staff will have access to the data with the consent of each subject. CMU staff will be accessing this data in their capacity as researchers and not in a clinical capacity. CMU staff will write applications that will export data from HealthVault and perform various types of analyses on the ODLs to generate visualizations such as charts or

graphs. These visualizations will be accessible to the subject on the laptop in the subject's residence through a laptop application provided by CMU.

Subjects may print out and share these reports with their healthcare providers. In addition, each subject's clinician may obtain a similar type of application from CMU for his or her EHR to view the visualizations. CMU research staff will fully integrate sensed and analyzed data stored in HealthVault with the PSC EHR.

Subjects will sign written authorization forms authorizing CMU researchers and their clinicians to receive the visualizations. The authorization forms will be signed in connection with the subject's enrollment in the study, together with informed consent documents and other research-related forms required by CMU's IRB.

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 C.F.R. §§ 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:

CMU Project Health Design Team

July 23, 2010

Page 4

- 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 disclosure 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.¹ 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. The Security Rule's technical safeguards that are most likely to be relevant to the Project are as follows:²

- 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.

¹ 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.

² Those standards with an (A) next to them are addressable; the others are required.

- 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

Pennsylvania does not have a comprehensive medical confidentiality law. Instead, the State has a patchwork of laws that apply to particular types of health care providers and specific types of health information. State laws that are potentially relevant to the Project are described below.

1. *Provider-Specific Laws*

Long-term care facilities. All clinical records of residents in long-term care nursing facilities are considered privileged and confidential. “Written consent of the resident, or of a designated responsible agent acting on the resident’s behalf, is required for release of information.” 28 PA. CODE § 211.5(b). The law does not specify the required content of a consent form.

Occupational therapists. Occupational therapists must maintain confidentiality of clients’ records. 42 PA. CODE § 49.24(2)(v). The law does not specify the information that must be included in a written consent to disclose confidential records. Occupational therapists must also obtain written informed consent from subjects involved in research activities indicating they have been fully advised of potential risks and outcomes. 42 PA. CODE § 49.24(2)(iii). The law does not specify the required content of a consent form.

2. *Sensitive Health Information*

Mental Health Records. All documents concerning persons receiving voluntary or involuntary inpatient or outpatient treatment by mental health facilities must be kept confidential. Unless the person has provided written consent, these records may not be released or their contents disclosed to anyone.” 35 PA. CONS. STAT. § 7111(a). Exceptions include disclosures to, among others, those actively engaged in providing treatment for the person or to persons at other facilities when the person is being referred to that facility and the record is necessary to provide for continuity of proper care and treatment. 55 PA. CODE § 5100.32. The re-disclosure of confidential mental health information is prohibited unless authorized under the law. 55 PA. CODE 5100.32(c). The law does not specify the required content of a consent form.

HIV-Related Information. Pennsylvania law establishes special protections for “confidential HIV-related information.” A person who obtains confidential HIV-related information in the course of providing any health or social services or pursuant to a patient release may not disclose or be compelled to disclose the information. 35 PA. CONS. STAT. § 7607(a). Several exceptions apply, including disclosures to the subject, health care providers rendering medical treatment or any person authorized by the patient’s written consent. The re-disclosure of confidential HIV-related information is prohibited unless authorized under the law. 35 PA. CONS. STAT. § 7607(b). The law does not specify the required content of a consent form.

IV. Legal Analysis

A. Subject Authorization for Use and Disclosure of Information

1. Transmission of Information by Patients, Caregivers and Sensors to HealthVault

ODLs relate to the health of an individual. Therefore, if ODLs are linked to identifiable information about an individual, they constitute protected health information under HIPAA, even though they are created by subjects rather than providers. But HIPAA restricts the use and disclosure of protected health information only by “covered entities,” which include health care providers and health plans. HIPAA does not regulate the disclosure of information by a patient or a patient’s caregiver. In addition, there is no Pennsylvania law regulating the transmission of ODLs by patients. As a result, neither HIPAA nor Pennsylvania law requires written authorization for the transmission of ODLs from subjects, their caregivers or the sensors to CMU. 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 by PSC to CMU and HealthVault

PSC is a covered entity under HIPAA and is subject to Pennsylvania’s confidentiality law governing long-term care facilities. Moreover, PSC’s occupational therapists are subject to Pennsylvania’s confidentiality law applicable to such professionals. Neither CMU nor HealthVault is a health care provider or a covered entity under HIPAA. As a result, the HIPAA exception covering disclosures for treatment purposes is not applicable. Written authorization of each subject is required for the disclosure of any health information by PSC or its occupational therapists to CMU or HealthVault.

There is an argument that the disclosures by PSC are being made to the individual who is the subject of the information (and therefore do not require authorization) because the individual

will control the information maintained in HealthVault. However, we believe this argument is unlikely to prevail because CMU researchers will also be accessing the information in HealthVault. As a result, disclosure of data from PSC's EHR and testing data generated by PSC's occupational therapists to HealthVault will require the subject's written authorization under HIPAA and Pennsylvania law. The authorization form used for this purpose should include all of the HIPAA-mandated elements identified in Section III.A.1 above. Because State law does not specify the format or content of the authorization, a HIPAA-compliant authorization should be sufficient for such disclosures, provided it specifically states that the authorization covers sensitive data such as mental health and HIV information. As indicated above, the authorization may be included in a document under which the subject provides informed consent to participate in the Project.

3. *Transmission of Information From CMU and HealthVault to PSC and Subjects*

CMU is a research institution that does not provide or bill third parties for health care services. Therefore, it is not a covered entity under HIPAA. In addition, neither HealthVault nor CMU is acting as a data custodian or other type of vendor of PSC or any other covered entity, but rather, receives information from subjects or from third parties such as PSC pursuant to each subject's authorization. As a result, neither CMU nor HealthVault should be considered a business associate of PSC for HIPAA purposes. Accordingly, the disclosure of protected health information (e.g. visualizations) by HealthVault or CMU to PSC or to subjects does not require subjects' written authorization under HIPAA. 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 CMU's or HealthVault's disclosures under the Project even if a portion of the information being disclosed was obtained from a covered entity such as PSC pursuant to the patients' authorization.

Similarly, State law does not restrict the manner in which CMU or HealthVault makes data accessible to subjects or transmits data to health care providers.³ While subjects may report sensitive health information such as mental health conditions or HIV-related information to HealthVault, these self-disclosures will not be subject to Pennsylvania's laws protecting the confidentiality of such information. The State's mental health law governs only health facilities and providers' disclosures of records. Likewise, the HIV applies only to persons who obtain such information "in the course of providing any health or social service."

³ Subjects may report sensitive health information such as mental health conditions or HIV-related information to HealthVault. But the self-disclosure of mental health information by subjects will not be subject to Pennsylvania's laws protecting the confidentiality of such information. The mental health law applies only to licensed mental health facilities. And the HIV is applicable only to entities disclosing information "in the course of providing any health or social service." Therefore, the re-disclosure of this information by HealthVault is not regulated under these laws.

B. Subject's 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. Neither HealthVault nor CMU is a covered entity. In addition, both receive information from subjects or from PSC pursuant to the subject's authorization. These records are not maintained on PSC's behalf as a business associate. Therefore, the records maintained in the HealthVault are not subject to the provisions of HIPAA granting individuals access to their records. Any visualizations or other data received by PSC from CMU that are integrated into PSC's EHR would become part of the designated record set maintained by PSC. Under HIPAA, each subject would have the right to access this information from PSC 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 HealthVault or CMU's trend reports but they will have the right to request amendments to any information integrated into the PSC EHR.

3. Accountings of Disclosures

Individuals are entitled to an accounting of disclosures made for certain purposes by covered entities. Because neither CMU nor HealthVault is a covered entity or a business associate acting on a covered entity's behalf, any disclosures of raw data or the trend reports made from HealthVault will not be subject to the accounting requirement. PSC, which is a covered entity, may transmit protected health information to HealthVault accounts. But all of these disclosures will be made pursuant to the subject's written authorization. Disclosures made with the individual's authorization are not subject to HIPAA's accounting requirement. Therefore, none of the disclosures made in connection with the Project should require an accounting.

C. Security Concerns

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 CMU; they apply only to information maintained or transmitted by PSC. This Section IV.C discusses the application of the Security

Rule to PSC's activities under the Project. We discuss in Section IV.D below the extent to which CMU should employ similar safeguards for risk management purposes, even though it is not technically subject to the HIPAA Security Rule.

1. *Access Controls*

PSC must have safeguards in place to ensure that only authorized PSC clinicians who are treating individuals participating in the Project have access to ODLs, visualizations or other information integrated by PSC into its EHR. 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 possible that all PSC clinicians will have access to any subject's records in the EHR 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.

The Security Rule's addressable access control standards include automatic log-off and encryption. It is our experience that, although addressable, the standard for automatic log-off has been widely adopted throughout the industry and is informally treated by regulatory authorities as a required standard. In contrast, encryption for data at rest has not been widely implemented by health care providers because of the negative impact on system performance. However, if PSC elects not to encrypt the ODLs, it should do so in accordance with a written security risk analysis that provides a rationale for not encrypting and recommends alternative safeguards.

2. *Auditing*

PSC's EHR must have the capacity to track each system user's access to ODLs or other data maintained in such system. In addition, the EHR must be able to track disclosures of this information by PSC clinicians to HealthVault. 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 PSC EHR 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. PSC should also 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.

4. *Transmission Security*

PSC will have to comply with the Security Rule's transmission security requirements when uploading information to HealthVault. While encryption is an addressable standard, there should be no significant obstacle to encrypting data transmitted to HealthVault using SSL encryption. It is our understanding that such encryption is contemplated under the Project.

No specific type of encryption is mandated under the Security Rule. However, in issuing guidance defining when protected health information is deemed "unsecured" for purposes of triggering a covered entity's breach notification obligations under Section 13402 of HITECH, the U.S. Department of Health and Human Services ("HHS") has taken the position that data at rest is not unsecured if it is encrypted in accordance with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices and data in motion is not unsecured if it is encrypted in accordance with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; 800-113, Guide to SSL VPNs; or others which are Federal Information Processing Standards (FIPS) 140-2 validated. See *HHS Guidance to Render Unsecured Protected Health Information Unusable, Unreadable or Indecipherable to Unauthorized Individuals*, 74 Fed. Reg. 19006 (April 27, 2009). Thus, even though the NIST standards are technically not mandated under HIPAA, they are becoming a widely accepted benchmark for determining whether encryption is sufficiently strong for HIPAA compliance purposes. Accordingly, the NIST standards should be followed to the fullest extent feasible.

D. Security Risk Management Considerations for CMU

While the data maintained on and transmitted from the subjects' laptops, the in-home sensors and HealthVault 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 CMU and the Project, and possibly trigger legal claims against CMU under state law negligence

CMU Project Health Design Team

July 23, 2010

Page 12

theories, especially since CMU is providing subjects with the technology that is being used to capture and transmit the ODLs. CMU might also be subject to breach notification obligations under state law.

Moreover, HealthVault likely falls within the definition of a “personal health record vendor” under HITECH.⁴ As a result, HealthVault 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 in connection with the Project. *See* 42 U.S.C. § 17937. Any such notification would heighten the risk of adverse publicity and legal claims against CMU.

For all of these reasons, it is recommended that CMU employ security safeguards similar to those adopted by PSC under the Security Rule. This would include:

- Facilitating password protection for the application used on the laptops to input ODLs and to send and receive ODL-related messages.
- Encrypting data residing on the laptops.
- Encrypting ODLs when transmitted between the laptops and HealthVault.⁵
- Establishing authentication and access controls for CMU personnel accessing ODLs and other health information maintained on HealthVault.

* * * *

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.

200015659.6

⁴ 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).

⁵ We understand that encryption of data being transmitted from sensors to laptops would undermine data collection. We do not believe the failure to encrypt these data is imprudent because the data is not interpretable without a decoder.