

To: SFSU 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 San Francisco State University (“SFSU”) 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 patients to Health Analytic Services, Inc. dba thecarrot.com (“The Carrot”) through smart phones is not subject to HIPAA or the California Confidentiality of Medical Information Act (“CMIA”). The transmission of information by The Carrot to subjects, SFSU researchers and the Family Health Center at San Francisco General Hospital (“FHC”) 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.
- Transmissions between FHC clinicians and subjects are governed by HIPAA and the CMIA. Under HIPAA and the CMIA, FHC may transmit health information to patients without written authorization. However, the disclosure of information about minors by FHC to either the minor or the minor’s caregiver may require authorization. For minors participating in the Project, FHC is obtaining the informed consent of both the minor and his or her parent or guardian. To address potential HIPAA and CMIA compliance issues, the informed consent documents should include an authorization for the transmission of information to the minor by FHC.

- Patients will not have any rights under HIPAA or the CMIA to request amendments or an accounting of disclosures of health information contained in The Carrot. Patients will have such rights with respect to health information maintained by FHC. Patients will have the right to access copies of their records maintained by The Carrot and FHC under HIPAA and the CMIA.
- FHC 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 its clinicians. The Carrot will also need to maintain similar controls and transmission security safeguards under California Security Law requirements.

II. Overview of the Project

The Project is titled “ODLs via Mobile Platforms for Youth with Obesity and Depression.” It focuses on low-income patients between the ages of 13 and 24 with obesity and depression. All subjects will be provided with smart phones or iPods with WiFi (both of which are referred to herein as “smart phones”), which they will use to regularly report observations of daily living (“ODLs”) such as mood swings, food intake, physical activity and other matters relating to their obesity and depression. The ODLs will not contain any HIV-related information. The smart phones may also be equipped with an application that permits subjects to report their medications. In addition to providing information through the smart phones, subjects may also report ODLs through a desktop or laptop computer if they own or have access to one.

The ODLs supplied by subjects will be transmitted from the smart phones through a WiFi connection to a website called The Carrot. An application developed by The Carrot will be installed on each smart phone. ODLs will not be stored on the smart phones. Any ODLs provided by subjects through a laptop or desktop computer will also be transmitted to The Carrot through SSL encryption.

Each subject will establish his or her own account on The Carrot. Each account will have a unique user identification and password that will be created by the subject. The subject must also click on The Carrot’s terms of use when establishing an account. The Carrot runs applications that will perform various types of analyses on the ODLs and generate trend reports in the form of charts, graphs and other user-friendly tools. The trend reports for a particular subject will be accessible to that subject through his or her password-protected account on The Carrot. A subject may access his or her trend reports through his or her account on The Carrot. The Carrot will also generate messages and reports relating to the management of obesity and depression to the smart phones used by subjects.

SFSU Project Health Design Team
July 23, 2010
Page 3

The trend reports will be accessible to each subject's clinicians and health coaches working at FHC, a hospital-based clinic. FHC clinicians and health coaches will be able to link electronically through the FHC electronic medical record system (the "EMR") to The Carrot to access the trend reports. The trend reports will be encrypted in transmission from The Carrot to the EMR through SSL. The trend reports can be downloaded into the EMR by the clinician or health coach. Subjects will not have any direct electronic access to the EMR but may exercise their traditional legal right to request a copy of their medical records. The trend reports will also be accessible to the SFSU research team through The Carrot. FHC clinicians or health coaches may send text messages regarding care management to the subject's smart phone based on the trend reports or other information available to them. The text messages cannot be encrypted but they will contain only non-medical information, such as notices to contact a clinician or go to The Carrot for more details.

Subjects will sign written authorization forms authorizing SFSU researchers and FHC 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 SFSU's and San Francisco General Hospital's IRBs. Enrollment will typically take place at the FHC or at the subject's school. The SFSU research team will notify The Carrot that a subject has signed the enrollment materials, which will then trigger notification by The Carrot to the subject to set up an on-line account.

Subjects over the age of 18 will sign their own authorization forms. For subjects between the ages of 13 and 18, the authorization will be executed by both the subject and the subject's parent or guardian. Individuals between the ages of 13 and 18 cannot participate in the Project without the consent of a parent or guardian.

Subjects are required to set up a password on their smart phone for initial log-in. Subjects are encouraged to log out after each session but the smart phone will not be deployed with an automatic log-off feature that is triggered after a period of inactivity. There must be a password created by the subject to access the application provided by The Carrot. A subject will not be able to access messages sent from The Carrot without accessing this application. But a subject will not have to use the application to see text messages from FHC clinicians or health coaches.

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

SFSU Project Health Design Team
July 23, 2010
Page 4

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

SFSU Project Health Design Team
July 23, 2010
Page 5

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

SFSU Project Health Design Team
July 23, 2010
Page 6

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.
- 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 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

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.

SFSU Project Health Design Team
July 23, 2010
Page 7

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:

- 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-disclosure of medical information unless a new authorization is provided or some other exception applies. Re-disclosure of general medical information to health care providers for treatment purposes is 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

SFSU Project Health Design Team
July 23, 2010
Page 8

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 both 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 form.

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 of health care that are 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 Phones and Devices to The Carrot*

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 Carrot. 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 The Carrot to FHC Clinicians, SFSU Researchers and Subjects*

The Carrot 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 the FHC clinicians, but rather, receives information from subjects. Therefore, The Carrot is not a business associate of FHC for HIPAA purposes. As a result, HIPAA does not regulate The Carrot’s disclosures under the Project.

However, because The Carrot maintains medical information supplied by the subject in order to make that information available through the trend reports and other means to the subjects and their providers, The Carrot is a “provider of health care” under the CMIA. Thus, transmissions by The Carrot are subject to the CMIA. Under the CMIA, The Carrot may disclose medical information in the trend reports to other providers of healthcare for treatment purposes without each subject’s authorization. The Carrot may also disclose medical information to SFSU researchers without a subject’s authorization under the CMIA’s research exception. Thus, even though The Carrot is subject to the CMIA, it 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 authorize these disclosures as part of providing informed consent to participate in the Project.

3. *Transmissions between FHC and Subjects*

FHC is a covered entity under HIPAA. Thus, FHC clinicians' and health coaches' text messages to subjects based on the trend reports will be subject to HIPAA. But under HIPAA, clinicians and health coaches may disclose protected health information about an individual to the individual without his or her authorization.

Under the HIPAA Privacy Rule, in most cases a parent is the personal representative of his or her minor children and must exercise the minor's rights with respect to the use and disclosure of protected health information. However, when a minor provides informed consent for treatment, the minor rather than the parent controls the disclosure of information related to such treatment.³ Another exception applies when a parent agrees to a confidential relationship between the minor and the provider. Under the Project, messages will be sent by FHC clinicians to minor subjects, not their parents. To avoid any claims that medical information was improperly sent to minors without parental consent even though the parent authorized the relevant treatment, during the informed consent process, parents of all minor subjects should authorize FHC to provide messages to the minor on an exclusive, confidential basis.

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. The Carrot is not a covered entity. In addition, it receives information from subjects; it does maintain records on FHC's behalf as a business associate. Therefore, the records maintained in The Carrot are not subject to the provisions of HIPAA granting individuals access to their records. Any information received by FHC clinicians from The Carrot that is integrated into the FHC electronic medical record system would become part of the designated record set maintained by the FHC. Under HIPAA, each subject would have the right to access this information from FHC upon request.

However, the CMIA's access to records provision applies to any "provider of health care," which includes The Carrot. Therefore, The Carrot will be required to provide such access under California law.

³ California law permits a minor who is 12 years or older to consent to mental health treatment or counseling on an outpatient basis if (1) the attending professional person thinks the minor mature enough to participate in outpatient services and (2) the minor would (A) present a danger of serious physical or mental harm to self or others without treatment or (B) is the alleged victim of incest or abuse. Cal. Fam. Code § 6924.

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 Carrot but they will have the right to request amendments to any information integrated into the FHC electronic medical record system.

3. *Accountings of Disclosures*

Individuals are entitled to an accounting of disclosures made for certain purposes by covered entities. Because The Carrot is not a covered entity or a business associate acting on a covered entity's behalf, any disclosures made from The Carrot will not be subject to the accounting requirement. FHC, which is a covered entity, will not be transmitting protected health information to The Carrot. Therefore, none of the disclosures made in connection with the Project should require an accounting.

C. Security 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 The Carrot. They apply only to information maintained or transmitted by FHC. However, as noted in Section IV.D below, the California Security Law applies not only to FHC, but also to "providers or health care" such as The Carrot. This Section IV.C discusses the HIPAA Security Rule requirements applicable to FHC under the Project.

1. *Access Controls*

FHC must have safeguards in place to ensure that only authorized FHC clinicians who are treating individuals participating in the Project have access to ODLs or other information integrated by FHC 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 possible that all FHC clinicians will have access to any subject's records in the FHC 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 FHC 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*

FHC's electronic medical record system 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. FHC 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*

FHC 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.

SFSU Project Health Design Team
July 23, 2010
Page 13

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

The Carrot must comply with California Security Law’s requirements when transmitting the trend reports to subjects, SFSU researchers and FHC clinicians. As noted above, we anticipate that the HIPAA Security Rule standards will serve as key industry benchmarks for evaluating compliance with the California Security Law. Thus, The Carrot will also need to employ security safeguards similar to those adopted by FHC under the Security Rule outlined above in Section IV.C.

The Carrot will send unencrypted text messages to subjects. As indicated above, encryption is an addressable standard under the HIPAA Security Rule, and by implication, under the California Security Law. It is our understanding that encryption of these messages is not technically feasible. Given the inability to encrypt, The Carrot is employing an alternative safeguard by limiting the text messages to generic information, such as notice to contact clinicians or check The Carrot’s website for a more detailed message. We believe The Carrot has a strong position that this approach satisfies HIPAA’s addressable encryption requirement, upon which The Carrot’s obligation under the California Security Law is based.

The Carrot might fall within the definition of a “personal health record vendor” under HITECH.⁴ If it does, The Carrot would have to provide subjects (and potentially the Federal

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 (“PHR”) is an electronic record of PHR identifiable health information (on an

SFSU Project Health Design Team
July 23, 2010
Page 14

Trade Commission and media outlets) with notice of any security breach involving information maintained on or transmitted under the Project. *See* 42 U.S.C. §17937. The Carrot would also be subject to breach notification obligations under California law.

* * * *

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.

200014001.4

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).