Sese Bennett

A Virtual CISO's Guide to Governance: Know the Why Before You Comply

Sese Bennett is virtual Chief Information Security Officer (CISO) for CereCore. CereCore provides comprehensive IT and application support, technical professional and managed support, IT advisory services, and EHR consulting for healthcare systems.

Anyone who has been in the health care industry for any length of time knows the truth. The compliance professional, while often overlooked, is arguably the most important person in the room. Other departments typically have a more prominent presence. However, without the compliance team at the table, it is nearly impossible to run any operation successfully.

Much like the world of banking, health care has a high standard of compliance to maintain. In fact, a recent AHA report cited that health systems, hospitals, and post-acute care (PAC) providers must comply with 629 discrete regulatory requirements across nine domains.[1] These include 341 hospital-related requirements and 288 PAC-related requirements. The four agencies that enacted these requirements are the Centers for Medicare and Medicaid Services (CMS), the Office of the Inspector General (OIG), the Office for Civil Rights (OCR), and the Office of the National Coordinator (ONC) for Health Information Technology.

Substantial financial support for administrative activities is required for health systems, hospitals, and PAC providers to maintain these regulations. AHA has reported that nearly $39 billion is spent annually.[2] From another perspective, this breaks down to $1,200 every time a patient is admitted. And that's just the administrative cost. Ensuring your organization has adequate staffing to enforce regulations for the various requirements is another beast of its own. The average size hospital dedicates 59 full-time equivalents (FTEs) to regulatory compliance, of which more than a quarter are doctors and nurses.

If you're considering ways to manage the delicate dance of time, money, and resources to maintain a profitable corporate governance strategy, you're not alone.

I have dedicated the past 30+ years of my career to helping individuals and big corporations ideate, develop, and maintain succinct and successful corporate governance plans. Read on to learn four strategies to ensure corporate compliance.

Strategy #1: Know Your Budget and Timeline Upfront

Many health care organizations lack the time and resources to activate a corporate governance plan. It is much more attainable to determine your budget and time constraints at the onset, then use that to guide your strategy and execution. In my experience, teams often run into trouble early on because they have vastly different expectations of what the budget and timeline should be. The C-Suite wants everything expedited, the IT department wants to buy the shiny new thing, and the Compliance team must make sure policies and procedures align with corporate compliance codes. It's easy to see how wires can get crossed.

Here are some tips to support cross-functional teamwork with the organization's best interests in mind. This will help ensure everyone stays on timeline and budget.

- **Identify the goal.** Set your goal, regardless of how you plan to reach it. Are you looking to create a Code of Conduct like MD Anderson did[3] so you can hold employees accountable and uphold the integrity of your organization? Or maybe you want to safeguard patients from disclosure of Protected Health Information (PHI), so you set up a program that issues policies on telephone messages between caregivers and patients in the workplace. Whatever the goal, make sure everyone is on the same page.
- **Recognize the cost.** It is critical to remember that the cost of setting up a corporate governance program will mean different things for different people. Sure, there's the financial cost required for the organization as a whole—but in reality, the time that people are required to give at different intervals throughout the project will vary. The combination of research, ideation, development, revisions, and ongoing education/training is a small price to pay to ensure your patient population receives proper care. Yet it does come at a price. Be prepared.

Strategy #2: Determine Your Leadership Structure

The U.S. Sentencing Commission[4] was created by the U.S. Congress in the 1980s in an effort to establish sentencing standards for the federal court system. In the guidelines, Congress outlines the seven elements of an effective compliance program:

1. Standards and Procedures
2. Governance and Oversight
3. Education and Training
4. Monitoring and Auditing
5. Reporting
6. Internal Enforcement and Discipline
7. Response and Prevention

In order to accurately implement each of these standards in your own organization, you have to determine which leadership structure will be responsible for carrying out the regulations. The hardest task for most organizations is getting your senior or C-suite level executives on board. Their time, like everyone's, is extremely limited. However, without their guidance, you risk putting your team and the program's success at a disadvantage. Determine who is needed from the top and let them know what will be required of them from a timing standpoint.

While titles and roles vary at every organization, best practice is to make sure you have a virtual Chief Information Security Officer (vCISO), CISO, CIO, or some other C-level title in your corner. The next grouping should be made up of mid-level managers. This group is especially important because they will communicate directly with the ground team that is executing the tactics of the program. Staying in lockstep with all levels of the organizational hierarchy will ensure a steady cadence of commitment to the overarching goals and execution of the plan.

Finally, if your leadership team is not meeting regularly to discuss progress, make updates, and mitigate pain points, you should assume this responsibility. The frequency of meetings is far less important than the quality of the conversation and the ability of key stakeholders to attend. Compliance committees vary in size and scope across hospitals and health systems, but they remain the foundation for ensuring the implementation of strong compliance programs.

Strategy #3: Be Aware of Penalties

No one likes to talk about the penalties until their organization is slapped with a major fine for a compliance breach. Save yourself the headache by knowing the rules, regulations, and laws that apply to your practice. Most often we see organizations fail to comply with issues related to patient safety, privacy of PHI, and billing practices.

It's no surprise that HIPAA violations are among the most common acts of noncompliance. HIPAA penalties are based on a tiered system with fines ranging from approximately $100 per violation to more than $63,000 per violation. An example of the penalty structure is shown below.

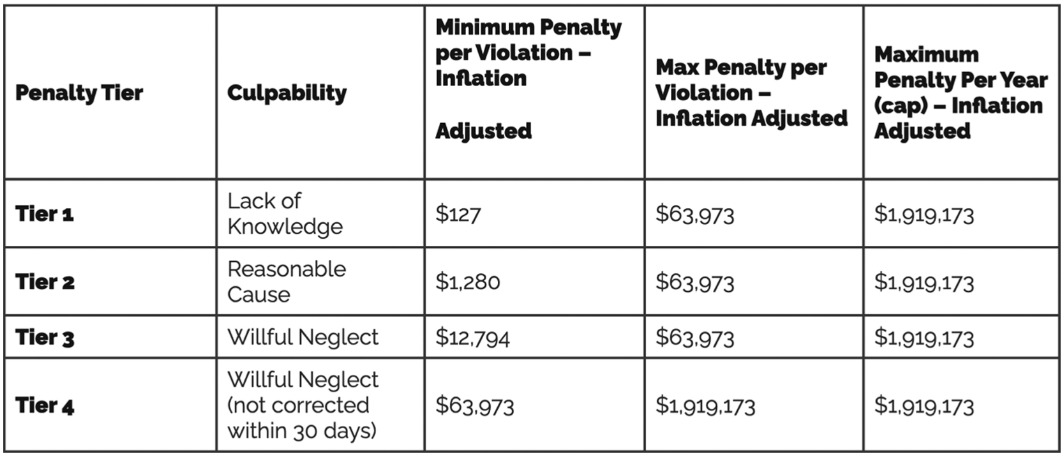
Other examples of noncompliance come into play with federal and state regulations, accreditation standards such as HITRUST, internal policies and procedures, financial requirements, and OSHA standards. While headline news is a constant reminder of the pitfalls that companies succumb to when they have a breach or lapse in judgment, it bears repeating—compliance is a team sport and it's not a matter of *if* something will happen, but *when*.

Conclusion

A compliance plan that sets realistic expectations for budget and timeline, with leadership structure in place, provides your team with a plan to meet compliance objectives. In addition, staying aware of penalties helps prevent the organization from making costly mistakes. As cybersecurity threats prevail within the health care industry, a well-thought-out compliance strategy enables your organization to meet health care's strict compliance standards without breaking the bank.

Endnotes

1. AHA, Regulatory Overload Report, available at *https://www.aha.org/guidesreports/2017-11-03-regulatory-overload-report*.
2. AHA, Regulatory Overload Report, available at *https://www.aha.org/guidesreports/2017-11-03-regulatory-overload-report*.



Penalty Tier	Culpability	Minimum Penalty per Violation – Inflation Adjusted	Max Penalty per Violation – Inflation Adjusted	Maximum Penalty Per Year (cap) – Inflation Adjusted
Tier 1	Lack of Knowledge	$127	$63,973	$1,919,173
Tier 2	Reasonable Cause	$1,280	$63,973	$1,919,173
Tier 3	Willful Neglect	$12,794	$63,973	$1,919,173
Tier 4	Willful Neglect (not corrected within 30 days)	$63,973	$1,919,173	$1,919,173

Source: *https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/*

3. MD Anderson's Standards of Conduct, "Do the Right Thing," available at *https://www.mdanderson.org/content/dam/mdanderson/documents/about-md-anderson/about-us/compliance-program/do-the-right-thing.pdf*.
4. *https://www.ussc.gov/*.

Reprinted from Journal of Health Care Compliance, Volume 25, Number 4, July–August 2023,
pages 41–44, with permission from CCH and Wolters Kluwer.
For permission to reprint, e-mail permissions@cch.com.