CAH LEADERSHIP:
THE INTERSECTION
OF GOVERNANCE
AND MANAGEMENT

BUSINESS INTELLIGENCE FOR CAHS:
MOTIVATING, INNOVATING
AND COLLABORATING YOUR
WAY TO OPERATIONAL
INTELLIGENCE

DEVELOPING
AN IT/DATA
SECURITY
STRATEGY

OUTSOURCED
REVENUE CYCLE
MANAGEMENT
Greetings,
Since your hospital is the heart of your community, it significantly impacts the wellness of your local economy. Working with rural providers for more than 50 years, we understand the magnitude of this responsibility.

In this edition of Community & Care Insights, we offer ideas to help you enhance your hospital’s financial and operational viability and begin to plan for conversion.

• As you’ve recently read in the news, the health care industry is increasingly threatened by multiple forms of cybersecurity attacks. On page 4, Eric Pulse shares a data security framework you can use at your CAH in developing a comprehensive data security strategy to help ensure your organization and its data is properly protected and prepared to respond to and recover from these complex privacy risks.

• On page 6, Rhonda Quast discusses the importance of carefully evaluating and conducting due diligence when outsourcing or co-sourcing management of your revenue cycle.

• Next, Paul Schulz shares the business intelligence process of motivating, innovating and collaborating to drive data-driven decision making—ultimately resulting in an operationally intelligent organization.

• Finally, Adam Strom explains how leadership intersects governance and management. He clarifies these roles, helping you to understand the differences and overlap between them to ensure all functions are effectively communicating and optimally working together on the new business of health care for your community.

Hopefully you’ll find these articles valuable—generating ideas on how to apply them to your operations. We welcome a dialogue, so please don’t hesitate to contact me or the authors with your questions or comments.

Stay In Touch,
Ralph Llewellyn, CPA, CHFP
Director of Critical Access Hospitals

Managing Complex Risk: 4
Developing an IT/Data Security Strategy
Eric Pulse, CISA, CISM, CRISC, GSEC, CFSA

Outsourced Revenue: 6
Cycle Management: Finding the Best Solutions to Inject Revenues Into Your CAH
Rhonda Quast, LPN

Business Intelligence for CAHs: 8
Motivating, Innovating and Collaborating Your Way to Operational Intelligence
Paul Schulz

CAH Leadership: 10
The Intersection of Governance and Management
Adam Strom, MBA

Contact Information
Eide Bailly LLP
US Bancorp Center
800 Nicollet Mall
Ste. 1300
Minneapolis, MN 55402
800.280.0354
www.eidebailly.com/CAH

Who We Are
As the nation’s rural hospitals began converting to critical access hospitals, Eide Bailly was there. Since 1998, we have worked alongside more than 250 critical access hospitals to define and measure governmental and third-party rules and regulations. We understand what it is like to operate a health care entity in a rural setting, and we develop an approach that recognizes and appreciates the uniqueness of rural America.

Learn more at www.eidebailly.com/CAH.
Eric Pulse, CISA, CISM, CRISC, GSEC, CFSA | Principal, Director of Risk Advisory Services

Eric Pulse is a principal at Eide Bailly and has nearly 20 years of experience as a consultant in the IT industry. He has worked in a multitude of industries, including health care, throughout his career. As Director of Risk Advisory Services, Eric provides leadership in developing and enhancing information technology risk advisory and security consulting practice for people, processes, methodologies and growth. He has experience performing IT audit and control reviews, service organization control reports, third-party IT audits, HIPAA security, and PCID Data Security Standard Compliance assessments. He has performed comprehensive assessments of external and internal computer systems and networks to determine security features and capabilities and to identify potential security system vulnerabilities.

605.977.4847 | epulse@eidebailly.com

Adam Strom, MBA | Health Care Consulting Manager

Adam has more than 10 years of health care experience in nonprofit, government and consulting capacities. He is skilled in governance, organization and leadership redesign and has executive leadership experience in clinical settings. Adam performs strategic market demand analyses for inpatient and outpatient providers to assist management in making strategy and planning decisions. In addition, he assists organizations in implementing Lean and Six Sigma performance improvement initiatives.

612.253.6606 | astrom@eidebailly.com
With increasing demands to deliver higher quality care and lower costs, it is easy to forget about the risks your organization faces while trying to protect patient information. The recent ransomware breach event at Hollywood Presbyterian Medical Center, as well as several other data breaches in the health care industry, serves as a high profile reminder of the importance of IT security in health care.

What are the risks?
Privacy risks in the health care industry are more challenging than ever. Every day we seem to hear about another incident that threatens to undermine the reputation of health care providers. Common threats include:

- Malware – attackers use software that is intended to damage, disable, or worse, compromise systems
- Data Leakage – attackers utilize weaknesses in an organization’s technology to capture data “leaking” from their environments
- Ransomware – hackers hold your data “hostage” and demand payment for providing you access to your own data
- Phishing Attacks – fraudulent emails are used to try to trick users into providing login credentials or account information to systems containing sensitive information
- Denial of Service Attacks – attackers frequently use a high volume of traffic to disrupt access to key network services
- Lack of Overall Security Strategy – the lack of an organizational security strategy leaves employees oblivious to many threats facing the organization

Considerations for a data security strategy
In order to develop a comprehensive data security strategy in today’s environment, you need to follow a common framework. The National Institute of Standards and Technology (NIST) recently released its Cybersecurity Framework* that provides straight-forward guidance and a risk-based approach to managing data and cybersecurity risks.

The fundamentals of a security strategy should support critical functions, from a business context, and related security risks and enable the organization to focus and prioritize efforts consistent with its business needs and objectives.

Going it alone can be a frustrating endeavor. Many organizations that attempt to build a security strategy “from scratch” often find themselves bound in minutia, as opposed to taking a more macro view of the risks presented, and controls in place to mitigate those risks. Fortunately, the framework provides a set of activities to achieve specific cybersecurity outcomes and provides examples of guidance to achieve those outcomes. The framework presents key cybersecurity outcomes identified by industry as helpful in managing cybersecurity risk.
Some key considerations include:

- Develop an organizational understanding to manage security risk to systems, assets, data and capabilities. This includes the identification and classification of critical data and identification of supporting applications, systems and locations of that data.
- Assess risks, threats and vulnerabilities that could impact critical data.
- Identify mitigating controls that protect data from risks, threats and vulnerabilities. These controls include the administrative, physical and technical safeguards in place throughout the organization.
- Develop and implement appropriate activities to identify the occurrence of a security event.
- Develop and implement activities to take action regarding a detected event.
- Develop and implement activities to restore capabilities or services impaired due to an event.
- Regularly test controls.

**What's next?**

Once an organization has developed a process of how to identify and protect critical data, as well as detect, respond to, and recover from a security event, it is important to create an understanding of and process to monitor critical functions that support the core aspects of a security strategy. There are several key categories to consider when developing the strategy.

**Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Identification considerations include:

- **Asset Management** - The data, personnel, devices, systems and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.
- **Business Environment** - The organization’s mission, objectives, stakeholders and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities and risk management decisions.
- **Governance** - The policies, procedures and processes to manage and monitor the organization’s regulatory, legal, risk, environmental and operational requirements are understood and inform the management of cybersecurity risk.
- **Risk Assessment** - The organization understands the cybersecurity risk to organizational operations (including mission, functions, image or reputation), organizational assets and individuals.
- **Risk Management Strategy** - The organization’s priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions.

**Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services and to support the ability to limit or contain the impact of a potential cybersecurity event.

Protection considerations include:

- **Access Control** - Access to assets and associated facilities is limited to authorized users, processes or devices, and to authorized activities and transactions.
- **Awareness and Training** - The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures and agreements.
- **Data Security** - Information and records (data) are managed consistently with the organization’s risk strategy to protect the confidentiality, integrity and availability of information.
- **Information Protection Processes and Procedures** - Security policies (that address purpose, scope, roles, responsibilities, management commitment and coordination among organizational entities), processes and procedures are maintained and used to manage protection of information systems and assets.
- **Maintenance** - Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
- **Protective Technology** - Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures and agreements.

**Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Detection considerations include:

- **Anomalies and Events** - Anomalous activity is detected in a timely manner and the potential impact of events is understood.
- **Security Continuous Monitoring** - The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
- **Detection Processes** - Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

**Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event and to enhance the ability to contain the impact of a potential cybersecurity event.

Responsive considerations include:

- **Response Planning** - Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
- **Communications** - Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
- **Analysis** - Analysis is conducted to ensure adequate response and support recovery activities.

*Managing Complex Risk Continues on Page 12*
If you are like many critical access hospitals (CAHs), you are strongly considering outsourcing your Revenue Cycle Management (RCM) for solid economic reasons. What we find, however, in our work consulting with CAH management and boards, is that the promises of what outsourcing RCM will do for you, overshadow the things you need to be considering when evaluating and managing a RCM vendor. The biggest thing to keep in mind is that when you outsource, you lose control over the processes; but you retain sole legal responsibility for your RCM. That means due diligence is extremely important.

Why is outsourcing so attractive right now?
As Health Care Reform changes reimbursement from fee-for-service to value-based payment structures, it has become increasingly difficult to maintain efficiencies in RCM, educate staff on reimbursement changes and achieve optimal reimbursement rates. These changes, coupled with the revenue cycle staff shortages that many CAHs across the country are experiencing, makes the option of outsourcing RCM more appealing.

As you examine the available RCM options, determining the best option for your organization may seem daunting. Contracts can be ambiguous and the use of third-party quality control metrics are typically not addressed. If you are feeling nervous about this decision-making process, you are not alone.

The majority of health care organizations recognize the need for assistance in navigating the options and finding the best solution for them. According to the Black Book™ Market Research survey on RCM:

- 83 percent of hospitals under 100 beds are pursuing RCM outsourcing due to staffing concerns and shortages
- 62 percent of small and community hospitals are considering using a consultant in their determination of a RCM solution, but 83 percent have reported difficulty securing RCM consulting engagements due to demand
- 80 percent of CFOs feel the pressure to make a decision regarding a RCM is actually a threat to their job stability
- 87 percent of small and community hospitals anticipate declining to negative profitability due to diminishing reimbursements, uncovered collections and underutilized or inefficient billing and records technology

Why it is so important to find the right vendor
Selecting the right vendor requires due diligence and managing expectations to ensure integrity, experience and compliance with billing rules and regulations. Whether you’re interested in outsourcing or co-sourcing (outsourcing some elements), you need to carefully review each vendor, rate them against your required criteria and provide insights and recommendations to ensure you will be capturing the full value for services rendered.

Here are some things to consider:
Advantages of outsourcing or co-sourcing:
- Access to trained revenue cycle personnel
- Economies of scale
- Alleviate overhead of hiring full-time staff to provide relief to your bottom-line
• Train-the-trainer—educating your staff along the way in a co-sourced arrangement
• Your staff will have more time to focus on the myriad of other revenue cycle project demands

Disadvantages of outsourcing or co-sourcing:
• Cost – long-term cost of outsourcing is greater than the short-term investment of updating current RCM software and education of staff
• Quality – few quality control metrics typically exist in agreements from outside, third-party consultants
• Control – outsourcing causes a potential loss of control of RCM operations due to the lack of ability to customize technology or processes to fit your organization’s practices
• Lack of local support – patients often express dissatisfaction regarding the lack of local availability they have come to appreciate in their community CAH

What often gets missed?
• Accountability: Contracts often do not define the resources which will be solely dedicated to your organization. During the first couple months, most vendors will give you a large amount of attention and provide ample reports. However, many CAHs don’t have the volume to sustain that level of attention and vendors often focus most of their resources on their “biggest” clients. Be sure you know the resources that will be dedicated to you.
• Pricing: We often find that pricing is variable, and vendors are paid by how much they collect. Often, the vendor will focus their resources on easy collections and reimbursements and not pursue all of your collections, leaving money on the table. Variable pricing also makes it hard to budget from month-to-month.
• Denials management: Pursuing appeals of denials require increased staff costs and expertise to be dedicated to your organization by the outsourced RCM. Many times these costs may be higher than the rate of compensation according to the contract. For this reason, some of our clients have experienced that their denials are being written off rather than appealed. This results in lost revenue for your organization.
• Vendor performance: It’s hard to know how a vendor is doing if you don’t take time to audit their work. Most CAHs do not have the staff to conduct independent reviews of vendor performance on a monthly or quarterly basis to make sure the figures match up and you are getting maximum reimbursement. A consultant can assist you with this.

Obtain an Independent Vendor Review
If you are considering a vendor, a consultant can help you perform due diligence and evaluate which vendor would be the best fit for you. If you already have a vendor, a consultant can help you evaluate their performance on a regular basis. It’s important to ensure you hire the right vendor, and that you get all the reimbursement you should be getting, as your organization’s viability often depends on it.

To learn more about selecting or evaluating a vendor, please contact Rhonda Quast at 701.476.8360 or rquast@eidebailly.com.
With the advent of Big Data, and health care reform driving organizations to be more efficient and cost effective, business intelligence (BI) has become an increasingly popular way to harness the power of data analytics and process improvement. Coupling BI to process improvement helps organizations migrate toward operational intelligence, setting the stage for change. Once the stage is set, effective change can happen.

Business Intelligence is developing a process that transforms operational data into actionable information to help facilitate better decisions for front-line change. It helps staff become more intelligent about the data they are seeing and using. Most Critical Access Hospital (CAH) management and governing boards would agree that operational data is necessary in today’s environment. Getting to the next level of this discussion, however, is a bit more complicated. A conversation around motivation, innovation and collaboration may be helpful.

Finding the motivation to change

Most payer models are shifting toward rewarding value over volume. When management discusses a paradigm shift, the change to create a value model compared to volume is a massive shift; and, in some cases may become difficult for CAHs to adjust. This is where the future of care (which is increasingly evolving to retail) will become a bigger challenge for health providers as consumers are offered more choices.

With many reasons to change and adjust how CAHs deliver care, why does it seem so hard to find the motivation to change? One of the reasons may be the complexity of systems. Change one thing and it can have a domino effect that creates doubt—and, in some minds, risk. “Can we do this? If we change this one area, it will change everything – I’m not sure we can handle that?” These can be some of the questions creating doubt.

The cause and effect of change has become so burdensome and expensive that it has given staff pause on the motivational side of the equation. So how do organizations address this? Courage. They have to find the courage to forge ahead. If they look for it, they can find it right where they are. More importantly, when discovered, it reminds staff that what is needed is right in their backyard. Fear contributes to organizations losing sight of what can be harnessed to solve problems. However, gathering information from organizational support systems, rallying staff and those in the community that they serve, can help shift attitudes to embrace change and overcome challenges.

The second thought to consider is how data can be motivational. Data can help organizations understand that there is great opportunity in some area of the service, or resources being consumed to provide care. When leaders see the dollars that could be saved, or how changes could help make nurses’ lives easier by tweaking processes, which translates to better patient care—that’s exciting! Again, the barrier in embracing this opportunity is often the complexity of systems. However, the abundance of data coming from a plethora of sources can be extremely useful. Please note that using data that staff can trust is a logical path. Data from an accurate and repeatable source is key to inspiring innovation.

Another option is to look at data through a tool that can pull from multiple sources. Today’s BI tools are making data visualizations more available and affordable for organizations trying to present opportunities from a spectrum of databases.

Why does presentation matter? Brains, hearts and souls operate differently as information is presented and consumed. Minds tell us...
literally that this number is a number, but hearts put emotion into
the message allowing context and depth. BI offers the correlative
functionality, which can help motivate audiences to ask questions,
moves beyond the data, and into the next very important stage:
innovation. This is where organizations need to understand how
important it is to look inside. If organizations review the data
gathered to make smart decisions about how to move forward,
the team can become more operationally intelligent. Operational
intelligence is an investment growing and matching human capital
with data available in the organization.

Innovation can be a wellspring of positive change
Innovation in health care slightly lags other industries, but advances
are occurring. When data can motivate, and staff want to innovate,
a great way to capture that energy is by leveraging the tool sets
garnered over the last decade that come from learning and doing
process improvement.

Innovation is creating a different future state. Data is most likely
the output of the current state (current processes), and when that
motivates staff to be innovative, those ideas can be modeled into
future state pictures. This is where improvement teams have grown
and migrated inside organizations that have spent a great deal of
energy removing waste and improving care processes. The skill
sets of project management, process design (flow charting), and
working with teams to implement changes are wonderful attributes
to give innovation launching pads into operations. A colleague once
told me that ideas without action are worthless, and ideas without
data are risky. In the wake of health care reform, that statement can
ring true. In light of current health care challenges, squandering
innovation due to lack of system data, understanding, or courage
to explore it can result in opportunities lost. However, innovation
needs collaboration to be most effective.

Collaboration takes human beings
Health care is a service industry whose HR budgets consume a
large percentage of resources. To overlook collaboration is to ignore
a significant amount of investment. If leadership ignores this aspect
and wonder why ideas are not gaining traction, tie it back to the
investment the organization has made in human capital. It’s about
people. Pulling data and presenting it can generate great ideas, but
if people don’t engage, it won’t work. This also includes patients
and the community health care organizations serve.

As a result, what can you do?
• Review data from systems (what reports are useful? What kind
  of reporting would be better?)
• Understand the data sources
• Ask: how can you expand the context of that data?
• Develop a process that transforms operational data into
  actionable information to facilitate better decisions for front
  line change
• Remember—nothing ventured, nothing gained

There are numerous reasons to change and improve operations,
unfortunately, the risk-free, tried-and-true options are limited.
That’s the dilemma organizations are facing. However, looking
inside and leveraging data currently in place, is a way forward.
Dive into your data, explore and learn what you can from your
reports. Work with your staff to correlate the data to strategic
objectives. Coupling the data with BI tools can help engage your
staff and allow innovation to find its path into your organization.

If you have questions about leveraging business intelligence, please
contact Paul Schulz at 701.239.8591 or pschulz@eidebailly.com.
CAH Leadership: The Intersection of Governance and Management

By: Adam Strom, MBA

If you are like many CAH boards, you spend the majority of your time focused on finances and physician recruitment. You know there are huge pressures facing an industry in tumultuous change; big issues like quality metrics, patient experience, determining where your organization falls into care coordination, and many others. You know this, but there’s limited time to address these things. If you’re a CEO, these issues are also top of mind and yet, the board doesn’t seem to be willing to hear your ideas on how to proceed. Board member or CEO – you have a sinking suspicion that no matter how hard you seem to be trying, you’re still somehow missing something that feels really important. You are.

Before we discuss how to get everyone focused on these matters, we’re going to talk about what really matters: care coordination and care management. That’s right. Care coordination refers to clinical guidelines (and clinical practice consistent with those guidelines) that address how individuals with certain diagnoses should move through the continuum of care, with a particular focus on communication among providers and facilities regarding the patient’s condition and treatment. Care management focuses on bringing needed resources to the patient.

Care coordination and care management are the new business of health care. Gone are the days when you were the only hospital or provider for patients to turn to. You may still be the only local hospital, but consolidation and efficiency mandates that CAHs coordinate care with other tertiary facilities and providers. So, your primary role – board member or management – is bearing the responsibility for effective, efficient care coordination and care management that creates a high quality patient care experience and results, ultimately, in helping the patient return to his or her desirable state of health. This is why you exist in your community today.

So, how do you get boards and management focused on this? It starts with clarifying the roles and responsibilities of governance (boards) and management. Go back to basics and figure out who should be doing what. Unless boards and management effectively own their roles and responsibilities, you will not be able to focus on what really matters.

First, let’s define leadership.

Leadership is the act of owning the responsibility to make decisions, being held accountable for your decisions, the outcomes of your decisions, and the actions of those you are responsible for. Both boards and management provide leadership.

Boards and CEOs – Who does what?
Determining the future vision is among the most important responsibilities and characteristics of organizational boards. Board vision should influence daily management and decision making. This is an example of an intersection, and there are others. Before proceeding, take a look at things that are distinct to the board (governance) and management functions:
In summary, the board focuses on governance, strategy and desired future market position. This has to take into account all of the big issues we mentioned earlier, as well as finances and physician recruiting. Management focuses on processes that support board policies and managing the organization to deliver quality and cost-effective care. Board vision ranks at the top along with overall responsibility for quality, care and organizational success, and needs to be brought to fruition with clear and effective board policies. The CEO will likely advise in their creation, but the board is tasked with creating, organizing and directing policies by delineating them into one of four categories:

1. **Ultimate Organizational Outcomes**
   - Establish/update the organization’s mission and vision statements
   - Focus mainly on intended long-term organizational impacts
   - Avoid directing programmatic or procedural methods of reaching these desired outcomes

2. **Board Role. Establish:**
   - The organizational charter (purpose)
   - The board’s role as serving the owners/stakeholders
   - The way in which the board will ensure strong committee performance
   - Performance expectations for board members and the board as a whole
   - How/when the board monitors its performance

3. **Board Dynamics With Staff.** The board does not involve itself with the staff, except when:
   - Ensuring the staff is producing what they are there to produce
   - Ensuring staff is not violating what is ethical and prudent

4. **CEO and Leadership Supervision**
   - Establish CEO job description and conduct annual performance reviews
   - Correlate principal CEO and leadership responsibilities with the ultimate organizational outcomes as described in (1) above
   - Take ownership in CEO succession planning

In looking at areas where board and CEO responsibilities are overlapping, let’s first identify two where there is limited or no overlap. First, selecting, hiring and evaluating the CEO is exclusively the responsibility of the board. Second, evaluating individual board member performance and the board’s performance as a whole will involve the CEO, but primarily through process management.

The primary, mutually shared responsibility of a board and management is high quality, safe patient access, care coordination and care management. The board needs to be responsible for quality of care, while the CEO ensures the organization manages and delivers as directed. This involves recruiting and retention, decision making, working with and supervising all staff, and ensuring quality systems and standards are in place and working. Additional, mutual areas of overlap or shared responsibility are financial sustainability, community service (especially in the case of 501(c)(3) tax-exempt, not-for-profit entities), and ethical behavior. The board provides financial oversight and protection of assets while the CEO implements financial policy and oversees financial management.

Mission, vision and values (culture) lie in the leadership intersection as well. While the board develops mission and vision statements and the appropriate policies, the CEO is primarily responsible for communicating these statements and managing in a way that achieves them. In terms of strategic planning, the board is responsible for the planning process and creating the actual plan. The CEO likely coordinates the planning process and ensures that it is implemented and designates who is responsible for the timetable of each element within. On legal and regulatory compliance, this needs to be the overall responsibility of the board, but also adhered to in the daily management and decision making of the CEO. Lastly, both board and CEO can serve as public liaisons, but the board would focus on matters of policy and the CEO takes the lead on areas relating to program and service delivery.

**The increasing weight of responsibility**

Boards need to be aware of the growing attention the federal government is paying to CAHs, ensuring they are held accountable for their fiduciary responsibilities. The Department of Justice has prosecuted CAH board members for fraud by management for lack of fiduciary oversight—so this is something that boards need to take very seriously. CAHs often have trouble finding experienced, qualified board members who understand the health care industry and the responsibility required for the position. While in many rural areas, board members are often local business owners, it may be prudent to look outside your local community for health care professionals who may be willing to serve on your board and meet with you via video conferencing, etc. Having the right people in all areas of leadership is necessary to ensure a successful future.

Now is the time to get clear on the roles and responsibilities of everyone involved in leadership and to have open, humble, brave discussions about what needs to change. If you need help facilitating this, independent consultants can help you address these issues.

Questions? Please contact Adam Strom at 612.253.6606 or astrom@eidebailey.com.
Mitigation - Activities are performed to prevent expansion of an event, mitigate its effects and eradicate the incident.

Improvements - Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event, which will support timely recovery to normal operations to reduce the impact from a cybersecurity event.

Recovery considerations include:

- Recovery Planning - Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
- Improvements - Recovery planning and processes are improved by incorporating lessons learned into future activities.
- Communications - Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other Computer Security Incident Response Teams (CSIRTs) and vendors.

Conclusion

Developing an organizational security strategy can be a daunting task. Many organizations have addressed organizational and data risk at some level, even if only conceptually. Unfortunately, a high-level and undocumented approach to securing critical data, including ePHI, is not effective. The process requires peeling back layers to understand where data rests, how it is transmitted and protected, how potential anomalies and threats are detected, and how the organization is able to respond to and recover from a potential incident.

Eide Bailly has a proven approach for assisting CAH organizations who desire assistance with creating an overall data security strategy based on an accepted framework.

Questions? Please contact Eric Pulse at 605.977.4847 or epulse@eidebailly.com.