SCCE™

corporatecompliance.org

# Compliance & Ethics PROFESSIONAL®

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

JUNE 2018

## Meet Thomas Topolski, CCEP-I

Executive Vice President, Turner & Townsend

*see page* **18**

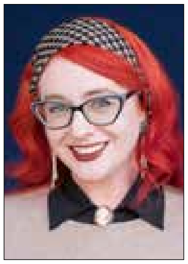
by Emmi Bane, MPH, CCEP

# Don’t pay for unnecessary snakes: A case study

- Be sure your information comes from the right place and goes to the right place; use primary sources, and know who your audience will be.
- Your compliance policies should be reflective of the same values as your practice and vice versa.
- By building your values into your practices, compliance is naturally integrated into the design and architecture of your product.
- Compliance education is most effective when it relates to how individuals will be directly affected by it and how compliance is relevant to job functions.
- Compliance must always evolve and must therefore be an iterative and inclusive process.

*__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.


Bane

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.

> 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.

## Step 2: Build your compliance program around your actual practices

This is really only good advice if your actual practices are compliant. But the point here is that your compliance program should not be some pie-in-the-sky choreography that the people on your team can't follow while you yell at them. (This metaphor is very personal to me, because I once took a tap class that inspired a recurrent nightmare and my youthful conception of Hell.)

After I identified what we absolutely had to do, I identified first what our practice actually was, and then what the best practice would be. Then I designed a way to get us from where we were to where we wanted to be.

Compliance isn't a magic trick, where something disappears from one place and reappears in another when you write a policy about it. What it is is a process—or a better metaphor is an infectious alien mind worm. Subtle, invisible, yet silently propagating, ultimately gloriously, inexorably victorious. What is there to fear? Why be the dance mom when you can be the dance itself?

**Build your program around your values**

This step is really a continuation of Step 1, because one secret to a good compliance program is that you never stop educating yourself. So before I tried to educate my team members, I let them educate me.

Most medical ethics programs are designed to protect vulnerable communities from preventable harms, but there is no one-size-fits-all model that applies to every community. The best insight into how to implement these safeguards most effectively and respectfully comes from the communities themselves. There are multiple, complex, and unique elements to each community, and developing a basic cultural competence requires exploring these. Learning the language of these communities is requisite to that competency. I listened to my coworkers. I learned what words or terms might be construed harmfully. I learned what language is preferred. For example, we avoid using the term "user" in our policies and service agreements, because the word has a markedly different connotation for our primary market. I heard what people valued and respected, and in turn I used those values as the foundation for our policies.

One benefit of building your own compliance program is that you can tailor it to your company culture and values from the outset. This way the compliance program can grow with the company.

**Build your values into your process**

We started at the beginning. By including privacy and security standards in our design—and by implementing a model of informed consent for data collection, protection, and sharing—we anticipated many of the functional requirements of the relevant laws, thereby reducing our regulatory burden substantially.

We also instituted a practice, known now as "Privacy by Design," in which Compliance is involved at the conception and architecture of each new feature, ensuring that little development time is ever required to undo work that has been done or to retrofit a feature for compliance. Our standards are built into our product at every point in the process. This also helps me to learn about the design and development process, allowing me to better assess the risk of operations. Involvement in the development process can help prevent risky features from being implemented, but more importantly, it can help your team members envision products from a compliance perspective.

Compliance should not exist to stifle the innovation of your team. Compliance should exist to help generate creative solutions to novel problems.

I recommend this approach if you don't really enjoy punishing people. Although my supremacy is founded on a justified reign of pure terror, and possibly a misinformation campaign about a pit of snakes, it's really much easier to help people find solutions for mistakes rather than to sanction them for making them, especially because eventually people will stop telling you about their mistakes, and then what are you paying for all these snakes for?

### Step 3: Educate others

The foundation of a good compliance program is the information you communicate and the effectiveness with which you communicate it. Using the knowledge and information I gained from my Compliance Academy, my reviews of government tutorials, and other peer-reviewed documents, I revised our privacy policy and our terms of service to be more accessible, specific, transparent, and accurate.

I then reviewed each skeleton policy to be sure that the requirements were met and that they were consistent with regulatory guidelines. Then I revised or rewrote them to add detail and better reflect our practices. I use an online text editor that allows me to track each change, save each iteration of the policy, attach version notes, and alert my team members when a document needed review. This keeps our process auditable, transparent, and collaborative, and it allows our documentation to evolve with us as we grow.

I also wanted to make sure the messaging behind the training was retained, because data protection, privacy, and security are important.

Our full catalogue of policies is now linked, indexed, and searchable by name and regulation number. Each entry includes the date at which the policy was last reviewed and the date of the next revision cycle. The revision cycles are noted on a connected calendar, which contains information about contracts, risk assessments, training periods, and regulatory deadlines.

Now all that was left was to communicate effectively. How hard could it be?

I recalled from my years as a research coordinator at a university hospital how arduous and irrelevant our trainings could seem. Obviously, I didn't want to see people checking out behind their glazing eyes, because it's terrible for my self-esteem, but I also wanted to make sure the messaging behind the training was retained, because data protection, privacy, and security are important.

**Bring it back to basics and stay relevant**

Ethics and law are not the same animal. (I am not a lawyer!) Laws are, however, generally at least tangentially based on moral precepts. When I educate our team about regulations, I make it relevant by distilling the law down to the ethical values and principles the regulation is designed to promote. I use examples from our products and designs to keep the conversation relevant.

Our company culture is built around respect for persons, which makes it easy to embrace and follow policies and regulations designed to protect the security and confidentiality of personal information. Our community understands and values the need for privacy, anonymity, informed consent, and transparency. I used these values to build a culture of compliance and ethics that reflects the beliefs and behaviors of our company reflexively. This makes regulations easy to understand and to follow, and it allows our designers, engineers, and support team members to identify early on in the development process which features will need to be developed in accordance with specific laws, and when they need to ask questions.

A good training program will tell people both what to do and why they should do it. The best ones tell them in a way that they can remember and extrapolate from. Using examples from each employee's workflow to illustrate your points will make the context of the lesson relatable and memorable. Building your summaries on what each individual needs to do helps keep training focused and relevant. It also helps to stimulate more thoughtful and germane questions, because people apply the principles to their own activities.

One of the lessons I took from the Compliance Academy was that a good measure of effective education is an increase in questions. Integrating compliance into the design process helps not only reinforce what rules apply to the process as is, but also helps team members to identify new situations that may require oversight or regulation as they arise. I am always thrilled when team members reach out to me with questions. It means that they are thinking about the impact of their contributions, and being mindful of our company values and policies in all areas of their work.

Building compliance into the development cycle starts by educating all team members about what the rules are and why we follow them, but it also means giving your team members the necessary tools to provide you with the feedback that helps you create effective policy. The more you know about the way your policies are interpreted, the more effectively you can create them.

The more you know about the way your policies are interpreted, the more effectively you can create them.

**Start over**

As our innovative minds continue to outpace the policies designed to regulate them, we will continue to be confronted by new situations, new contexts, and new interpretations. Don't be afraid to hear a question you don't know the answer to. Say that you do not know! Say that you will get back to them! And then find your best variety of peer-reviewed sources; take a look at the examples from your peers; and evolve carefully, ethically, with integrity, and with the utmost respect for persons.

The laws will change. The world will change. Our attitudes about privacy, security, ownership, and alien mind worms will change (trust me on this one). Evolution itself is an iterative process; gradual change over time leads to actionable adaptation to an environment. It is the organism that cannot adapt to change that does not survive. Respond to your environment. Recognize that cultural competence is not a goal to be achieved but a process to maintain. Rewrite your policies in response to the times, and rewrite them again next year. Pay attention to the changing needs of your team members, your audience, and your community. Evaluate yourself, evaluate your context, and keep asking questions like, "What are you going to do with all those snakes?" ✳

1. Department of Health and Human Services: HIPAA Omnibus Rule. 45 CFR Parts 160 and 164. January 25, 2013. Available at https://bit.ly/1UdIxkk.
2. Available at https://bit.ly/2qjBUUW.
3. See https://www.samhsa.gov/.
4. See https://github.com/.