Five Essential Capabilities of Healthcare Board ECRM

1. Establish Appropriate Governance

With respect to ECRM governance, the role of the board is to set direction and provide ongoing oversight. In other words, the board establishes and communicates, “This is where we are going (with respect to ECRM), and this is why we are going there.” C-suite executives and their teams are then responsible for execution.

2. Resource Skilled People

The success of any business program or initiative requires employing the right number of people with the right skills, knowledge, experience, and passion about the subject matter. Fitting your ECRM program with the right number of people often requires organizations to leverage a combination of internal and external resources. Leveraging internal resources includes not only hiring skilled ECRM staff but also creating a risk-aware culture throughout your organization. In addition, part of your leadership responsibility as board members is to build understanding of the value and benefits of your ECRM program in order to justify the resources allocated to support it.

3. Adopt Industry-Standard Processes

At the most basic level, a process is a specific way of doing something. Organizations with a mature ECRM process have formal, well-documented, and consistently followed policies, procedures, and practices for risk management. These policies and procedures help ensure a risk management process that is predictable, measurable, and controlled, and which aligns with the principles of continuous process improvement (CPI). As with other core capabilities, healthcare organizations can benefit by referencing standards-based guidance on cyber risk management processes.

4. Employ Relevant Technology

Nearly all healthcare industry organizations already employ technology tools and automation to streamline clinical, administrative, and operational processes. Technology tools can also enable ECRM workflows and efficiency. More importantly, technology tools are essential for the scalability of your ECRM program.

It is simply not possible to complete—and maintain—an adequate risk analysis without using an appropriate technology and automation solution. And since the results of your risk analysis serve as the foundation for your ECRM strategy, it is critical to have the right ECRM technology solution in place. That means using standards-based technology. The advantage of using standards-based technology is that standards (such as the NIST Framework) have been developed, vetted, and successfully deployed across multiple organizations in multiple industries. Standards-based technology delivers consistent, predictable, repeatable, and measurable results, with the added benefit of explicit recognition (in the case of NIST) by the U.S. Department of Health and Human Services Office for Civil Rights (HHS/OCR) as a valid approach to ECRM. (OCR is the agency tasked with enforcing the HIPAA Privacy, Security, and Breach Notification Rules).

5. Ensure Organizational Engagement

The success of your ECRM program depends on the extent to which the entire organization is actively engaged in ECRM. Everyone in your organization has a role to play in your program. Even if your board and C-suite are providing appropriate leadership and oversight, if your organization’s other executives, managers, and workforce members are not engaged in your ECRM program, it will fail. Without engagement and ownership of risks by line-of-business, process, and functional leaders, risk-related decisions will be made by people without the full strategic business view. This is why engagement is so critical.