

To: University of California at Berkeley 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 University of California at Berkeley 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 California 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 the University of California San Francisco (“UCSF”) to The Healthy Communities Foundation (the “Foundation”), Google Health and The Carrot will require patient authorization under HIPAA. The California Confidentiality of Medical Information Act (“CMIA”) will require patient authorization for the transmission of information by UCSF to The Carrot and Google Health. This authorization can be incorporated into the Project’s informed consent document.
- The transmission of information from The Carrot and Google Health to subjects, The Foundation and UCSF is subject to the CMIA but these transmissions should fit within CMIA exceptions that preclude the need for each subject’s authorization. However, for risk management purposes, it would be prudent to obtain each subject’s authorization for these transmissions as part of the informed consent process.
- Neither the transmission of health information by patients to UCSF through smart phones or CyTek cards (if utilized) nor the transmission of such information by The Foundation to UCSF is subject to HIPAA or the CMIA. However, for risk management purposes, it may nonetheless be prudent to obtain each patient’s authorization for these transmissions as part of the informed consent process.

Foundation Project Health Design Team

July 23, 2010

Page 2

- Patients will not have any rights under HIPAA or the CMIA to request amendments or an accounting of disclosures of health information maintained by The Foundation, The Carrot or Google Health. Patients will have such rights with respect to health information maintained by UCSF under HIPAA and State law. Patients will have the right to access copies of their records maintained by UCSF, The Carrot and Google Health under HIPAA and the CMIA.
- UCSF clinicians 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 the clinicians. The Carrot and Google Health will also need to maintain similar controls under the California Security Law. While neither HIPAA nor the California Security Law impose security obligations on information maintained by The Foundation, 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 “Crohnology.MD.” It focuses on the collection of observations of daily living (“ODLs”) from individuals with Crohn’s Disease. ODLs will potentially be captured in two ways. First, the Foundation will provide subjects with devices such as scales and pedometers that can measure the subject’s weight, walking speed and other daily activities. Second, the Foundation may provide subjects with a CyTek report card that the subject can use to input data about his or her activities and symptoms that are relevant to Crohn’s Disease. The ODLs will not contain any HIV-related information but they maintain contain information about a subject’s mental health conditions. None of the subjects will be minors.

The data collected by the devices and the CyTek card (if utilized) will be transmitted through a wireless interface to a smart phone that the Foundation will provide to each subject. The data will be encrypted while it is stored on the smart phone. The application on the phone that must be used to access the data or the phone itself will require a password for access.

The data will then be transmitted wirelessly from the smart phones to a storage server maintained by the University of California, San Francisco (“UCSF”). Subjects will also have the option of taking their CyTek card (if utilized) to the UCSF clinic, where it can be scanned. Wireless transmissions are secured in accordance with Continua Health Alliance standards. The UCSF server is located in a secure facility that is maintained by an entity called Academic Research Services, which satisfies National Institutes for Health security standards for research projects.

Foundation Project Health Design Team

July 23, 2010

Page 3

Applications running on the UCSF storage server will generate presentations analyzing the ODLs transmitted about each subject. The Foundation's research team will have access to these presentations as well as the raw data maintained on the server. The presentations will also be made accessible to physicians who are members of the UCSF faculty practice plan and nurse practitioners working with them. Clinicians will go to an SSL-encrypted website established by UCSF for this purpose.

Subjects will have alternative mechanisms for accessing their presentations. A subject could set up a personal health record account on Google Health. If a subject selected this option, UCSF could access lab and medication data through Google Health with the subject's authorization. Alternatively, a subject might access his or her presentations through The Carrot. In either case, the subject would be responsible for establishing account with a unique user identification and password. UCSF will establish an interface with Google Health and The Carrot to facilitate the encrypted transmission of presentations.

Subjects will sign written authorization forms authorizing Foundation researchers and UCSF clinicians to receive the subject's trend reports. 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 UCSF's IRB. Enrollment will typically take place at UCSF practice sites.

### **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.

Foundation Project Health Design Team

July 23, 2010

Page 4

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 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.<sup>1</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>1</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>2</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. *California Confidentiality of Medical Information Act***

The California Confidentiality of Medical Information Act (the "CMIA") applies to all licensed health care professionals, hospitals, other licensed health care facilities, Knox-Keene health plans and the contractors of any of the foregoing. The CMIA also defines a "provider of health care" to mean:

Any business organized for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual, shall be deemed to be a provider of health care subject to the requirements of [the CMIA].

Cal. Civil Code § 56.06(a).

Individuals and entities subject to the CMIA may disclose a patient's medical information only with the patient's authorization, except for specified purposes. Cal. Civil Code § 56.10. Two notable exceptions permit a health care provider to disclose medical information to:

---

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

- other health care providers of health care for purposes of diagnosis or treatment of the patient; or
- to clinical investigators and accredited public or private nonprofit educational or health care institutions for bona fide research purposes, provided the recipient does not re-disclose the information in a way that would identify the patient.

Cal. Civil Code § 56.10(c)(1) and (7).

The CMIA requires that a patient's written authorization contain many of the HIPAA-mandated elements. If an authorization is obtained, it must: (1) be handwritten by the person who signs it or is in a type face no smaller than 14-point type; (2) be clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization; (3) be signed and dated by the patient or authorized representative; (4) state the specific uses and limitations on the types of medical information to be disclosed; (5) state the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information; (6) state the name or functions of the persons or entities authorized to receive the medical information; (7) state the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information; (8) state a specific date after which the provider of healthcare, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information; and (9) advise the person signing the authorization of the right to receive a copy of the authorization. Cal. Civil Code § 56.11.

The CMIA prohibits re-disclosures of medical information unless a new authorization is provided or some other exception applies. Re-disclosures of general medical information to health care providers for treatment purposes would be permitted.

The CMIA requires providers of health care, upon request, to provide each patient, at no charge, with a copy of any medical profile, summary, or information that it maintains. Cal. Civ. Code 56.07. A separate California statute gives patients the right to inspect and obtain copies of their patient record upon request. Cal. Health & Safety Code 123110(a),(b). The law also entitles a patient to provide a 250 word written addendum with respect to any item or statement in his or her record that the patient believes to be incomplete incorrect. Cal. Health & Safety Code 123111. A "patient record" is a "record in any form or medium maintained by, or in the custody or control of, a healthcare provider relating to the health history, diagnosis or condition of a patient or relating to treatment provided or proposed to be provided to the patient." Cal. Health & Safe Code 123105(d).

## 2. *Mental Health Laws*

Under California's Lanterman-Petris-Short Act, the records of health care facilities providing mental health treatment are subject to special protection. Cal. Welf. and Inst. Code § 5328. The Act applies to specialized mental health facilities and general hospitals. Mental health records may be disclosed only pursuant to an authorization of the patient, except in limited circumstances. The Act does not generally specify the form or content of an authorization.

## 3. *California Security Law*

California law imposes a general obligation on "providers of health care" to employ "appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information." Cal. Health and Safety Code § 130203 (the "California Security Law"). Providers must reasonably safeguard confidential medical information from any unauthorized access or unlawful access, use or disclosure. This law applies to providers subject to the CMIA.

The precise nature of these safeguards is not specified in the statute. We anticipate, however, that the security standards issued under HIPAA will serve as key industry benchmarks for evaluating compliance with the California Security Law. We believe this will be the case for several reasons:

- The term "administrative, technical and physical safeguards" mirrors the language used in the HIPAA privacy and security rules. *See* 45 C.F.R. §§ 164.308-312 and 164.530(c).
- The California Security Law specifically references a provider's compliance with "other related state and federal statutes and regulations" as a factor in evaluating whether a provider's safeguards are adequate.
- HIPAA has effectively become a recognized "standard of care" for security in the health care industry because it applies nationally and provides the most detailed set of security standards issued under relevant laws or regulations.

## **IV. Legal Analysis**

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

#### **1. *Transmission of Information From Individuals to UCSF***

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 CMIA restrict the use and disclosure of protected health information only by “covered entities” or “providers of health care.” Neither statute regulates the disclosure of information by a patient of the patient’s own health information. As a result, neither HIPAA nor the CMIA require written authorization for the transmission of ODLs from smart phones and other devices to the UCSF 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 UCSF to The Foundation, The Carrot and Google Health***

UCSF is both a covered entity under HIPAA and a “provider of health care” under the CMIA. Therefore, the written authorization of each subject is required for the disclosure of any health information by UCSF to The Foundation, The Carrot and Google Health unless an exception applies.

Because The Foundation, The Carrot and Google Health are not health care providers, the HIPAA exception covering disclosures for treatment purposes is not applicable. Any disclosures by UCSF would appear to require the subject’s written authorization under HIPAA. The authorization form used for this purpose should include all of the required elements in Section III.A.1 above. As indicated above, the authorization may be included in a document under which the subject provides informed consent to participate in the Project.

The CMIA will also apply to transmissions of medical information from UCSF to The Foundation, The Carrot and Google Health. Under the CMIA, UCSF may disclose medical information to other providers of healthcare for treatment purposes without each subject’s authorization. UCSF may also disclose medical information to researchers without a subject’s authorization under the CMIA’s research exception. Thus, even though UCSF is subject to the CMIA, it will not need authorization from subjects to disclose information to The Foundation. Nonetheless, 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 the disclosure of their

ODLs by UCSF and authorize these disclosures as part of providing informed consent to participate in the Project. In addition, there is no exception covering disclosures by UCSF to The Carrot or Google Health; authorization of each subject will be required for these disclosures.

**3. *Transmission of Information From The Carrot and Google Health to The Foundation, UCSF and Subjects***

The Carrot and Google Health do not provide or bill third parties for health care services, and therefore, they are not covered entities under HIPAA. In addition, they are not acting as data custodians for UCSF, but rather, receive information from subjects. Therefore, The Carrot and Google Health are not business associates of UCSF for HIPAA purposes and HIPAA does not regulate their disclosures under the Project.

However, because The Carrot and Google Health maintain medical information supplied by subjects in order to make that information available to subjects and UCSF, The Carrot and Google Health are “providers of health care” under the CMIA. Thus, transmissions by The Carrot and Google Health are subject to the CMIA. Under the CMIA, they may disclose medical information to other providers of healthcare (such as UCSF) for treatment purposes without each subject’s authorization. They may also disclose medical information to Foundation researchers without a subject’s authorization under the CMIA’s research exception. Thus, even though The Carrot and Google Health are subject to the CMIA, they will not need authorization from subjects to make the disclosures contemplated by the Project. Nonetheless, 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 the disclosure of their ODLs by The Carrot and Google Health, and authorize these disclosures as part of providing informed consent to participate in the Project.

**4. *Transmissions From The Foundation to UCSF***

The Foundation is an entity 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 UCSF. Therefore, The Foundation is not a business associate of UCSF for HIPAA purposes. In addition, the Foundation is not likely to be viewed as a “provider of health care” under the CMIA because it is not in the business of maintaining medical information on behalf of patients or providers. Accordingly, neither HIPAA nor the CMIA is likely to regulate The Foundation’s disclosures under the Project. However, for risk management purposes, it would be prudent to obtain each subject’s authorization for these disclosures as part of the informed consent process.

## **B. Subject's Rights**

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

As indicated in Sections III.A, 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. Therefore, subjects have a right to access only records maintained by UCSF under HIPAA. Subjects have similar rights under California law.

The Carrot and Google Health are not covered entities under HIPAA but they are "providers of health care" under the CMIA. Therefore, subjects have a right to access any health information maintained about them by The Carrot or Google Health under the Project.

Because The Foundation is not a covered entity under HIPAA or a provider of health care under the CMIA, its records would not be subject to the patient access provisions of HIPAA or State law.

### **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 by The Foundation, The Carrot or Google Health, but they will have the right to request amendments to any information maintained by UCSF.

### **3. *Accountings of Disclosures***

Individuals are entitled to an accounting of disclosures made for certain purposes by covered entities. Because UCSF is a covered entity, disclosures made from the UCSF server will be subject to the accounting requirement. But such 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 Considerations**

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 The Foundation, The Carrot or Google Health. They apply only to information maintained or transmitted by UCSF. However, as noted in Section IV.D below, the California Security Law applies not only to UCSF, but also to

“providers of health care” such as The Carrot and Google Health. This Section IV.C discusses the application of the Security Rule to such disclosures under the Project.

## 1. *Access Controls*

Healthcare providers must have safeguards in place to ensure that only authorized personnel who are treating individuals participating in the Project have access to ODLs or other information integrated into their electronic medical records systems. 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 UCSF 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.

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 a provider 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*

UCSF must have the capacity to track each system user’s access to ODLs or other data maintained in such 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.

## 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. UCSF 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*

UCSF will have to comply with the Security Rule's transmission security requirements when transmitting information to the subjects. While encryption is an addressable standard, there should be no obstacle to encrypting data transmitted through the portal using SSL encryption.

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 The Carrot, Google Health and The Foundation**

The Carrot and Google Health will have to comply with the California Security Law's requirements. As indicated above, we anticipate that the HIPAA Security Rule standards will serve as key industry benchmarks for evaluating compliance with the California Security Law. Therefore, The Carrot and Google Health will have to employ safeguards similar to those adopted by UCSF under the Security Rule.

California's Security Law requirements would not apply to The Foundation as it is not a covered entity under HIPAA or a "provider of health care" under the CMIA. However, it would be prudent from a risk management standpoint to establish reasonable security safeguards to

Foundation Project Health Design Team

July 23, 2010

Page 14

protect these data. In the event of a security breach, the absence of such safeguards could lead to adverse publicity about The Foundation and the Project. A security breach could also possibly trigger legal claims against The Foundation under state law negligence theories, especially since The Foundation is providing subjects with the technology that is being used to capture and transmit the ODLs. The Foundation might also be subject to breach notification obligations under California law.

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

- Facilitating password protection on the smart phones or the application used on the smart phones to input ODLs and to send and receive ODL-related messages.
- Encrypting data residing on the smart phones and CyTek cards (if utilized).
- Encrypting ODLs when transmitted between the smart phones and the UCSF server and from the server to The Foundation and subjects.
- Exploring whether it is technically feasible to encrypt data transmitted from sensor devices to the UCSF server.
- Establishing authentication and access controls for UCSF and Foundation personnel accessing ODLs and other health information maintained on UCSF 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.