COSMOS
Navigate the Compliance Universe

CEP Magazine - June 2018
Don't pay for unnecessary snakes: A case study

By Emmi Bane, MPH, CCEP

Emmi Bane (Emmi@weconnectrecovery.com) is Chief Compliance, Ethics and Privacy Officer at WEconnect in Seattle, WA.

I am, primarily, a medical ethicist whose focus is on the ethical collection, storage, and downstream policy governing large genetic research banks. I specialize in data governance and data privacy and policy. The female-founded company I work for makes a mobile application that connects individuals who are recovering from substance abuse and addiction to their support and accountability network. The application was designed by, and with input from, primary community stakeholders.

I began working with my company originally in the capacity of a medical ethicist to create and implement policy. Initially our only operational documents were a skeleton privacy policy and a document outlining terms of service, which was vague.

Our company, like many new health information technology organizations, operates in a regulatory gray area. We do not provide healthcare. We are not a medical service. We do not receive federal funding, nor did we, at the outset, work with any entity that did. We did, however, recognize that the information that people provided us with was at best sensitive, and that we had a real obligation to respect and secure it at every point in the process. The founders were responsive to the privacy concerns and questions from the community, and they wanted to design their privacy policies and practices to reflect the highest standard of security, confidentiality, and respect for the community.

Step 1: Educate yourself

I had spent nearly all of my previous professional life in healthcare, so I was aware there were additional laws and restrictions that applied to information about a person's health. What I didn't know much about was the aspect of compliance and regulation that didn't relate to health information privacy.

Our small tech company in Seattle hoped to integrate into larger national healthcare systems. We needed more than just a great search engine and a motivated ethicist. We needed reliable, actionable information; we needed guidelines and practices; and we needed legitimacy.

When I was hired to create a compliance program, our app was a very simple version used by several private companies, but we knew that the laws change once you're publicly traded. We also knew that if and when we partnered with larger institutions with federal funding (called covered entities), we would become a business associate, and as a result of the HIPAA Omnibus Rule,[1] we would ultimately be held to many of the same standards as the covered entities themselves.

It was evident that we needed not only a set of policies, but also a robust and accessible compliance and training program that would reflect both the current regulatory framework and anticipate the changing needs of the evolving regulatory landscape. We needed to build a compliance program and education curriculum from scratch, because nothing that existed was the right fit for us. The first thing we needed to do was determine what laws

applied to us to ensure that we weren't inadvertently violating any of them.

I started by researching the two most obvious laws: HIPAA and 42 CFR Part 2.[2]

Source selection

What I learned is that there is an enormous amount of overwhelming information out there. If you search for "HIPAA guide," it will yield a morass of nonsense, with several websites that contain less content than a banner ad. There are multiple businesses out there, happy to handle it for you for varying fees. And there are many, many, official documents, and not all of them are great. I spent a lot of time with federal guidance documents, simplified texts, and FAQs on government websites to ensure that I was building my foundational knowledge from primary source material and that I was comfortable enough with the original text of HIPAA to determine when a non-governmental source was providing reliable information.

For all the terrible and poorly researched scams lurking out there, some extremely helpful resources do exist. Many presentations on policy simplification, implementation, and guidance are available through professional or government organizations like the Substance Abuse and Mental Health Services Administration (SAMHSA).[3] Many companies make their operating policies, such as their codes of conduct, available to the public. Our program is a reflection of multiple different regulatory requirements. We worked hard to identify the best practices and policies of our contemporaries, and we looked at how other innovative companies were conducting themselves. Good examples make great resources.

One of the most useful sources recommended to me by a colleague was GitHub, an open-source aggregator of common codes, policies, and practices that encourages public submission and revision.[4] GitHub provides a fairly comprehensive set of operating policies that reflect federal regulatory standards for sensitive data. Having even a skeleton framework in place can make your operations seem so much less overwhelming and can provide you with some reliable structure. However, these templates are just that, templates, and should be thoroughly reviewed and modified to apply to your company. A prefabricated set of policies are not a sufficient compliance framework on their own, they will not contain any jokes, and furthermore, a vague policy is not an effective one. Your policies should not only contain jokes, which will make them bearable to both read and write, but should be a direct reflection of your operating policies.

Know your audience

One of the inherent advantages I had in building this program was the culture of the company I was building it for. Our founders demonstrated their respect and value for a robust compliance culture early and often. Our legal counsel, although a valued and cooperative colleague, is entirely distinct from our Compliance department (party of one!). A not insignificant portion of our budget was allocated to getting me trained and certified by a ratified professional association (in the interest of full disclosure, and for those of you in the way back, I have been certified by SCCE). The founders of the company gave me both time and resources. I wanted to be sure that I created a compliance program that reflected that respect both in policy and in construction.

Fear and discipline have their proponents, but in my opinion, mutual respect is a key component of operating successfully. You can't be flexible about the law, but you can be flexible about your schedule. Because I was building the program, I decided when things needed to be done. I did my best to consider the timelines and requirements of my team members in this process in order to integrate compliance as a natural process element rather than a performative nuisance.

I was always happy to reschedule a meeting, or re-prioritize a project. You may think this will free up time for

inflicting punitive tortures on the cringing penitents, but trust me when I tell you that you will save even more time by not designing a labyrinth of torments or relying on dubious methods like sinister locked cabinets or pits of snakes.

In the long run, it makes far more sense to let it be known that you are a supportive, congenial, flexible team member rather than a strict disciplinarian. This integrates compliance more laterally than other models of corporate organization, but it has the benefit of making compliance more approachable and accessible, which is ultimately the goal.

In my experience, being willing to demonstrate flexibility really underscored the instances where I needed to assert myself and made it clear when things I needed were crucial or time sensitive. In a culture of mutual respect, people were willing to pay me the courtesy of prioritizing my needs when necessary. If this doesn't work for you, I know where you can get some snakes.