An Agile Approach to Privacy and Security

Brendan Seaton

Associate Editor/Editorial Advisor, HIM&CC, President of ITAC Health and Chief Creative Officer for Privacy Horizon Inc.

Agile development has become the new standard for software development. Supplanting the traditional ”Waterfall” methodology used by developers for decades, Agile turns development on its head by focusing on customer needs, business value, stakeholder engagement, rapid development and early and predictable delivery.

Agile is characterized by the incremental and iterative development of software products. It seeks to bring software products to market quickly, and continuously improve the products over time. It eschews the highly structured and rigid methods of the past where engineering trumped utility. In our fast-paced world driven by innovation and digital disruption, Agile has proven to be more effective than other traditional methodologies. Without question, Agile is here to stay.

I believe it is fair to say that addressing privacy and security in today's agile environment is challenging at best, and nonexistent at worst. Our Privacy by Design (PbD), Privacy Impact Assessment (PIA), and Threat and Risk Assessment (TRA) methodologies were built for the waterfall world. These methods were born out of privacy principles and privacy laws developed in the late 1990s and early 2000's. Many privacy and security officers don't know how to fit into the rapidly spinning world of agile iterations and sprints, where software architectures, privacy and security features, and data flows are moving targets.

We need to rethink our approach to privacy and security in an Agile world. We need to adapt our PbD, PIA and TRA methodologies to support agile development. At the same time, we can adopt the principles of Agile development to improve our privacy and security practices by effectively responding to customer (i.e. patient) needs and providing business value to our organizations.

> *“Agile has proven to be more effective than other traditional methodologies. Without question, Agile is here to stay.”*

The following are a few practical steps privacy and security officers can take to ensure that that privacy and security becomes an integral part of the organization's Agile development approach.

Learn and teach: Privacy and security officers should familiarize themselves with the basic concepts of Agile development. You don't need to become an agile expert. But you do need a working knowledge of the methodology so that you can contribute in a meaningful and appropriate way.

Similarly, agile developers must become familiar with privacy and security requirements. Privacy and security officers should ensure that each member of the development team has received privacy and security awareness training and is familiar with privacy and security requirements defined in legislation, standards, guidelines and policies.

Take your place: The Agile development methodology defines a number of roles that can enable privacy and security officers to directly engage in the development process. This includes:

- **Privacy and security stakeholder** - Privacy and security officers are important stakeholders who can help to define requirements for the new system. It should be noted that numerous stakeholders may be involved in the project who will be competing with privacy and security for priority and resources. The privacy and security stakeholder must make the case for investing in privacy and security features that meet customer and business needs.
- **Privacy and security mentor** - Privacy and security officers can be mentors or experts who can assist the development team to develop solutions to meet privacy and security requirements.
- **Privacy and security evangelist** - privacy and security officers acting at the corporate level can promote a privacy and security culture and the adoption of privacy and security standards, guidelines and best practices that apply to all development initiatives.

Tell your stories: one of the key building blocks of Agile development is the user story. User stories are short, simple descriptions of features told from the perspective of the person who desires the new capability, usually a user or customer of the system. They typically follow a simple formula: As a <type of user>, I want <some goal> so that <some reason>.

For example: As a patient, I want access to my electronic health record so that I can become more involved in the management of my chronic disease, or: as a physician, I want secure remote access to my EMR system so that I can respond to patient needs at any time, from anyplace.

Agile developers will take the user story and develop the functionality necessary to meet the user need.

Privacy and security officers should ensure that user stories are in place for each key privacy and security requirement for the system. They should also ensure that user stories submitted by other stakeholders address privacy and security requirements as needed.

Manage the risks: Privacy and security specialists have much to contribute to the identification, assessment and management of risks associated with the agile development exercise. This could include threat modeling, incident management, conventions for addressing common security vulnerabilities (e.g. response to the OWASP top 10), legislative and policy compliance. Risk management it Is also a method to help priorize the development of features impacting privacy and security.

Sprint to the finish: A sprint is an activity during a set period of time where specific work has to be completed and made ready for review. Privacy and security officers should ensure that each sprint addresses privacy and security in user stories as appropriate. Privacy and security features should be tested and validated at the end of each sprint.

When we talk about customer needs and business value with respect to healthcare IT, privacy and security should be high on the list of priorities. While it is challenging to privacy and security specialists, Agile offers new opportunities to engage in the development process. The appropriate response to Agile is to embrace it. This will serve to improve the privacy and security of our health information systems.