Relinquishing Privacy to Research

I have always loved medicine. The science is intriguing and you can get involved if you want, which I did as a teenager, volunteering at the local hospital and giving blood every time a blood drive came through my community. As with many people who thought they would follow a certain path as a child, I took a left turn at college and decided on a different career direction, but I never lost my love of medicine and the science behind it. As an adult, I have continued to participate in spot studies and recently signed up for the All of Us Research Program sponsored by the US National Institutes of Health (NIH).[1] I cannot remember what triggered me to do it a year or two ago. I do remember the day I went in to get the testing and lab work done, but I do not remember any big concern over my privacy. I knew I was surrendering my medical statistics to science, but I did not pour over the detailed privacy statements and controls available to me; I signed up because it seemed like the right thing to do. I do not mind lab tests or blood draws, so I said yes. And today, I still am pleased with my decision.

Cindy Baxter, CISA, ITIL Foundation
Is an assistant vice president at State Street Corporation, Boston, Massachusetts, USA, and a member of its risk assurance team, where she works on the first line of defense for State Street's Global Markets business unit. Prior to working at State Street, Baxter managed a global application development management (ADM) compliance team at AIG focused on software development life cycle (SDLC), identity and access management (IAM), and IT security screening for AIG's commercial market segment. Her technical experience comes from her role as IT director of operations at Johnson & Johnson's global command center and her work in technical sales and engineering at AT&T as a relationship director for several Fortune 100 clients. She is grateful to have learned technology from the ground up, and happy to have arrived at a career in audit and risk management, which allows her to leverage her experience across four industries.

I am not alone. More than 350,000 participants have signed up for the All of Us Research Program as of 22 October 2020, a third of the way to the goal of one million participants for the planned 10-year duration of the study.[2] I had heard about the famous Framingham Heart Study, which began in 1948 and is now on its third generation of participants.[3] With no Internet in 1948, privacy must have felt different: no social media, no information network, no big data either, just paper records. In fact, the US Health Insurance Portability and Accountability Act (HIPAA) was not established until 1996.[4] Privacy has truly come of age with information systems disciplines, and the IS auditor has a critical role in reviewing research compliance and fostering awareness regarding the complexities of the networked healthcare research that the All of Us Research Program represents. It is important to examine attitudes regarding privacy, pose questions about the ethics the IS auditor may choose to consider and outline a proposed framework using the backdrop of medical research underway in the All of Us Research Program as an example of how the NIH is handling the program's privacy.

Privacy Defined

What is privacy? Merriam-Webster defines "privacy" as:[5]

- "Freedom from unauthorized intrusion"
- "Secrecy, i.e., the condition of being hidden or concealed"
- "The quality or state of being apart from company or observation, i.e., seclusion"

When you ask individuals how they define privacy, most people would say it is defined as the expectation that one's matters are hidden from others, whether it is employers, insurance providers, neighbors or the public. Privacy is something expected and agreed upon from the definition perspective, yet privacy is all about what each individual chooses to shield and chooses to disclose. It is the self-determination implicit in the definition of privacy that makes it so hard to categorize in an easy outline of what to protect and what to allow, especially when considering that privacy protections start with the individual and how that individual chooses to handle dissemination of their own information.

In the 1990s and at the turn of the century while information systems professionals contemplated the challenge of privacy, technology became ubiquitous, interconnected and economical, reshaping expectations as more and more people gained access to and could share personal stories on a wide scale. Before the advent of cheap and easy Internet access, privacy was a matter of trust between individuals, agreed upon with a handshake or sealed with a contracted nondisclosure agreement, often a paper copy. Mindsets changed in the 1990s as schools considered the Internet a learning necessity. Social media was not much of a concept before the late 1990s/early 2000s, with the likes of Friendster (2002), LinkedIn (2003), Myspace (2003), Hi5, (2003) and SixDegrees (1997).[6] Social media was, well, social, and initial concerns revolved more around freedom of speech than privacy considerations. By 2008, Myspace was on the decline and Facebook became a household word, changing the expectations people had for what was private. In less than a decade, stories people shared with friends and acquaintances went from casual conversations to widespread posting.

The concept of technology-enabled personal stories gave privacy the myriad of definitions we live with today. While the core Merriam-Webster definition is just as relevant, interpretations vary from person to person. It is human nature to share stories and to embellish to heighten the interest of listeners. From ancient times when stories were told by a fire to theater productions authored by Chaucer, Cervantes, or Woody Allen, to the everyday story retellings that are common in pubs and places of gathering today, people have had a penchant for communicating, even more so when the story is focused on themselves. Wherever you find people telling stories and creating gatherings, you are bound to find sellers who are interested in reaching that audience. Street vendors have been bastions of commerce at gatherings for centuries and, as the stories and events move to the online environment, vendors are there, ready to sell anything of interest. It is no surprise that medical supplies, medical information and medicines themselves have become part of the convenient and omnipresent information flow in some very public forums.

Structure for Medical Research Privacy

HIPAA arrived just in time to provide a foundation for medical community structure at the onset of the social technology revolution. But who reads the HIPAA statement they sign or remembers the statement if they read it before? And now, with most medical records on-network instead of safely stored in paper files, who researches the privacy and security considerations before jumping into the convenience of online medical portals that provide easy access to doctors' visits, pharmacies and medical information? This proliferation of information sharing and marketing means due diligence by the IS auditor is even more important. The framework needs structure, and both patient and researcher/doctor accessibility need to be examined closely.

Before discussing a framework for auditing a privacy model similar to the All of Us Research Program, the key attributes should be reviewed. The NIH All of Us Research Program handles two main pillars of privacy governance, one for volunteer candidates who agree to donate their medical information to the study and one for institutions and their researchers. The volunteer participant obligations are handled with an emphasis on education and awareness by the NIH. Research institutions such as Massachusetts General Hospital (Boston, USA), which signed me up for the program, solicit participants via doctor visits. If a patient is interested in volunteering as a research subject, a short series of online videos, provided by the NIH, must be reviewed by the participant, with interactive questions and answers that check for understanding in terms of the release of the subject's private information. The prospective volunteer is given options regarding the degree of participation, with each option allowing candidate volunteers a broader and broader release of their medical

Enjoying this article?

- Read *Privacy in Practice 2021: Data Privacy Trends, Forecasts and Challenges*. *www.isaca.org/privacy-in-practice-2021*
- Learn more about, discuss and collaborate on privacy in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

information, including providing lab samples and full release of medical information available through the medical network for the length of the study. Candidate volunteers can change their choices at any time and, once again, the short videos remind and require consent at each online option review point. Candidate volunteers are made aware that some information about their own individual statistics will be available via their doctors' regular visit results, but emphasis is made regarding the anonymizing of their data. Instead of personal information, volunteers have access to generalized insights and newsletters summarizing research progress.

The framework philosophy for the research institutions and their individual researchers is handled very differently. Structure and approvals provide the foundation of the researcher guidelines. Institutional oversight is a requirement, and even with consent between the NIH and the research institution, individual researchers must apply to the program directly, with their institution's approval. Step 1 is the institution's application to the All of Us Research Program followed by completion of the Data Use and Registration Agreement. To further provide consistency of data collection, participating research organizations and their qualified researchers must use a common data hub for their work. Security descriptions detail minimum requirements to be used for the research work, creating a foundation for consistent security governance across the institutions and researchers involved.

Researchers who want to join the program can find the list of approved institutions on the All of Us website, enabling them to quickly identify their eligibility before starting the application process. Researchers who apply face a long list of requirements including:

- An ethical conduct of research policy[7]
- A publication and presentation policy
- A data users' appeals policy that identifies where/how work must be conducted and the requirements for clear, approved research intent
- A policy on stigmatizing research
- The Framework for Access to All of Us Data Resources v1.1, which was updated on 12 May 2020

IS Audit Value Proposition and Execution Model

The rigor of the All of Us Research Program participation framework for both volunteers and researchers is without question. The benefit of large-scale and diverse medical research is also understood as a key facilitator to medical progress. To derive the largest and most equitable benefit from the research, participating institutions must solicit a wide array of volunteer candidates. Likewise, appropriate screening of research institutions and researchers alike is necessary to bring the best minds to the program without compromising research efficiency and without risking a breach of privacy that would devastate the program and impact future medical discoveries. The IS audit team tasked with assurance testing has the responsibility of examining all aspects of the controls established and has a special ethical obligation to conduct operations testing with respect and protection of the test data provided.

With such a complex structure involving so many people with so many backgrounds, how can an IS auditor create the most meaningful audit result? As with all audit programs, the scope of work is defined in collaboration with the business/institution being audited. Careful review of how and what to test in a reasonable time frame must be established to avoid getting lost in a sea of data. Consideration of phased audit events, where subprocesses are reviewed and completed before moving to the next subprocess may help in defining a reasonable scope and assist in providing timely manageable categories of results. Once conversations have occurred between the audit team and the team being audited, a documented scope, with full concurrence by all stakeholders, will open the door to the audit work ahead.

With scope in hand and concurrence obtained, the audit team must delve into all policies and standards, not only at the sponsor organization level (in this example, the NIH), but also at the local policies and standards level provided by the organization being audited. The NIH is a huge government workhorse, but participating organizations are as diverse as the communities they serve.[8] The audit scope, test objectives, test plans and scripts need to serve the group being audited, no matter how small or large. Key milestones to keep in mind are the following:

- The scope should embody the intent of the audit and include the policies and standards that are applicable to the processes that will be audited. Objectives of the audit should be clear to those who will be reviewed.
- Familiarity with the way things work at the local organization level is a must. Time spent with those who do the work is the best reality check and may uncover gaps against the requirements even before the operational testing starts.
- Control points to test must be identified, and the activities performed at those control points must be clear and documented.
- The audit plan must include the test objectives aligned against the requirements. Test objectives must be concise and directly relate control points being examined to the scope of work and the standard requirements of the institution.
- Test steps or scripts need to be outlined and time for testing in the live environment requested from the organization being audited to ensure access to processes and information. When historical data is being examined as part of the audit testing, it is paramount that the data be gathered objectively and, as often as possible, gathered directly from the data source or by examining the activity being performed in the operational environment.
- A key element of successful testing once the test scripts are written is to perform a "test of one" to verify the test is meaningful and aligns with the requirements under review.
- Test questions from you as the auditor are bound to arise as you do the work. As you question what you observe, gain understanding by going to source personnel for clarifications and cross-checking, when possible, with other reliable and objective sources to confirm your understanding is accurate.
- Conclusions you reach need concurrence from the business regarding what you have observed. This will verify that the results are a true representation of what is occurring—before you publish the outcome of your audit work.

When auditing sensitive information such as adherence to HIPAA and appropriate participation by researchers in programs such as the NIH All of Us Research Program, expect that you as the auditor will be exposed to confidential private information and consider your obligations as well. The access you receive for the audit is not just a matter of compliance by the institution and by you, it is a matter of trust between you and the party you audit. Your work uncovers and improves the complex process that medical technology and data information have become. As information systems and interconnected networks of hospitals and clinics share data, the discovery of medical advances accelerates for the benefit of all. Your objective to audit performance against requirements, couched in a firm belief of respecting the privacy of the data you review, will positively impact the success of research and encourage people like me to continue volunteering.

Endnotes

1 National Institutes of Health, All of Us Research Program, USA, 2020, *https://allofus.nih.gov/*
2 National Institutes of Health, "All of Us Expands Enrollment and Engagement Efforts With New Awardees," News and Events, USA, 22 October 2020, *https://allofus.nih.gov/news-events-and-media/announcements/all-us-expands-enrollment-and-engagement-efforts-new-awardees*
3 Framingham Heart Study, About, USA, *https://framinghamheartstudy.org/fhs-about/*
4 American Hospital Association, HIPAA, USA, 17 November 2017, *https://www.aha.org/advocacy/compliance/hipaa*
5 Merriam-Webster, "privacy," USA, 2020, *https://www.merriam-webster.com/dictionary/privacy*
6 Modern Marketing Partners, "Five of the Top Social Media Networks Before Facebook," 23 April 2020, *https://www.modernmarketingpartners.com/2020/04/23/5-of-the-top-social-media-networks-before-facebook/*
7 National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, *The Belmont Report*, USA, 18 April 1979, *https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html*. The report defines ethical principles and guidelines for research policy.
8 National Institutes of Health, All of Us Research Program, Health Care Provider Organizations, USA, *https://allofus.nih.gov/funding-and-program-partners/health-care-provider-organizations*