Text Messaging to Communicate With Public Health Audiences: How the HIPAA Security Rule Affects Practice

Hilary N. Karasz, PhD, Amy Eiden, JD, and Sharon Bogan, MPH

Text messaging is a powerful communication tool for public health purposes, particularly because of the potential to customize messages to meet individuals' needs. However, using text messaging to send personal health information requires analysis of laws addressing the protection of electronic health information.

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule is written with flexibility to account for changing technologies. In practice, however, the rule leads to uncertainty about how to make text messaging policy decisions.

Text messaging to send health information can be implemented in a public health setting through 2 possible approaches: restructuring text messages to remove personal health information and retaining limited personal health information in the message but conducting a risk analysis and satisfying other requirements to meet the HIPAA Security Rule. (*Am J Public Health*. Published online ahead of print February 14, 2013: e1–e7. doi:10.2105/AJPH.2012.300999)

AS PUBLIC HEALTH PROFESS- sionals, one of our key roles is to provide credible, timely health information to the public. The explosion of new information channels over the past decade means that there are more opportunities to reach audiences, whether through traditional methods such as the television news or newspapers or through newer technologies such as the Internet and social media. Text messaging is another important communication channel that public health departments should consider, particularly for communities with less access to costlier technologies such as smartphones.

Text messages are 140- to 160-character messages sent from cell phones or computers over wireless carrier networks to end users' cell phones. Text messaging (also known as Short Message Service, or SMS) is an increasingly prevalent form of communication among all age groups.[1] In 2011, 73% of adults with cell phones reported using texting, up from 65% in 2009.[1] According to the cell phone industry, more than 2 trillion text messages were sent in the United States in 2011.[2]

In 2008, recognizing the potential power of texting to reach a variety of audiences to improve health, the communications team at Public Health—Seattle & King County began a 5-year research-in-practice project to explore local audience needs and interests regarding text messaging from the department, along with the legal, financial, and logistical implications of adopting text messaging in a local public health setting. In the course of the research, multiple health applications were identified for text messaging, including public health emergency preparedness,[3] smoking cessation programs,[4,5] physical activity promotion,[6,7] medicine adherence,[8] and other health-related protection and promotion behaviors.[9,10] Text messaging has also shown promise for vaccine uptake[11] and appointment reminders.[12–14]

A key theme of the texting for health literature is that text messages are valued when they are perceived as highly relevant, customized, and simple.[15–18] In the context of provider–patient communication, a customized text message might include an individual's health information, in which case senders must consider implications of the Security Rule promulgated under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Pub L No. 104-191).[19]

Here we describe our analysis of the impact of the HIPAA Security Rule on sending text messages containing individuals' health information. Our team of subject matter experts took 2 approaches to sending such messages. In the first approach, individuals' health information was stripped from text messages to avoid triggering the Security Rule in the first place. The second approach, which addressed the issue of complying with the Security Rule when incorporating individual health information into messages, included conducting an in-depth analysis of risks inherent in texting personal health information.

Our examples shed light on the complexities of implementing the federal Security Rule within a local health department context. Individual states also may have relevant laws that health departments will want to review. During our project, we reviewed Washington State laws and concluded that our risk analysis under the federal Security Rule provided an appropriate framework for Washington's requirements. We offer recommendations for future policy work and suggestions that will make it more feasible for local health departments to use text messaging to reach their audiences.

HOW HIPAA APPLIES TO TEXT MESSAGING

HIPAA is best known for the Privacy Rule,[20] which applies to individual health care information in all forms, whether oral, paper, or electronic. But HIPAA also includes the Security Rule, which applies when health care information is electronic. Whereas the Privacy Rule defines the circumstances in which individual health care information may be disclosed, the Security Rule defines the requirements for making such disclosures in electronic form.

HIPAA Statutory and Regulatory Framework

Pursuant to congressional authorization, the US Department of Health and Human Services (HHS) issued the Privacy Rule and Security Rule to implement certain

provisions of HIPAA.[21,22] HHS issued the rules through a formal rulemaking process that included publication of proposed rules and a period of public comment before publication of the final rules.[21,22] Congress provided for the rules to be enforced.[23]

HHS has authority to enforce the rules, including investigating complaints and conducting compliance reviews.[24] The HHS Web site contains information about complaints, investigations, and breaches but not in a format that allowed us to determine whether there have been enforcement actions or breaches involving text messaging.[25]

Covered Entities and Their Business Associates

Not all health departments in possession of health care information are covered by the Privacy Rule and Security Rule. The rules apply only to "covered entities" and their "business associates." A covered entity is a health care provider who electronically submits health care information in connection with certain transactions, a health plan, or a health care clearinghouse.[26] If an organization conducts functions that make it a covered entity but other functions that do not, it may elect to be a "hybrid entity" and place only its covered functions under the rules.[27]

A business associate is a person or entity that performs certain functions or activities involving the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.[26] Our health department is a covered entity, so we are subject to the Privacy Rule and Security Rule.

Protected Information and the Privacy Rule

Under the Privacy Rule, individually identifiable information held by a covered entity about an individual's health care is confidential. The Privacy Rule broadly defines confidential information as information that

> [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.[26]

In most contexts, this information is termed protected health information (PHI). The Privacy Rule applies to all PHI, whether electronic, paper, or oral. Under the Privacy Rule, an individual may authorize PHI to be disclosed. In addition, there are a variety of circumstances in which PHI may be disclosed without an individual's authorization, including in certain circumstances to protect public health.

The Privacy Rule came into play as we piloted our second-dose influenza text reminder service. Public Health—Seattle & King County conducts influenza vaccine clinics in which we provide free influenza vaccine to low-income or uninsured county residents. These clinics serve the dual purpose of increasing access to influenza vaccine and providing an opportunity to test Public Health—Seattle & King County's capacity to distribute vaccinations or other medicine rapidly to large numbers of people in the event of an emergency.

In November 2010, researchers conducted the daylong pilot project at 2 mass vaccination clinic settings in King County. The 1225 attendees included an ethnically and racially diverse group of adults and children. The department advertised the clinic through the media, community-based organizations, and flyers distributed in the community. Although most individuals require only a single dose of seasonal influenza vaccine, some children require a second dose 30 days after the first to become fully protected.

To help remind parents of children who required a second dose, we wanted to send them text messages 30 days after the flu clinic that clearly stated that it was time for their children to obtain the flu vaccine booster. Because we did not plan to hold a follow-up clinic, we needed to direct these parents to community resources. In this case, we referred parents to pharmacies and community clinics. Our draft message was as follows: "It's time for [child name]'s second dose of seasonal flu vaccine. Visit a pharmacy or clinic today for the booster to keep your child protected."

It is typically permissible to disclose information about a child's health care to his or her parents. When a patient is a minor, a covered entity usually may share PHI with parents or other legal representatives.[28] The second-dose project presented this scenario: we wanted to disclose PHI to the child's parent or guardian, which was entirely permissible under the Privacy Rule. However, the information needed to be delivered in a secure manner per the Security Rule.

Electronic Information and the Security Rule

The Security Rule is different than the Privacy Rule. Even if a disclosure is permissible under the Privacy Rule—for example, when authorized by a patient or when necessary to protect public health—any disclosure that is electronic must be made in a manner that complies with the Security Rule.[29] Electronic PHI is PHI that is "transmitted by electronic media" or "maintained in electronic media."[26] Electronic media include "electronic storage media" and "transmission media used to exchange information already in electronic storage media."[26]

We are not aware of case law or HHS guidance addressing whether text messages are subject to the Security Rule. In consultation with subject matter experts in our information technology, risk management, and legal departments, we concluded that a text message arguably is within the definition of electronic media because it involves data that exist in electronic form prior to transmission. In this way, transmission via a text message is different than transmission via telephone or facsimile. Because of this conclusion, we decided that, until there is authoritative guidance, we should proceed cautiously and assume that the Security Rule applies to text messages containing PHI. Consequently, to avoid triggering the Security Rule at all, we initially decided to use the approach of omitting PHI from our second-dose text messages.

APPROACH 1: EXCLUDING PROTECTED HEALTH INFORMATION

To send influenza vaccine reminders to parents, we wanted a simple, direct text message that all parents would understand easily and that would not trigger the Security Rule. Research shows that text messages are best when they are simple and customized.[16–18] In line with the principle that clear communication is preferable—particularly in the case of health issues, given that health literacy is a significant issue[30]—our original

text message draft was a simple message that would trigger parents' memories of having signed up to receive the text message, describe who should receive the second dose, and provide a call to action. Again, our original proposed message was "It's time for [child name]'s second dose of seasonal flu vaccine. Visit a pharmacy or clinic today for the booster to keep your child protected."

To help evaluate whether this message contained PHI, we assessed whether a third party could infer the child's identity from the message. We used this approach not because it is a legal standard but as a framework to help us evaluate whether a message would have the effect of disclosing PHI. For example, if a person other than the intended recipient intercepted the original message, that person would have the name of the child and a reference to a second dose of flu vaccine. This would mean that the unintended recipient could infer that the child received a first dose of flu vaccine, which is PHI.

Rewriting the Message

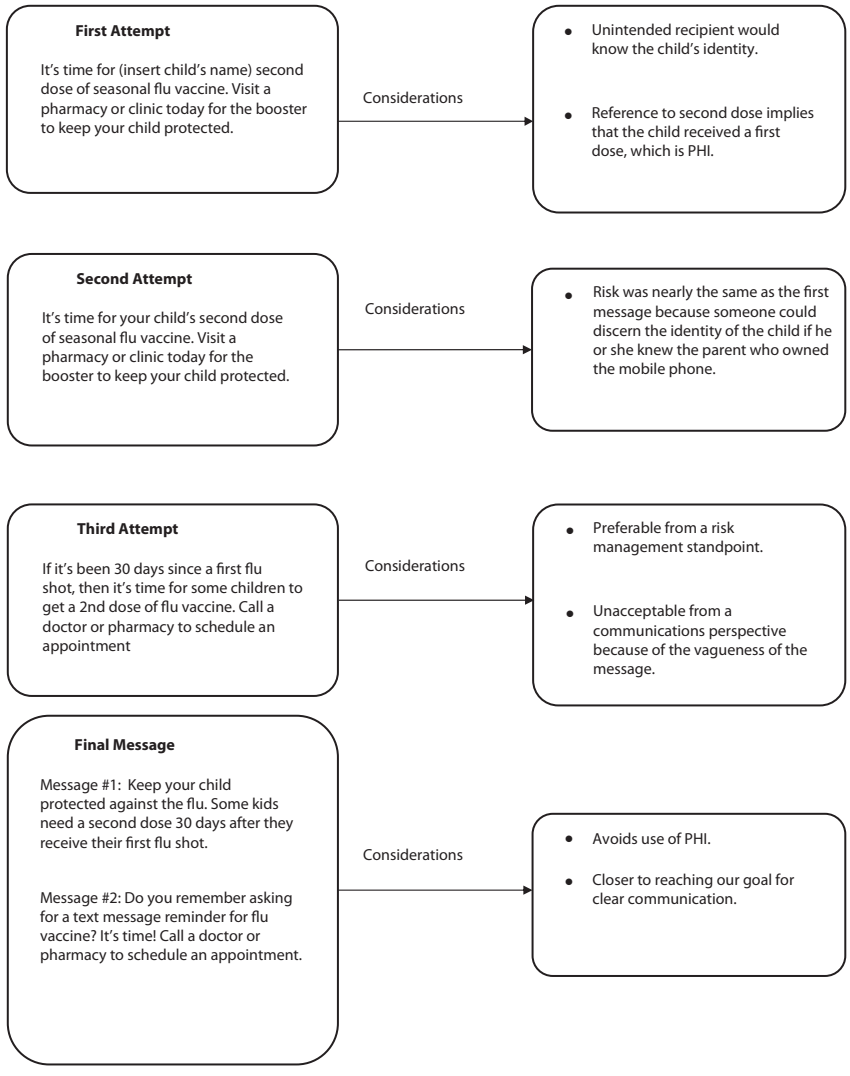
We removed the name, replacing it with a generic "your child," but felt that the risk was nearly the same because a third party who saw the text message would be able to discern the identity of the child if he or she knew the parent who owned the mobile phone. We then crafted several different messages and assessed each message for clarity on one hand and risk of disclosing PHI on the other. The following is an example: "If it's been 30 days since a first flu shot, then it's time for some children to get a second dose of flu vaccine. Call a doctor or pharmacy to schedule an appointment."

Although this message mentioned flu shots and second doses, the message was vague, and its ambiguity potentially undermined our health department's credibility because the message conveyed the impression that we did not know whether or when the parent's child received the vaccine.

Final Message

After writing and analyzing several similar messages, we settled on a 2-message approach that all members of our team felt was reasonably clear but did not include PHI. The first message was "Keep your child protected against the flu. Some kids need a second dose 30 days after they receive their first flu shot." The second message was "Do you remember asking for a text message reminder for flu vaccine? It's time! Call a doctor or pharmacy to schedule an appointment."

The first message was intended to trigger thinking about flu vaccine and a second dose. The second message, sent moments after the first, personalized the message without referring specifically to the health care the person received. The question "Do you remember asking for a text message?" instead of "Do you remember your child getting a flu shot?" avoids the mention of health care. This example illustrates how stripping PHI from health messages can reduce the simplicity and clarity of the intended message. Figure 1 summarizes the risk and



Note. PHI = protected health information.

FIGURE 1—Risk and communication considerations in crafting text messages to send health information.

communication considerations for each message.

Eighty-four percent of parents whose children needed a second dose of vaccine opted in to the texting program. It was not an aim of this project to evaluate health outcomes associated with the text message reminder; rather, the aim was to assess the feasibility of implementing such a system within a local health department. Further studies need to be designed to measure the impact of text reminders on health outcomes.

APPROACH 2: COMPLYING WITH THE SECURITY RULE

In the second-dose example, we omitted PHI from the message. Under certain circumstances, however, public health programs may want to send PHI or may not be able to avoid including PHI in the message. When this is the case, there is a need to address the Security Rule standards. To analyze the security standards within the context of sending PHI via text messaging, we convened a team of information technology security and risk management experts to conduct a risk analysis and assessment of the Security Rule.

Security Rule

The Security Rule requires a covered entity to implement 3 types of safeguards for electronic PHI: administrative (policies and procedures to protect PHI),[31] physical (typically physical measures to protect electronic information and its equipment),[32] and technical (such as specific technology employed to protect PHI).[33] For each type of safeguard, the Security Rule sets forth standards. The rule also sets forth standards for organizational requirements and for policies and procedures and documentation requirements (see the box on the next page).

A covered entity must comply with each of the standards in the Security Rule. Many of the standards include specific measures, termed "implementation specifications," that are relevant to meeting the standard. Some measures are termed required and must be implemented. By contrast, some measures are termed addressable. When a measure is addressable, then a covered entity must evaluate whether that measure is "reasonable and appropriate." If the covered entity determines that the measure is not reasonable and appropriate, then the covered entity must evaluate whether an alternative measure is necessary to comply with the standard.[34] Under the Security Rule, the covered entity would need to implement alternative measures, if necessary, before transmitting PHI electronically such as via text messaging.

Risk Analysis

Two key implementation specifications in the Security Rule under the administrative safeguards are risk analysis and risk management. Specifically, a covered entity must

> [c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.[35]

Our risk analysis examined effects on our security environment specifically if we sent text messages containing PHI.

We worked with independent cybersecurity consultants and referred to HHS Security Rule guidelines[25] to assess potential risks and vulnerabilities of using text messaging to send PHI along the entire pathway from cell phone number collection and storage to transmission to cell phone system vendors, aggregators, carriers, and finally to the end user. We explored the likelihood of interception along the pathway and discussed the potential impacts on the individual and our organization if an impermissible disclosure occurred. We then identified multiple mitigation strategies to protect against the threat of impermissible disclosure and documented the process.

Health Insurance Portability and Accountability Act Security Rule Standards

Administrative safeguards
Security management process: 164.308(a)(1)
Assigned security responsibility: 164.308(a)(2)
Workforce security: 164.308(a)(3)
Information access management: 164.308(a)(4)
Security awareness and training: 164.308(a)(5)
Security incident procedures: 164.308(a)(6)
Contingency plan: 164.308(a)(7)
Evaluation: 164.307(a)(8)
Business associate contracts and other arrangements: 164.307(b)(1)

Physical safeguards
Facility access controls: 164.310(a)(1)
Workstation use: 164.310(b)
Workstation security: 16.310(c)
Device and media controls: 164.310(d)(1)

Technical safeguards
Access control: 164.312(a)(1)
Audit controls: 164.312(b)
Integrity: 164.312(c)(1)
Person or entity authentication: 164.312(d)
Transmission security: 164.312(e)(1)

Organizational requirements
Business associate contracts or other arrangements: 164.314(a)(1)
Requirements for group health plans: 164.314(b)(1)

Policies and procedures and documentation requirements
Policies and procedures: 164.316(a)
Documentation: 164.316(b)(1)

Key Conclusions From Our Risk Analysis

Along the continuum from provider to telecommunications system to end user, our analysis revealed potential vulnerabilities and risks that PHI could fall into the wrong hands every step of the way. Some risks are wholly controlled by the covered entity, and health departments can put alternative measures into place to minimize those risks. For example, employees can be (or already are) trained in methods to ensure that PHI is protected on department computers, and this type of training could be expanded to include text messaging.

There are also risks over which a health department has limited control. For example, texting vendors and aggregators, who provide the software that moves messages from databases to the wireless telephone carriers, may have stronger or weaker security controls built into their text message platforms. Therefore, covered entities could choose to contract only with vendors with adequate security measures in place. In addition, health departments may choose to store all PHI in their own databases on their own computer servers to minimize access by unauthorized individuals.

Finally, there are risks in sending text messages over which the health department has no control. Once the text message has left the realm of the vendor or aggregator, it is under the domain of the wireless telephone carriers with which the health department would have no contractual agreement. In addition, there are risks associated with the end user. For example, the end user may not password protect his or her mobile phone, which would leave text messages vulnerable to access by an unauthorized individual.

Transmission Security Standard

Along with conducting a risk analysis, which is only one aspect of the Security Rule, we evaluated the complete list of standards within the Security Rule to determine which standards specifically applied to text messaging. As mentioned, many of the standards were already being met through current policies and procedures. For example, we have policies and procedures in place that address standards such as workforce security, facility access controls, and business associate contracts.

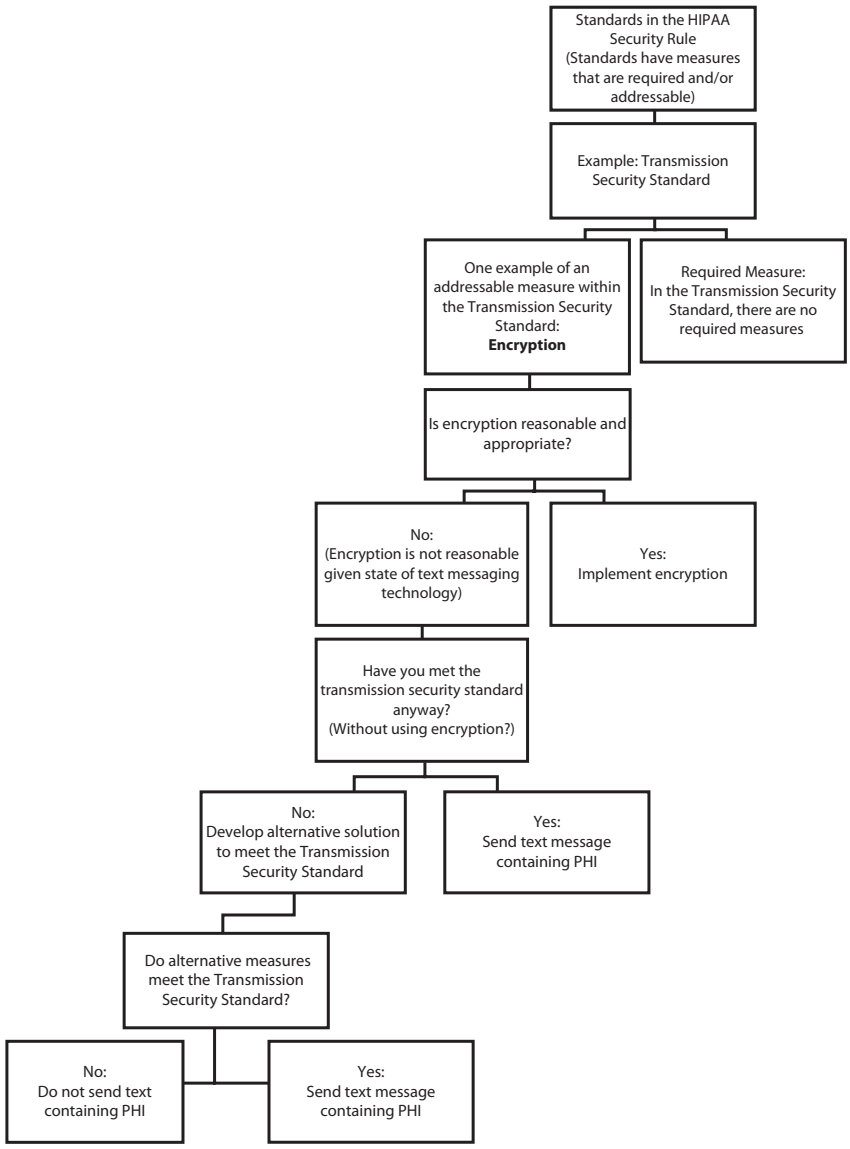
The key standard that warranted additional analysis was the transmission security standard. This standard requires a covered entity to

> implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.[36]

An addressable implementation specification under this standard is encryption.

Encryption

Although encryption is a feasible option when sending PHI via e-mail, it is not a realistic option for text messaging given the current state of technology. That being the case, encryption is not "reasonable and appropriate." Our next task was to evaluate whether an alternative measure was needed to meet the transmission security standard. Our team agreed that we would not meet the transmission security standard without addressing the encryption measure. Therefore, we would need to



Note. HIPAA = Health Insurance Portability and Accountability Act.

FIGURE 2—Process of addressing Security Rule standards for a covered entity that wants to send protected health information (PHI) via text messaging.

implement alternative measures such as the mitigation strategies that our risk analysis revealed. Examples of potential mitigation strategies include limiting who within the workforce sends text messages, explaining risks to the end user and recommending that end users password protect their phones, and requiring adequate security certifications from text messaging vendors. Figure 2 describes the process of addressing Security Rules with encryption as an example.

CONCLUSIONS

Even after implementation of steps to mitigate risk, no communication method is 100% secure, and text messaging is no different. Ultimately, the decision to send text messages with PHI is a policy decision in which the risks and the benefits are weighed by decision-makers. The Security Rule allows for sending PHI via text message if all of the standards are met, but the risk of failing to meet the standards is ultimately borne by the covered entity. A covered entity must exercise discretion in deciding whether it has identified reasonable and appropriate measures to sufficiently meet the transmission security standard.

Despite inherent risks, public health departments have a responsibility to use communication channels that will reach their communities effectively, particularly in instances in which there is a benefit to the public's health. Texting is a powerful communication channel, in part because it can be customized. If all personally identifying information is removed, this may eliminate the greatest strength of text messaging.

Currently, there is a lack of clear and specific guidance on how health entities can use text messaging that contains PHI. Our department is large with substantial resources, but even so, we were hard pressed to analyze all of the risks associated with sending PHI via text message and identify all available mitigation solutions.

It would be helpful if the HHS Office of Civil Rights or another interested federal agency issued guidance outlining which alternative measures to encryption and mitigation strategies would enable health departments to meet the transmission security standard. For example, would mitigation strategies focused on the end user enable health departments to comply with HIPAA? Such mitigation might include having recipients sign a waiver indicating that they understand the risks associated with receiving a text message.

The relevant federal entity could issue guidance on mitigation strategies at the vendor and carrier levels as well by conducting and making available assessments of transmission risks associated with mobile carriers and telecommunications systems. Such risk assessments could be conducted on a yearly basis to aid covered entities in selecting text messaging vendors. Finally, health departments could be provided with suggestions to reduce risks at the health department systems level such as recommendations for double entry of cell phone numbers when clients opt in to a program.

In summary, we recommend that the federal government take steps now to clarify how health departments can reasonably use text messaging to send protected health information. Text messaging is a technology that reaches the vast majority of US adults and has the potential to be a powerful tool to improve health and well-being. Until guidance is available and regulations are better defined, many health departments will lose the opportunity to use the technology in the most effective way. ■

About the Authors

Hilary N. Karasz and Sharon Bogan are with Public Health—Seattle & King County, Seattle, WA. Amy Eiden is with the King County Prosecuting Attorney's Office, Seattle.

Correspondence should be sent to Hilary N. Karasz, PhD, Public Health—Seattle & King County, 401 5th Ave, Suite 1300, Seattle, WA 98104 (e-mail: hilary.karasz@kingcounty.gov). Reprints can be ordered at http://www.ajph.org by clicking the "Reprints" link.

This article was accepted July 20, 2012.

Contributors

H. N. Karasz originated the study and devised the project strategy. A. Eiden led the legal interpretation. S. Bogan managed project implementation. All of the authors conceptualized ideas, analyzed legal and communication frameworks, and wrote and reviewed drafts of the article.

Acknowledgments

This work was partially supported by the Centers for Disease Control and Prevention (grant 5P01TP000297).

Note. This work is the responsibility of the authors and does not necessarily represent the official views of the Centers for Disease Control and Prevention.

Human Participant Protection

Our research activities were approved by the institutional review board at the University of Washington. The second-dose pilot was considered by the board to be a quality improvement activity and did not require human participant approval.

References

1. Smith A. Americans and their cell phones. Available at: http://www.pewinternet.org/Reports/2011/Cell-Phones.aspx. Accessed December 2, 2012.

2. CTIA. Quick facts. Available at: http://www.ctia.org/advocacy/research/index.cfm/AID/10323. Accessed December 4, 2012.

3. Merchant M, Elmer S, Lurie N. Integrating social media into emergency preparedness efforts. *N Engl J Med.* 2011;365(4):289–291.

4. Haug S, Meyer C, Schorr G, Bauer S, John U. Continuous individual support of smoking cessation using text messaging: a pilot experimental study. *Nicotine Tob Res.* 2009;11(8):915–923.

5. Free C, Knight R, Robertson S, et al. Smoking cessation support delivered via mobile phone text messaging (txt2stop): a single-blind, randomised trial. *Lancet.* 2011;378(9785):49–55.

6. Prestwich A, Perugini M, Hurling R. Can implementation intentions and text messages promote brisk walking? A randomized trial. *Health Psychol.* 2010;29 (1):40–49.

7. Bauer S, de Niet J, Timman R, Kordy H. Enhancement of care through self-monitoring and tailored feedback via text messaging and their use in the treatment of childhood overweight. *Patient Educ Couns.* 2010;79(3):315–319.

8. Lester RT, Ritvo P, Mills EJ, et al. Effects of a mobile phone short message service on antiretroviral treatment adherence in Kenya (WelTel Kenya1): a randomised trial. *Lancet.* 2010;376 (9755):1838–1845.

9. Armstrong AW, Watson AJ, Makredes M, Frangos JE, Kimball AB, Kvedar JC. Text-message reminders to improve sunscreen use: a randomized, controlled trial using electronic monitoring. *Arch Dermatol.* 2009;145 (11):1230–1236.

10. Fjeldsoe BS, Marshall AL, Miller YD. Behavior change interventions delivered by mobile telephone short-message service. *Am J Prev Med.* 2009;36(2):165–173.

11. Kharbanda EO, Stockwell MS, Fox HW, Andres R, Lara M, Rickert VI. Text message reminders to promote human papillomavirus. *Vaccine.* 2011;29 (14):2537–2541.

12. Guy R, Hocking J, Wand H, Stott S, Ali H, Kaldor J. How effective are short message service reminders at increasing clinic attendance? A meta-analysis and systematic review. *Health Serv Res.* 2012;47(2):614–632.

13. Leong KC, Chen WS, Leong KW, et al. The use of text messaging to improve attendance in primary care: a randomized controlled trial. *Fam Pract.* 2006;23(6):699–705.

14. Downer SR, Meara JG, Da Costa AC, Sethuraman K. SMS text messaging improves outpatient attendance. *Aust Health Rev.* 2006;30(3):389–396.

15. Karasz H, Li-Vollmer M, Bogan S, Offenbecher W. Targeting young adult texters for public health emergency messages: a Q-study of uses and gratifications. In: Ahmed R, Bates BR, eds. *Health Communication and Mass Media: Applying Research to Public Health Policy and Practice*. Surrey, England: Gower Publishing. In press.

16. Smith M, Harris L. Text "ahhhhh" for me please. In: Fogg BJ, Adler R, eds. *Texting 4 Health: A Simple, Powerful Way to Improve Lives*. Palo Alto, CA: Stanford University; 2009:49–57.

17. Patrick K, Raab F, Adams M, Dillon L. mDiet: a personalized approach to weight management using text messaging. In: Fogg BJ, Adler R, eds. *Texting 4 Health: A Simple, Powerful Way to Improve Lives*. Palo Alto, CA: Stanford University; 2009:35–49.

18. Centers for Disease Control and Prevention. Text message requirements and best practices. Available at: http://www.cdc.gov/SocialMedia/Tools/guidelines/pdf/textmessages.pdf. Accessed December 2, 2012.

19. 45 CFR 160, 164, subparts A and C (2011).

20. 45 CFR 160, 164, subparts A and E (2011).

21. US Dept of Health and Human Services. Summary of the HIPAA Privacy Rule. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html. Accessed December 2, 2012.

22. US Dept of Health and Human Services. Summary of the HIPAA Security Rule. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html. Accessed December 2, 2012.

23. 42 USC 1320d-5 (2011).

24. 45 CFR 160, subparts C–E (2011).

25. US Dept of Health and Human Services, Office for Civil Rights. Health information privacy. Available at: http://www.hhs.gov/ocr/privacy/index.html. Accessed December 2, 2012.

26. 45 CFR 160.103 (2011).

27. 45 CFR 164.103 (2011).

28. 45 CFR 164.502(g) (2011).

29. 45 CFR 164.302 (2011).

30. Kripalani S, Weiss BD. Teaching about health literacy and clear communication. *J Gen Intern Med*. 2006;21(8):888–890.

31. 45 CFR 164.3048 (2011).

32. 45 CFR 164.310 (2011).

33. 45 CFR 164.312 (2011).

34. 45 CFR 164.306(d) (2011).

35. 45 CFR 164.308(a)(1)(ii)(A) (2011).

36. 45 CFR 164.312(e) (2011).