Title

Governance strategies for conducting text messaging interventions in clinical research.

Journal

Clinical and translational science, 7(2)

ISSN

1752-8054

Authors

Anderson, Nicholas
Morrison, Caitlin
Griffin, Jonathan
et al.

Publication Date

2014-04-01

DOI

10.1111/cts.12156

Peer reviewed

Governance Strategies for Conducting Text Messaging Interventions in Clinical Research

Nicholas Anderson, Ph.D.[1], Caitlin Morrison, M.P.H.[2], Jonathan Griffin, M.D., M.H.A.[3], William Reiter, M.D.[4], Laura-Mae Baldwin, M.D.[2], and Kelly Edwards, Ph.D.[5]

Abstract

There is increasing interest in medical text messaging interventions being used to achieve positive patient outcomes across a range of clinical research and health practice environments. Short messaging service (SMS) is a low-cost tool that provides an easy communication route to engage potentially broad populations through text messaging, and is part of the growing social trend toward increased adoption of personal communication technologies by patient populations. Testing the effectiveness and impact of various communication strategies requires navigation of a complex web of clinical and research regulations and oversight mechanisms. We describe a case study of the implementation of SMS to provide bidirectional communications between physicians and patients involved in routine care reminders to illustrate the review processes and governance structures needed. By mapping the regulatory and approval processes required to manage and steward a research study across clinical and community boundaries, we provide a guide for other translational health researchers who may utilize similar kinds of personally owned technology interventions as research tools. Clin Trans Sci 2014; Volume 7: 127–131

Keywords: translational research, clinical trials, computers, ethics

Introduction

The broad acceptance of mobile phone usage[1] coupled with the national adoption of electronic health records (EHRs) has provided the opportunity for using text messaging as a widespread and low-cost tool for patient engagement.[2–10] As short messaging service (SMS) systems and patient-owned devices exist outside the traditional clinical practice environments, clinical research that tests the health impacts of interventions using personally owned technology must address two sets of regulations related to patient privacy and health system regulatory requirements: the Health Insurance Portability and Accountability Act (HIPAA, HIPAA Privacy Rule) and human subjects' research requirements. Effective stewardship of personal information and patient-provider communication through text messages or other forms of personally owned technology remains an evolving landscape of unclear boundaries of information ownership, indemnity, and policy adherence.[11–13] Furthermore, when conducting research to evaluate the effectiveness of these technologies, researchers and clinical groups must navigate a complex intersection of institutional clinical and research regulations. Despite a well-established regulatory norm of separating clinical care from research to protect patients, when these lines become blurred, ethical challenges arise.[14,15] This paper reviews the available tools, strategies, and roles needed for conducting clinical research involving communications with personally owned technology, using text messaging as an example.

Case Study

We conducted a pilot clinical trial involving a cohort of patients within a primary care clinic based in Montana to assess whether text messaging would increase patient adherence to recommended lipid testing, and whether patients would engage in two-way messaging with the clinic. The technical architecture of the trial was developed using a three-part system: (1) REDCap,[16] a broadly used clinical trial management software platform; (2) a custom developed text messaging scheduling and management system; and (3) an industry web-based text messaging platform. Project stakeholders included clinicians and academic researchers, and required developing governance of the systems and data use across an HIPAA covered entity, a research entity, and a third-party company.

Over a period of 4 months, the project sent targeted messages to enrolled patients from the clinical health system through the third-party SMS system to the patients, and managed the delivery and responses of the messages. Messages that were consistent with expected results (i.e., "1, For Yes; 2, For No") were tracked in the REDCap system, messages that were unexpected in format (e.g. "I want to come in today") were reviewed daily by nursing staff for potential clinical action. Summary data from the trial were de-identified and made available to the researchers at the conclusion of the trial.

Tools and instruments for human subjects protection and research stewardship

When conducting research involving patients within an HIPAA covered entity, defined as an environment where health care is provided as a normal course of business, the researcher must adhere both to regulations in the institutional regulatory environment as well as to regulations regarding human subjects protection defined through HIPAA. Federal regulations protecting human subjects require that all research protocols must be submitted to a clinical covered entity's privacy board (which may be designated as the Institutional Review Board or IRB), which reviews the protocol and assures that protections are in place for participants and their identity, and that the risk of the research does not outweigh the benefits. Since SMS-based clinical research interventions require identifiable information in the form of telephone numbers as well as access to demographic or other clinical information depending on the target patient population and SMS outreach use case, there are multiple layers of permissions needed and oversight required. The tools below represent those typically used to clarify

[1]Department of Pathology and Laboratory Medicine, University of California, Davis, Sacramento, California, USA; [2]Department of Family Medicine, University of Washington, Seattle, Washington, USA; [3]Internal Medicine, St. Peters Medical Center, Helena, Montana, USA; [4]NorthWest EHR Collaborative, Anaconda, Montana, USA; [5]Department of Bioethics and Humanities, University of Washington, Seattle Washington, USA.

Correspondence: Nicholas Anderson (nranderson@udavis.edu)

DOI: 10.1111/cts.12156

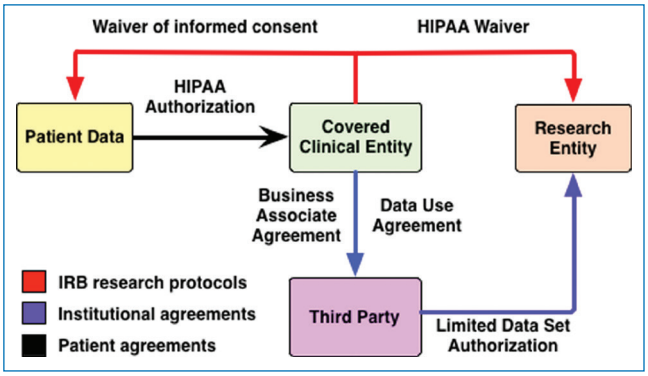

Figure 1. Overview of tools and relationships.

responsibility and relationships for conducting research with protected health information (PHI) and other clinical information (*Figure 1*).

HIPAA waiver or limited data set (LDS) authorization

The HIPAA of 1996 defined the HIPAA Privacy Rule, which instituted widespread practices of protection for PHI and has been effective since 2003. Under this rule, PHI cannot be released without explicit patient permission. However, because it is often impracticable to obtain such permission, institutions can grant a waiver of authorization (HIPAA waiver) under specific circumstances when appropriately justified. The HIPAA waiver defines the level of PHI accessible to researchers and the acceptable use of PHI. The HIPAA waiver for the release of information covers a data set containing PHI (names and phone numbers). If the researcher is only using an LDS (a data set that contains only dates, ages as values, or city/state or zip codes, and no other PHI), then an LDS authorization may be used in place of an HIPAA waiver.

HIPAA waiver/waiver of informed consent

When researchers seek to contact patients, they are required to gain formal consent through procedures in the study protocol or to provide the IRB with an appropriate justification for a waiver of informed consent. An HIPAA waiver may be used in situations with no patient contact, for example, preparatory to research studies or retrospective chart review. The HIPAA waiver and waiver of informed consent are agreements between the researcher and the IRB that grants the researcher authority to use patient data without either formal written consent and/or written HIPAA authorization from the patient. In this SMS project, researchers wanted to interview patients who had received text messages, and because the patients agreed to be contacted by researchers via personal contact with their physician, a waiver of informed consent was appropriate.

Business associates agreement (BAA)

As health care environments do not often have the technical resources to provide governed text messaging for patient communication, frequently they must outsource components of this service and develop governance for the transfer and management of PHI outside the health system boundaries. A BAA is developed as a legal agreement between a clinical entity and a third party, effectively stating that the third party is charged to do business on behalf of the clinical entity, with all the authority and accountability that also comes with that responsibility. The BAA grants authority to the third party to provide a service on behalf of the clinical entity. The business associate must be able to provide this service and assure security and compliance with the HIPAA Privacy Rule when handling PHI.

Data use agreement (DUA)

A DUA is created by the clinical entity (e.g., its IRB or ethics and corporate compliance committee) and is signed by the researchers to specify the terms of use for the patient or institutional data. A DUA generally defines the use of an LDS, and specifies that researchers: will not attempt to reidentify individuals from data provided, will use appropriate data security safeguards, will report any violations, and if they provide the limited data set to an agent or subcontractor of the research entity, will ensure that the subcontracting agent adheres to the same restrictions.

Authorized roles and relationships

There are four roles that represent authorities in defining the conduct of clinical research with personally owned technology: patient, clinical entity, research entity, and third party. We define the relationships based on these roles and the responsibilities as outlined and designated by agreements and tools outlined above.

Patient

Patients have the right to give full and informed consent to research and to the uses of their clinical health information. When this is impractical, the HIPAA regulations require the clinical entity to convene a Privacy Board to review the research uses of PHI. In accordance with regulatory allowances, many clinical entities designate the duties of the Privacy Board to an IRB. In this case, the IRB acts on behalf of the patient to ensure appropriate use and disclosure of PHI for research purposes. The IRB oversees a research entity's request to use PHI about patients associated with a clinical entity, including approval of the HIPAA waiver and the waiver of informed consent. These agreements grant the research entity appropriate access to PHI while establishing the appropriate level of involvement of the patient, if any.

Clinical entity

The clinical entity has fiduciary responsibility for patients and PHI within the system. Safeguards, such as LDSs and DUAs, can protect patient interests and, therefore, clinical entity responsibilities. There may be policy-driven vetting procedures required by the clinical entity leading to formal authorization of the HIPAA waiver on behalf of the patient.

Research entity

The research entity is granted authority by the patient to use their data for research through defined research protocols. The research entity is further granted authority by the clinical entity to access clinical data through DUAs, and through HIPAA waivers and authorizations.

Third-party entity

A third-party entity is an external company that provides service outside the HIPAA covered clinical entity or research entity. The clinical entity may authorize a third-party entity to use patient data for contacting an individual and conducting an intervention

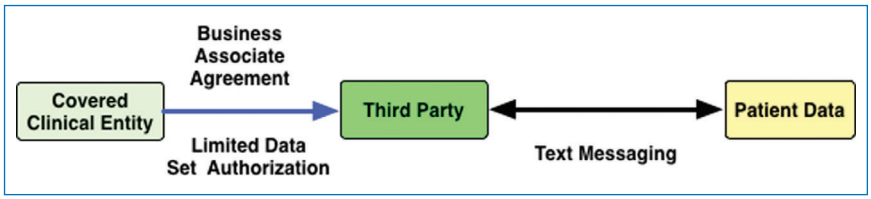

Figure 2. SMS as clinical activity.

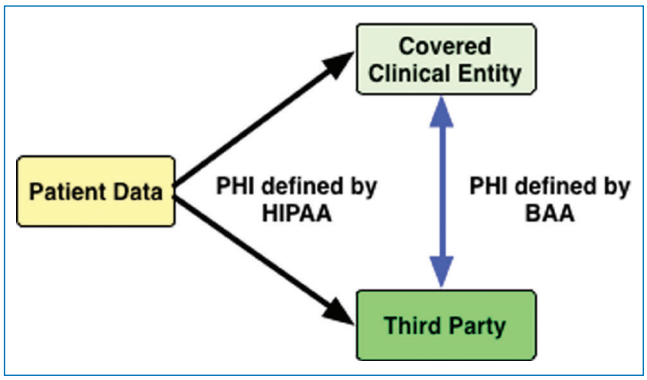

Figure 3. Defining PHI transfer using SMS for research.

associated with personally owned technologies through a BAA. This agreement describes the intent, agents, and obligations of the third party to ensure security and auditing of use of the patient data.

Implementation

We describe three stages that outline a model environment, beginning with a clinician who sees patients, and resulting in the ability to use patient-provided SMS data from patients' personally owned technology for research.

Framing SMS as a clinical activity that can be used for research

Text messaging patients as a care innovation does not require a formal written consent and HIPAA authorization signed by multiple parties; instead, it is an agreement established between patient and provider. Health care providers are able to access patient information and communicate freely with patients regarding their care. When a provider adopts text messaging as part of their routine care, it has the potential to facilitate enrollment, enhance standardized patient engagement, and create sustainable partnerships that support the technology adoption. In the context of routine care, SMS technology interventions are provider-driven, and do not call upon human subjects regulations as research is not yet occurring (*Figure 2*).

To implement best text messaging practices, healthcare organizations generally will need to define contractual business relationships with third-party text message service providers through a BAA. This arrangement is similar to outsourcing agreements that clinical entities establish with other organizations such as billing, payroll, or transcription. It is necessary to establish connectivity and data transfer strategies between the SMS platform and the clinical practice management or EHR system. BAAs allow SMS service providers to act as agents for supporting the technology requirements to carry out SMS communication and outreach desired by the clinical entity.

Defining parameters of PHI transfer when using SMS for research

Establishing clinical text messaging data governance rules that define the flow of PHI, articulate the relationship of the research entity to patient care, delineate systems security requirements, and clarify responsibilities of partnering brokers of the data is a challenging and important initial step. Providers must decide the SMS use case most useful to deploy (e.g., reminders, updates, and education) and identify appropriate patient cohorts. Depending on the intended summary message content and the original data sources used to select patient cohorts, patient information required to send messages may combine cell phone numbers with other personal data. Patient cohort data sets may require a PHI sanitizing process before being transmitted to the SMS service provider through a secure route, which may be automated, manual, or a combination of the two.

The BAA serves to stipulate that all data transfers and all agents handling PHI are obligated to adhere to HIPAA regulations (*Figure 3*). The flow of information needs to be mapped and tested to establish points of review and ownership, and to define what roles and processes can be systematized. Presence of PHI content contained within the text messages must be analyzed to ensure compliance with HIPAA and BAA documentation. Identifying whether SMS information content is identifiable can be challenging. For example, is a text message reminder to get a lipid lab test identifiable? If so, is there any risk to the patient? There is published guidance on how to best construct a message that falls into accordance of HIPAA.[8]

Commercial SMS providers employ several methods of managing text message initiation, delivery, and receipt confirmation. A BAA defines that the third parties delivering text messages act as an agent of the covered clinical entity. As agents providing a service to clinical entities, the SMS providers are responsible for protecting PHI throughout the end-to-end message transmission process, including maintaining historic record logs of messages. If clinically driven messaging involves a response from the patient, the text message provider is responsible for the information once it is received and until it is transferred to the clinical entity. At the point that the messages are transferred to the clinical entity, the responsibility is passed to the clinical entity, which should have processes to ensure that unexpected content is captured and reviewed for potential clinical follow-up.

Establishing research oversight of SMS data

A clinical entity may adopt text messaging, but does not support research until the research entity receives data. A clinical entity can establish a relationship with a text message management entity (SMS provider), deploy the text message system, and record data from the text messaging activity without Human Subjects approval (*Figure 4*).

Once research begins, the IRB approval for the research uses of PHI details the management of PHI, as well as the level of interaction with the patient (e.g., patient interviews). The HIPAA waiver and Waiver of Informed Consent exist as part of the IRB approval and define the scope of data for research uses. To date, most research entities analyze text message data *post hoc*,[3–6,8–11]

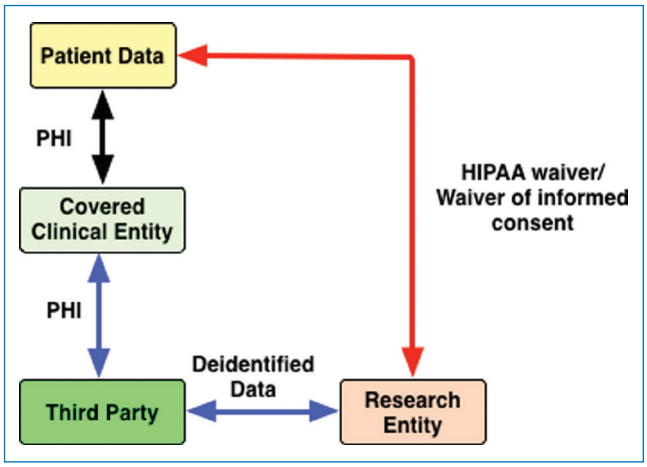

Figure 4. Establishing research oversight.

after being carried out by the clinical entity and third party, though there is likely be more real-time work in the future. Depending on the structure of the project, members of the third-party entity or the clinical entity may be included as collaborators on the IRB application.

Discussion

In order to develop research environments that use data captured from patients and which are then shared across clinical and third-party technical infrastructures, there need to be well-defined protocols and high-quality communication between all entities involved. Utilizing the tools discussed in this paper along with clearly defined roles and relationships streamlines the opportunity to develop strategic planning and adoption of SMS within a new environment. It is critical to ensure that all entities understand the legal and ethical obligations of stewardship that accompany the tools used to protect patient interests and personal health information. Each entity has a different interest and, therefore, maintaining clear roles and a shared understanding of these obligations is essential to the integrity of the project. As the potential implementations for text messaging in healthcare settings is broad, including research motivations into these types of projects could lead to a better understanding of the most effective use of text messaging while assisting the clinical entity in meeting their goals.

The case study that led to this paper established the range of tools and stages described previously, and supported a successful clinical trial (data published elsewhere). The technical infrastructure design defined the capabilities and alignment of the governance tools, and revealed several; challenges in attempting to "automate" such environments. Considerable attention was devoted to a study and infrastructure design that involved identifying, consenting, and creating targeted messages and expected result values. Despite this, since personally owned devices with SMS capabilities are broadly available technologies that are often fully incorporated into patients daily lives, we found that that it was difficult to plan for all eventualities in how messages were received or responded to. This is a significant research area to be explored—both in understanding different styles to better communicate with patients, as well as improved technologies to parse and manage complex text responses. We learned that establishing appropriate governance within the clinical system required monitoring all responses that were not formatted as expected, and supporting the rare case that included an actionable patient response. We expect that technologies for parsing and better classifying responses will aid this in the future, but it will remain the responsibility of the clinical entity under HIPAA regulations to ensure that the mission to the patients is a priority over the potential research uses.

Given the complexity of the agreements and these evolving social relationships to the technology and health system, deciding explicitly who is maintaining privacy and security requirements and managing data sets at each stage of the project is critical. Depending on the capacity of the three entities (i.e., clinical, third party, and research) a project coordinator who can access all levels of data may best fit this role. If the project coordinator is a member of the research entity, the IRB approval will need to allow the research entity access to a more identifiable data set. All members of the research entity need to be well versed in HIPAA and the definition of identifiable PHI.

Summary

As patient sophistication and adoption of mobile technologies develops, there will be an increase in opportunities for personally controlled technologies and information to interact with clinical systems. There has already been a rise in clinical practices utilizing text or e-mail systems for appointment reminders, though presently this is largely limited to identifiable or specialized information (e.g., overdue lab work) and to largely unidirectional modes. Conducting research utilizing these services crosses clinical and patients' personal domains, and requires navigation of two formal regulatory environments: HIPAA and protection of human subjects. This preliminary review of tools, roles, and implementations strategies may be helpful for defining appropriate governance for research use of clinical text messaging that is distinct from requirements in clinical environments alone.

Acknowledgments

This work was supported by ONC grant # 90HT0047/01, the Northwest EHR Collaborative, Anaconda, Montana and the St. Peter's Medical Group, Helena, Montana. We gratefully acknowledge Mandy Morneault for regulatory policy review.

References

1. Smith A. Americans and Text Messaging, Pew Internet. *Pew Research Center*, 2011 (Accessed October 6, 2013).

2. Lee S, Xin X, Lee WP, Sim EJ, Tan B, Bien MPG, Lau AS, Thumboo J. The feasibility of using SMS as a health survey tool: an exploratory study in patients with rheumatoid arthritis. *Int J Med Inform.* 2013; 14: 1–8.

3. Whitford HM, Donnan PT, Symon AG, Kellett G, Monteith-Hodge E, Rauchhaus P, Wyatt JC. Evaluating the reliability, validity, acceptability, and practicality of SMS text messaging as a tool to collect research data: results from the Feeding Your Baby project. *J Am Med Inform Assoc.* 2012; 19(5): 744–749.

4. Ríos-Bedoya CF, Hay C. Feasibility of using text messaging for unhealthy behaviors screening in a clinical setting: a case study on adolescent hazardous alcohol use. *J Am Med Inform Assoc.* 2013; 20(2): 373–376.

5. Menacho LA. Short text messages to motivate HIV testing among men who have sex with men: a qualitative study in Lima, Peru. *Open AIDS J.* 2013; 7(1): 1–6.

6. Vervloet M, Linn AJ, vanWeert JCM, deBakker DH, Bouvy ML, vanDijk L. The effectiveness of interventions using electronic reminders to improve adherence to chronic medication: a systematic review of the literature. *J Am Med Inform Assoc.* 2012; 19(5): 696–704.

7. Stenner SP, Johnson KB, Denny JC. PASTE: patient-centered SMS text tagging in a medication management system. *J Am Med Inform Assoc.* 2012; 19(3): 368–374.

8. Nundy S, Razi RR, Dick JJ, Smith B, Mayo A, O'Connor A, Meltzer DO. A text messaging intervention to improve heart failure self-management after hospital discharge in a largely African-American population: before-after study. *J Med Internet Res.* 2013; 15(3): e53.

9. Pop-Eleches C, Thirumurthy H, Habyarimana JP, Zivin JG, Goldstein MP, deWalque D, MacKeen L, Haberer J, Kimaiyo S, Ngare D, et al. Mobile phone technologies improve adherence to antiretroviral treatment in a resource-limited setting: a randomized controlled trial of text message reminders. *AIDS*. 2011; 25: 825–834.

10. Bennett DA, Emberson JR. Text messaging in smoking cessation: the txt2stop trial. *Lancet*. 2011; 378(9785): 6–7.

11. Karaz, HN, Eiden A, Bogan S. Text messaging to communicate with public health audiences: how the HIPAA Security Rule affects practice. *Am J Public Health*. 2013; 103(4): 617–622.

12. Anderson N, Edwards K. Building a chain of trust. In: *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies – GTIP '10*. New York, USA: ACM Press; 2010: 15–20.

13. Bishop M, Gates P, Yellowlees P, Silberman G. Facebook goes to the doctor. *Proceedings of the 2011 Workshop on the Governance of Technology Information and Policies.* December 5–9, 2011, Orlando, FL, PP. 13–20.

14. Miller F, Giacomini M, Ahern C, Robert J, deLaat S. When research seems like clinical care: a qualitative study of the communication of individual cancer genetic research results. *BMC Med Ethics.* 2008; 9: 4.

15. Brody H, Miller FG. The Research-Clinical Practice Distinction, Learning Health Systems and Relationships. *Hastings Cent Rep.* 2013; 43(5): 41–47.

16. Harris PA, Taylor R, Thielke R, Payne J, Gonzalez N, Conde JG. Research electronic data capture (REDCap)—a metadata-driven methodology and workflow process for providing translational research informatics support. *J Biomed Inform.* Apr 2009; 42(2): 377–378.