patientprivacyrights

privacytrustframework

ABSTRACT

Today's data-rich networked society can make deployment of trusted electronic systems practical and painless, but the current environment is dominated by untrusted systems that use privacy policies and click-through agreements as a legal hammer, not as a means of establishing trust. Patient Privacy Rights and the bipartisan Coalition for Patient Privacy, in concert with Microsoft and PricewaterhouseCoopers (PwC), developed and tested a set of privacy principles and standards, operationalized in criteria that can be built into all electronic systems, platforms, and applications that handle personal data and use the privacy policy as a way of aligning business practice with trust factors enforceable by an easy audit mechanism. In 2008, Patient Privacy Rights, PwC, and Microsoft developed and validated this robust privacy certification program on HealthVault, showing how the Trust Framework can be used for a formal privacy certification process. The Trust Framework differs from other certification processes because it is designed specifically to enhance consumer engagement, education, and trust in electronic systems, platforms, and applications that hold individuals' personal health information. This writing describes the set of 75+ auditable criteria that measure privacy and align privacy policies to acceptable business practices that establish trust.

OVERVIEW

The PPR Trust Framework is a set of 75+ auditable criteria that measure how much technology protects data privacy. PPR and the bipartisan Coalition for Patient Privacy, in concert with Microsoft and PricewaterhouseCoopers (PwC), developed and tested a set of privacy principles and standards, operationalized in criteria that should be built into all electronic systems, platforms, and applications that handle personal health data in order to prove they are worthy of public trust.

The copyrighted Patient Privacy Rights Trust Framework can be used to measure and test whether health IT, platforms, applications, and research projects comply with the gold-standard privacy principles the bipartisan Coalition for Patient Privacy established in 2007-2008 over a period of 18 months. A patent is pending to assure that this system can be widely used to measure how closely systems, platforms, and applications meet patients' expectations for control over personal data, and expectations of state-of-the art data security.

Today's data-rich networked society makes deployment of trusted electronic systems practical and painless. Patient Privacy Rights believes organizations can earn public trust by attesting and adhering to the principles outlined in its Trust Framework and privacy certification process. In 2008, PPR, PwC, and Microsoft developed and tested this robust privacy certification program on HealthVault. Several key consumer organizations, including the ACLU and Consumer-Action, participated in the development and testing of the Trust Framework.

The PPR Trust Framework process itself is based on the bipartisan consumer privacy policies and principles established in 2007 as a result of a very inclusive, thoughtful process by members of the bipartisan Coalition for Patient Privacy, which promotes patient empowerment and privacy (control over health information).[1] These privacy policies and principles are well known, published, and have remained the foundation for all of PPR's advocacy efforts since their inception.[2] Both the 2007 privacy

principles and PPR's Trust Framework are grounded in Americans' longstanding civil, human, and ethical rights to health information privacy.

PPR's Trust Framework could be used for a formal privacy certification process. It differs from other health IT certification processes because it is designed specifically to enhance consumer engagement, education, and trust in electronic systems, platforms, and applications that hold individuals' personal health information.

Existing certification processes, such as the Office of the National Coordinator for Health Information Technology's Permanent Certification Program (PCP), focus on data security and compliance with Meaningful Use objectives and measures.[3] Other systems, such as the self-certification program for compliance with U.S.-EU Safe Harbor Framework, ensure that organizations comply with certain "adequacy" standards for privacy protections. However, this self-certification process is designed to benefit organizations and facilitate involving data transfer for business dealings, not promote consumer trust.[4] Alternatively, PPR's privacy certification method is designed to assure consumers that the electronic systems containing their personal health information are truly private, trustworthy, and allow patients to control how and by whom their information is used.

Starting from the baseline requirement that systems must have state-of-the-art data security certification (i.e., comply with the PPR Trust Framework requirements for strong data security) systems, platforms and applications must demonstrate compliance with more than 75 auditable privacy principles (Appendix A), such as:

- Whether or not a patient has control over his/her PHI;
- Whether or not the organization obtains meaningful consent before disclosing any data;
- Whether or not the organization obtains new consent before secondary uses of data occur;
- Whether or not a patient has the ability to selectively share data; and
- Whether or not the organization uses servers in the United States.

BENEFITS

The Trust Framework use for certification or research will be very beneficial for many reasons. Finally the public will easily be able to "tell the good guys from the bad guys."

Developers of health IT systems, platforms, applications, and organizations that claim to be committed to privacy should absolutely be able to outwardly reflect that avowed commitment. Organizations whose operations demonstrate the strongest commitment to the privacy of its patients and customers will want to make the public aware of this commitment. Privacy seals could be awarded for compliance with the PPR Trust Framework and would distinguish trustworthy organizations that are truly making a full and good-faith effort to honor individuals' right to privacy from all the rest.

Public awareness of privacy-positive companies and organizations would be a very significant step and create pressure to restore privacy and the Constitutional liberties and freedoms that the Digital Age has violated. As more and more consumers—of healthcare and other products and services—become better

educated about their privacy rights and the existing and growing threats to those rights, they will look for privacy-committed companies with whom to do business. Consumers will reward good business practices by participating in systems or projects that are publicly committed to operate in compliance with the Trust Framework's privacy principles.

Another great benefit of the using the PPR Framework is the integral role it could play in building a vibrant, trusted research ecosystem. In general, the public is altruistic and willing to participate in research, provided that they know they have control over their information and can choose the type of research in which they participate. Furthermore, they want to know that the platforms and applications they donate their information to are trustworthy and secure. The trust framework offers research organizations and institutions the opportunity to demonstrate their commitment to informed consent and strong data security and data privacy protections.

But patients are the greatest beneficiaries of the Trust Framework. They should be able to protect themselves and be able to easily see which electronic records systems, applications, and websites to avoid. Systems, websites, and applications that attest to complying with the PPR Trust Framework openly demonstrate that patients' data will remain private, secure, and available only for the purposes they've specified.

Restoring patient control by empowering patients to make meaningful choices of HIT systems and products based on attestation to the tough privacy principles and criteria they expect for health information is critical to restoring patient privacy and trust in the healthcare system and the Internet. Use of the Patient Privacy Rights Trust Framework will offer all health care consumers the ability to control their most sensitive and sacred personal information and reap the rewards of health IT by enabling them to select systems worthy of trust.

ACKNOWLEDGEMENTS

I would like to acknowledge and extend my heartfelt gratitude to the many individuals who have made the development of the PPR Trust Framework and this paper possible.

There are too many to name them all, but the following contributors were particularly instrumental in the completion of this project: Cliff Baker of PwC; Katherine Ball, MD; Dane von Breichenruchardt, President of the Bill of Rights Foundation; the late Gary Chapman of the University of Texas LBJ School of Public Affairs; Michelle De Mooy of Consumer Action; Richard Dick, PhD; Dan Garrett, Partner and HC IT Practice Leader at PwC; David Hilgers, Partner and Chair at Brown McCarroll, L.L.P.; Ashley Katz of PPR; John Metz of Just Health (CA); Brian Mulconrey of Tomorrow's Enterprises; Peter Neupert of Microsoft, HealthVault; Sean Nolan of Microsoft, HealthVault; Michael D. Ostrolenk of The Liberty Coalition; Jim Pyles, Partner at Powers, Pyles, Sutter, & Verville; Greg Scandlen of the Heartland Institute; Timothy Sparapani of the ACLU; Michael Stokes of Microsoft, HealthVault; Patsy Thomasson of the Ben Barnes Group; Jim Turner, Principal at Swankin and Turner; William Yasnoff, MD of NHII Advisors.

Special thanks go to PPR's Kat Johnson and Atalie Nitibhon and Professor Latanya Sweeney of Harvard University for their assistance in writing and reviewing this paper.

[1] The Coalition for Patient Privacy's framework of consumer privacy policies and principles was announced to Congress in a letter that represented the views of 10 million Americans. See: http://patientprivacyrights.org/media/Letter_to_Congress_Final_10_17.07.pdf?docID=2281.

[2] Ibid.

[3] The Office of the National Coordinator for Health Information Technology. (2011, March 31). *Standards and Certification Criteria Final Rule*. Retrieved from http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__standards_ifr/1195

[4] Export.gov. (n.d.). *U.S.-EU Safe Harbor Overview*. Retrieved November 28, 2012, from http://export.gov/safeharbor/eu/eg_main_018476.asp

Appendix A

The consumer-led Patient Privacy Rights Trust Framework includes 15 clear principles:

Principle # 1. Patients can easily find, review, and understand the privacy policy.

Principle # 2. Privacy policy fully discloses how personal health information will and will not be used by the organization. Patients' information is never shared or sold without patients' explicit permission.

Principle # 3. Patients decide if they want to participate.

Principle # 4. Patients are clearly warned before any outside organization(s) that does not fully comply with the organization's privacy policy can access their information.

Principle # 5. Patients decide and actively indicate if they want to be profiled, tracked, or targeted.

Principle # 6. Patients decide how and if their sensitive information is shared.

Principle # 7. Patients are able to change any information that they input themselves.

Principle # 8. Patients decide who can access their information.

Principle # 9. Patients with disabilities are able to manage their information while maintaining privacy.

Principle # 10. Patients can easily find out who has accessed or used their information.

Principle # 11. Patients are notified promptly if their information is lost, stolen, or improperly accessed.

Principle # 12. Patients can easily report concerns and get answers.

Principle # 13. Patients can expect the organization to punish any employee or contractor that misuses patient information.

Principle # 14. Patients can expect their data to be secure.

Principle # 15. Patients can expect to receive a copy of all disclosures of their information.

The charts on the following pages illustrate the auditable criteria for each of the 15 principles that demonstrate whether or not an organization is in compliance with the PPR Trust Framework.

#	Principle	Req. #	Requirement	Status	Document XREF	Comment
1	Patients can easily find, review, and understand the privacy policy.	1.1	Privacy policy includes a short summary accurately describing the patient's control of their data and all access to that data. The policy must specifically list any organizational personnel by organizational role that access data for operational purposes.			
		1.2	The policy must be easily accessible from the organization's home page.			
		1.3	Privacy policy must not use passive structures ("we share" vs. "the sharing"), qualifying verbs and adverbs ("use" and "will" vs. "may," "occasionally," and "from time to time"). We encourage the policy to use short sentences and small words.			
		1.4	Privacy policy must have topic headings that link to plain language explanations of the type of data accessed and how the data are handled. We encourage the use of charts and tables.			
		1.5	Privacy policy shall attain a Flesch Reading Ease score of 45 or higher.			
		1.6	Privacy policy shall attain a Flesch-Kincaid Grade level score of 12 or lower.			
		1.7	Privacy Policy shall use a minimum 9 pt. font.			
		1.8	Privacy policy is available in the native language of the organization's significant customer populations. Additionally, localization of deployment targets the designated official language of jurisdictional area.			
		1.9	Privacy policy provides easy access to definitions of technical terms.			
		1.10	Privacy policy includes explicit language on process and notification of "material changes" and allows customers a defined timeline to opt out prior to policy changes.			

#	Principle	Req. #	Requirement	Status	Document XREF	Comment
2	Privacy policy fully discloses how personal health information will and will not be used by the organization. Patients' information is never shared or sold without patients' explicit permission	2.1	Privacy policy states that personal information is collected only with informed consent, unless otherwise required by law.			
		2.2	Privacy policy must clearly state what the organization will and will not do with personal health information.			
		2.3	Privacy policy fully describes use of internet monitoring technologies, including but not limited to beacons, weblogs, and cookies.			
		2.4	Privacy policy fully describes all data sharing circumstances that require a patient to opt-in.			
		2.5	Privacy policy fully describes what ability the patient has to change, segment, delete, or amend their information.			
		2.6	Privacy policy fully describes who can access the information and when.			
		2.7	Privacy policy fully describes under what circumstances data are externally disclosed.			
		2.8	Privacy policy fully describes with whom data are shared.			
		2.9	Privacy policy fully describes how information is not disclosed.			
		2.10	Privacy policy describes how all access to data is recorded and how resultant audit trails are accessible to the patient.			
		2.11	Privacy policy describes procedures the organization will follow in the event of a security breach.			
		2.12	Privacy policy describes the organization's process for receiving and resolving complaints.			
		2.13	Privacy policy describes a mechanism for Third Party resolution of complaints.			
		2.14	Privacy policy confirms that all persons with access to the data must comply with privacy policies.			

#	Principle	Req. #	Requirement	Status	Document XREF	Comment
3	Patients decide if they want to participate.	3.1	System provides clear notification of informed consent during registration. All patients must opt-in.			
		3.2	System allows patient to opt out at any time, and the opt out process must be simple and clearly stated in the privacy policy.			
		3.3	System provides capability for all access to the patient's data to be removed at any time. Patient has the ability to permanently delete all information upon closing an account.			

#	Principle	Req. #	Requirement	Status	Document XREF	Comment
4	Patients are clearly warned before any outside organization(s) that does not fully comply with the organization's privacy policy can access their information.	4.1	Organization must contractually require all persons with access to data to clearly disclose whether they comply with its privacy policies. Audit trails are sufficient to verify data access compliance.			
		4.2	For internet applications, the organization must ensure the patient can easily access any other website's privacy policy before linking to another site.			
		4.3	The organization shall prominently display the PPC™ seal of any organization that has obtained PPC ™ certification prior to obtaining informed consent for information sharing.			
		4.4	Organization ensures visual indication that distinguishes between outside organizations governed by HIPAA and outside organizations that are not governed by HIPAA with additional links to educational information explaining the difference.			

#	Principle	Req. #	Requirement	Status	Document XREF	Comment
5	Patients decide and actively indicate if they want to be profiled, tracked, or targeted.	5.1	Any profiling must be optional (opt in) with the ability to opt out.			
		5.2	The system must allow patients to clearly identify data used for profiling and targeting.			
		5.3	Patients must be able to opt out of any profiling at any time. The opt out process must be simple and clearly stated in the privacy policy.			
		5.4	The patient may chose which specific data elements may be used for profiling and targeting.			
		5.5	Opting out of profiling and targeting has no secondary effects on the patient. This is clearly stated in the privacy policy.			
		5.6	The system never shares profiling data without patients' prior informed consent.			

#	Principle	Req. #	Requirement	Status	Document XREF	Comment
6	Patients decide how and if their sensitive information is shared.	6.1	System allows patient to selectively release each element of their health information.			

#	Principle	Req. #	Requirement	Status	Document XREF	Comment
7	Patients are able to change any information that they input themselves.	7.1	System allows patient to delete, change, or annotate each element of their health information.			
		7.2	The patient may permanently delete their personal information from the system upon patient request.			

#	Principle	Req. #	Requirement	Status	Document XREF	Comment
8	Patients decide who can access their information.	8.1	Access to personal health information and system functions is limited by role-based and individual access.			
		8.2	System provides the functionality to control access to the data.			
		8.3	System provides functionality for access to specific system functions (e.g., viewing audit records).			
		8.4	The ability to control the type of access that is provided to the system (e.g., read, write, delete) is controlled by the patient.			
		8.5	The system specifies how long access to data is available (e.g., indefinitely or one week).			
		8.6	Organization must document processes in place for emergency access to data and demonstrate that the procedures are operating effectively either through testing or analysis of actual events.			
		8.7	All aggregation processes must be documented and assure that the organization uses state of the art methods to prevent the disclosure of identifiable information.			

#	Principle	Req. #	Requirement	Status	Document XREF	Comment
9	Patients with disabilities are able to manage their information while maintaining privacy.	9.1	Corporate commitment to Section 508 of the Rehabilitation Act in 1998 and specific Voluntary Product Accessibility Template (VPAT) for product.			
		9.2	Full compliance with 508 and VPAT.			

#	Principle	Req. #	Requirement	Status	Document XREF	Comment
10	Patients can easily find out who has accessed or used their information.	10.1	Organization maintains audit trails of every event. Retention cycles for maintaining audit trails are based on the minimum HIPAA-entity requirements (e.g., six years).			
		10.2	Audit trail includes who performed the action.			
		10.3	Audit trail includes what action was performed.			
		10.4	Audit trail includes what data object was involved.			
		10.5	Audit trail includes when the action occurred.			
		10.6	The system does not allow the audit trail function to be "turned off." The audit record cannot be altered, and records do not expire.			
		10.7	Audit trails must be readily available to the patient.			
		10.8	Audit logs can be searched or filtered by who performed the action.			
		10.9	Audit logs can be searched or filtered by what action was performed.			
		10.10	Audit logs can be searched or filtered by what data object was involved.			
		10.11	Audit logs can be searched or filtered by when the action occurred.			

#	Principle	Req. #	Requirement	Status	Document XREF	Comment
11	Patients are notified promptly if their information is lost, stolen, or improperly accessed.	11.1	Following discovery of a breach of personal health information, organizations must notify each individual whose information has been, or is reasonably believed to have been, accessed as a result of such breach. Organization must comply with the most restrictive federal or state requirements, which, at this time, is the breach notification law of the State of California			

#	Principle	Req. #	Requirement	Status	Document XREF	Comment
12	Patients can easily report concerns and get answers.	12.1	The organization must have a process that enables patients, advocates, employees, and government regulators to report potential or actual privacy violations.			
		12.2	The organization must acknowledge a patient's concerns, investigate, and inform the patient of the outcome of the investigation and take any corrective action within fifteen business days.			
		12.3	The organization provides a link to the PPC™ website allowing the patient to file a complaint with PPC™ if the patter is not resolved by the organization to the patient's satisfaction.			
		12.4	The organization will provide a quarterly report to PPC™ that describes the privacy complaint, resolution, and actions to ensure the problem does not recur.			

#	Principle	Req. #	Requirement	Status	Document XREF	Comment
13	Patients can expect the organization to punish any employee or contractor that misuses patient information.	13.1	The misuse or improper access of confidential personal health information must include penalties up to and including termination of employment and referral to public prosecutors.			
		13.2	All key personnel with system access must have at least one day of privacy training on an annual basis. On an annual basis, all personnel with system access must have at least: • One hour of privacy training • One hour of security training			
		13.3	All personnel with system access must sign appropriate annual agreements to illustrate their understanding of the organization's privacy policies.			

#	Principle	Req. #	Requirement	Status	Document XREF	Comment
14	Patients can expect their data to be secure.	14.1	The system has undergone a security assessment by an independent third party, and there is a viable plan in place to mitigate any identified issues. (Reference PPC website for a list of Third-Party assessors and certifications accepted by PPC.)			
		14.2	The organization has designated a person with responsibility for and authority over privacy matters.			
		14.3	Organization only stores patients' information in the United Sates, its territories, or in countries that meet the requirements of the EU Data Protection Directive.			
		14.4	Organizations have processes and tools in place to identify and track where patients' information is allowed to be stored by the organization or its business partners acting on its behalf.			

#	Principle	Req. #	Requirement	Status	Document XREF	Comment
15	Patients can expect to receive a copy of all disclosures of their information.	15.1				