Understanding the Role of Trust in the Protection of Privacy

By Kenneth G. Hartman, CISSP, CPHIMS, GSEC

Introduction

Not everyone recognizes how the concepts of privacy and security differ, and how they relate. In fact, the term "privacy and security" is tossed about as if the two concepts were a single hyphenated noun – "privacy-and-security." [1] This paper is an attempt to convey an overarching way to think about the relationship and differences between these important topics. For additional information refer to the HIMSS Privacy & Security Toolkit, an expanding storehouse of valuable information that delves into these topics in depth.

Patricia, a middle-aged woman was rear-ended at a red light. Her health insurance company turned her down based on the psychologist's notes contained in her medical record from five years ago, when she had obtained therapy after the sudden death of her fiancé. The stunned victim insisted that her insurer had misinterpreted the psychotherapy notes. To make matters worse, her therapist had assured her the sessions would remain confidential. [2] A groundswell of horror stories such as this, including many large scale breaches involving the disclosure of thousands of records led to the creation of the HIPAA Privacy Rule [4] in the United States, following an international trend in strengthened privacy rules.

Since the HIPAA Privacy Rule became effective in April of 2003, privacy regulations have continued to evolve. On February 17, 2009, President Obama signed into law the *American Recovery and Reinvestment Act (ARRA)*. This legislation aims to stimulate the economy through investments in infrastructure, unemployment benefits, transportation, education, and healthcare, providing nearly $20 billion to aid in the development of a robust IT infrastructure for healthcare and to assist providers and other entities in adopting and using health IT. In addition, the *Health Information Technology for Economic and Clinical Health Act (HITECH)* provisions of ARRA in Title XIII (Subtitle D) include important changes in Privacy, resulting additional Privacy regulation and changes to HIPAA. [5]

The general public has also become much more aware of privacy breaches, thanks in part to the *HITECH Breach Notification Interim Final Rule* that requires public notification for breaches impacting more than 500 individuals. [6]

The Importance of Understanding Privacy

Privacy is much more than compliance with HITECH and the HIPAA Privacy Rule. The root issues are also deeper than the latest privacy breach broadcasted by the public media. Privacy matters to the people that healthcare serves, therefore as Health IT professionals we can all benefit from an enhanced understanding of privacy. A more complete understanding of the various aspects of privacy will allow all of us to be more empathetic to the various privacy expectations of our patients and to be more motivated to secure the protected health information entrusted to us. Lastly, an enhanced understanding of privacy by patients, providers, and Health IT

Professionals will improve health information exchange because the exchange of personal and private information can only work in a framework of trust.

A Definition of Privacy and Security

At a basic level, "privacy" is *what* is to be protected and "security" is *how* it is protected. Dixie Baker, PhD has defined privacy in *Health Informatics: A Systems Perspective* as follows:

> **Privacy** is assurance that one's health information is being collected, accessed, used, retained, and shared only when necessary and only to the extent necessary and that it is being protected throughout its life cycle consistent with fair privacy practices, applicable law and regulations, and the preferences of the individual. [7]

The textbook also provides a working definition of security in the context of health information:

> **Security** refers to the protection of the confidentiality of private, sensitive, and safety-critical information, the integrity of health data and metadata, and the availability of information and services, including measures to assure the authenticity of identity and data provenance, and to maintain an accounting of actions taken by users, software programs, and systems. [7]

Trust & Privacy

Trust and privacy are inextricably linked. Violations of privacy undermine trust. After all, it is really my trust that is violated if my privacy is breached. An understanding of the role of trust is essential for an effective understanding of privacy. Making decisions about one's privacy is a direct expression of one's freedom of self-determination. The extent to which I can or cannot express my privacy preferences is a direct reflection of the autonomy that I have. [4]

Trust is essential to the exchange of meaningful value in a free market. I choose to enter into a transaction because I *trust* that the value that I receive will be equal to or greater than the value that I pay. Trust also requires vulnerability. [5] If there is no risk that I will be short-changed, there is no need to trust.

The relationship that a patient has with his or her physician is a prime example. The patient understands that to receive proper healthcare, intimate details must be shared with the physician. The patient understands that information (that they would much rather remain private) must be divulged or the treatment will be sub-optimum. In the most basic sense, the treatment is a "transaction" and both the patient and the physician trust that the other party will fulfill their mutual obligations.

When third party payers are involved, trust is still a prerequisite—it's just that there are more parties involved in the transaction and more distance between them, the provider, and the patient. If the patient wants the payer to reimburse the cost of his or her care, the patient has to trust the payer regardless of their feelings of vulnerability. The payer and provider also must trust each other to honor their contracts and to provide fair value for services rendered. As Sissela Bok has written, "Whatever matters to human beings, trust is the atmosphere in which it thrives." [9]

It is easy to recognize that the patient is much more vulnerable to the physician and extends much greater trust. Indeed, many would argue that it is because of this very vulnerability that the patient's right to privacy must be respected and protected with appropriate care—hence the need for Health IT specific privacy legislation, in the form of the HIPAA Privacy Rule and the subsequent enhancements resulting from HITECH.

Certain researchers posit that if only patients were better educated, they would be more trusting of the healthcare system, and much more willing to consent to releasing information [6]. However, there is a proven security principle called "Reluctance to Trust" that states trust should always be closely held and never loosely given [7]. Therefore, a good case can be made in support of limiting trust to only what is needed to facilitate transactions in a specific context. For example, I trust my financial planner with my financial information and my physician with my health information, but not vice-versa. [8].

Trust is also related to competence. One is willing to share private details with a physician or other skilled service provider, because we trust that they will competently use that information on our behalf. If I do not trust the competence of the service provider, I will not put myself in a position of vulnerability to that person. A key component of one's decision to release private information is one's judgment about the other's ability to protect the privacy of the information entrusted.

Evolutionary psychologists have shown that distrust is a hardwired defense mechanism, necessary to survival [9]. We are pre-programmed to look for indicators that others are either trustworthy or not. Psychologists have also shown that our default intuitive judgments are not always accurate, but more and higher quality information leads to better decision making [9].

For this reason, increasing transparency enhances trust. The breach notification database maintained by the Department of Health & Human Services is a very good example of an effort to increase transparency. This is also why providers are required to maintain an "accounting of disclosures" when transmitting protected health information.

When thinking about privacy, it is important to remember that trust is transitive. "Once you dole out some trust, you often implicitly extend it to anyone the trusted entity may trust." [7] We must be sensitive to the fact that this is what makes many people uneasy about sharing personal information. Whether one is aware of it or not, the decision to trust and share personally identifiable information is based on a risk calculation that is part of our psychological hardwiring. An individual may not accurately perceive the risk [9] but it is clear that one's experience and assessment of the other's reputation are predominant factors in the decision making process [10]. Our hardwired "trust" defense mechanism makes us more trusting of people that we see face to face and interact with frequently. Proximity plays an important role in trust [11], [12]

Providing care to a patient requires more than just a physician. It requires a team of dedicated professionals, many often working in the background. As stated earlier, judgments about competency factor into decisions regarding privacy. Policies and procedures, as well as organizational maturity and transparency make a patient more comfortable about releasing personal health information. [13]

Consent

One of the fledgling efforts in the health privacy realm is a concept called "granular consent." This innovation attempts to clarify the patient's privacy expectations in an efficient and structured manner. Rather than requesting blanket consent to release information, granular consent is a framework to identify and manage each patient's private health information in a manner that empowers the patient to make decisions about the sharing of their information and preserves their freedom of self-determination—garnering increased trust in the process!

A group of industry experts that advises federal regulators on health information policies pertaining to security and privacy, dubbed the "Tiger Team," called for more study of the granular consents concept, recognizing the lack of technology currently available to selectively exclude different types of data from health information exchanges. The August 19, 2010 Tiger Team report to ONC Health IT Policy Committee states the following pertaining to granular consents:

> *The Tiger Team believes that methodologies and technologies that provide filtering capability are important in advancing trust and should be further explored. There are several efforts currently being piloted in various stages of development. We believe communicating with patients about these capabilities today still requires a degree of caution and should not be over sold as fail-proof, particularly in light of the reality of downstream inferences and the current state of the art with respect to free text. Further, communicating to patients the potential implications of fine-grained filtering on care quality remains a challenge.* [14]

Although more work needs to be done to make granular consents a reality, the Tiger Team did outline a more workable concept called "Meaningful Consent," wherein patient consent would be required to exchange data via a health information exchange or other third party, such as an e-prescribing gateway [14]. The Tiger Team did outline specific guidance for consent to be meaningful:

- The individual must be allowed adequate time to make a decision.
- Consenting to information exchange is not to be a condition of receiving necessary medical services.
- The individual is to get a clear explanation of the choice and its consequences using clear language.
- The consent is to be revocable.

Fair Information Principles

Another important advancement is the publication of "Fair Information Principles" in the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*, which outlines the basic principles as to how health organizations are to manage electronic health information. [15] These principles are summarized below:

1. **Individual Access** – Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.

2. **Correction** – Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.
3. **Openness and Transparency** – There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.
4. **Individual choice** – Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information.
5. **Collection, Use, and Disclosure Limitation** – Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.
6. **Data Quality and Integrity** – Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.
7. **Safeguards** – Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
8. **Accountability** – These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

In making their policy recommendations, the Tiger Team mapped these principles to the rationale in their recommendations. They were also unabashed in affirming the following core value:

> *The relationship between the patient and his/her health care provider is the foundation for trust in health information exchange; thus providers are responsible for maintaining the privacy and security of their patients' records.* [14]

Conclusion

When Patricia's psychotherapy notes were mishandled back in 2001, it was not only a violation of her trust, but also her doctor's trust. No doubt her psychotherapist made a good faith promise to her, trusting that "the system" would know and respect her expectations.

In the past decade, lots of work has been done by countless groups and individuals to make the systemic improvements needed to safeguard and enhance the personal privacy of health records. However, as the granular consents discussion shows, much more work is needed—and this work is ongoing.

This paper has attempted to show that trust is integral to privacy and that enhancing trust is not simply a matter of additional education. Trust requires transparency and establishing a track record of trust-worthiness. Trust is

required for transactions. The more important the transaction (such as life or death) the more trust required. Because proximity plays an important role in trust, the role of the physician in establishing and maintaining trust is paramount.

However because the chain of trust extends way beyond the physician, tools such as the *Fair Information Principles* provide important guidance on how to manage personal private information in a trustworthy manner. Transparency is important, because more information leads to better quality decision making. Recognizing that we, as humans are hardwired to make trust judgments is important. Rather than dismissing this fact, it is important to validate this need and support it by creating systems and conducting business in a manner that respects privacy and enhances trust.

References

[1] D. B. Baker, *Personal Privacy vis-à-vis Information Security.*

[2] J. D. e. a. Bransford, How People Learn: Brain, Mind, Experience, and School, Washington, D.C.: National Academy Press, 2000.

[3] T. Francis, "Spread of Records Stirs Patient Fears Of Privacy Erosion," The Wall Street Journal, 26 December 2006. [Online]. Available: http://tinyurl.com/72vgyyx. [Accessed 4 April 2012].

[4] U.S. Department of Health & Human Services, "The Privacy Rule," [Online]. Available: http://tinyurl.com/lcw63a. [Accessed 28 May 2012].

[5] U.S. Government Printing Office, "Public Law 111 - 5 - American Recovery and Reinvestment Act of 2009," [Online]. Available: http://tinyurl.com/6lsp7q5.

[6] U.S. Department of Health & Human Services, "HITECH Breach Notification Interim Final Rule," [Online]. Available: http://tinyurl.com/lmhono.

[7] G. Brown, Ed., Health Informatics: A Systems Perspective, Chicago: Health Administration Press, 2012.

[8] E. L. Deci and R. M. Ryan, Intrinsic Motivation and Self-Determination in Human Behavior (Perspectives in Social Psychology), New York: Plenum Press, 1985.

[9] "What is Trust?," ChangingMinds.org, [Online]. Available: http://tinyurl.com/cp8r37. [Accessed 4 April 2012].

[10] S. Bok, Lying: Moral Choice in Public and Private Life, New York: Vintage Books, 1978.

[11] S. R. M. M. Simon, M. J Stewart Evans, M. Alison Benjamin, B. David Delano and M. M. David W Bates, "Patients' Attitudes Toward Electronic Health Information Exchange: Qualitative Study," *Journal of Medical Internet Research,* 2009.

[12] S. Barnum and M. Gegick, "Reluctance to Trust," US Department of Homeland Security, Build Security In, 15 September 2005. [Online]. Available: http://tinyurl.com/7elfs32. [Accessed 14 April 2012].

[13] C. McLeod, "Trust," *The Stanford Encyclopedia of Philosophy,* no. Spring 2011 Edition, 2011.

[14] D. Ropeik, How Risky Is It Really?, New York: McGraw-Hill, 2010.

[15] A. Partida and D. Andina, "Vulnerabilities, Threats and Risks in IT," in *IT Security Management*, vol. 61,

Springer Netherlands, 2010, pp. 1-21.

[16] J. Bruneel, A. Spithoven and A. Maesen, "Building Trust: A Metter of Proximity?," *Frontiers of Entrepreneurship Research,* vol. 27, no. 15, p. Article 1, 2007.

[17] T. Gossling, "Proximity, trust and morality in networks," *EUROPEAN PLANNING STUDIES ,* vol. 12, no. 5, pp. 675-689 , 2004.

[18] L. Dimitropoulos, V. Patel, S. Scheffler and S. Posnack, "Public Attitudes Toward Health Information Exchange: Perceived Benefits and Concerns," *The American Journal of Managed Care,* vol. 17, no. 12, pp. SP111-SP116, 2011.

[19] HIT Policy Committee Privacy and Security Tiger Team, "Transmittal Letter, October 18, 2011," [Online]. Available: http://tinyurl.com/6tqq9wq.

[20] H. Anderson, "Patient Consent Guidelines Endorsed," Healthcare Info Security, 19 August 2010. [Online]. Available: http://tinyurl.com/7pnddqf. [Accessed 15 April 2012].

[21] Office of the National Coordinator for Health Information Technology, 15 December 2008. [Online]. Available: http://tinyurl.com/7jqkc4c.