Next Generation Patient Safety in Healthcare

From an Executive Perspective

Dr. Bertine Colombo McKenna
Executive Healthcare Advisor

GreyCastle security

500 Federal Street
Troy, NY 12180
(800) 803-4350

www.greycastlesecurity.com
intel@greycastlesecurity.com

GreyCastle security

1. The New Era of Cybercrime

Healthcare has had many cyberattacks in the last year. Making this a top safety issue in a healthcare organization is challenging – a challenge that executives must make a top priority. The 2018 Environmental Scan, released by the American Healthcare Association, was a reminder of the complicated business that healthcare represents. When developing new innovative programs to serve our patients and competing in an ever-complicated environment, we don't often stop for a minute and ask "are we protecting our patients' privacy thoroughly?" Unlike any other business, healthcare leaders go to work every day with the knowledge that they have the ability to protect and enhance lives and unintentionally hurt them as well. This white paper is directed at the fundamentals that must be undertaken in the healthcare environment to protect the organization and its patients from cybercrime.

2. Healthcare's Challenge with this Patient Safety Issue

For the first time in history, cybersecurity has become a life or death issue. No healthcare organization is immune to today's threat landscape. According to a recent study done by the Ponemon Institute, data breaches have cost healthcare organizations $6.2 billion with the average electronic health record (EHR) costing $355.

In the high paced world of healthcare where every day represents a new modality, a new technology, a new system of care, a new political worry, we have to make sure that we are protecting patient privacy. Imagine, if you will, a situation where a healthcare organization is developing its population health plan. In the thousands of steps necessary, is cybersecurity part of the planning? As we plan to ensure that information is shared for coordination of care, are we stopping to say, "can we protect their identity?" In population health efforts, are we asking partners if they are taking proactive cybersecurity measures? When the latest innovative monitoring system becomes available, are we asking if the manufacturer has built-in protection from cyberattacks before we buy it? In developing telemedicine programs, are we asking question about privacy and cybersecurity as we develop these programs? In the latest news article about Amazon, JP Morgan and Berkshire Hathaway's announcement about developing

healthcare programs causes me to wonder, how this will impact privacy and cybersecurity? Renewed focus on Telemedicine programs should be coupled with a full assessment of how patient privacy can be protected

Recall, when patient safety began to be part of our conversation, years ago, it became part of how we developed new programs, ensuring potential safety hazards were evaluated and mitigated preprogram startup. When quality became a key component of healthcare program planning, we built in quality measures by which to evaluate the program and held them as important as financial measurements. Are we doing this in the new era of cybercrime?

Envision the benefits and opportunities this problem creates. Not only can your organization be the leader in this space, you can achieve immediate financial savings by implementing proactive cybersecurity measures, comply with various regulations such as the Health Insurance Portability and Accountability Act (HIPAA), establish a competitive advantage by becoming the preferred healthcare solutions provider, but also ensure the protection of your patients' safety and well-being.

3. The New Approach to Patient Safety

How do we begin to protect our patients as we develop new ideas, programs, systems of care, and digital solutions?

Most articles and white papers on this topic are focused on the information technology and assessment solutions that are currently thought to be the best practice. However, as a former healthcare executive and a current consultant, I am struck by the fact that this needs to be approached in a very different way.

As I study the solutions that many organizations are using, it focuses on how the current information system can be strengthened with information technology and the ways in which one can assess their systems.

I do not have an information technology (IT) background, as I am a former healthcare executive who served as Chief Operating Officer (COO), and therefore, this whitepaper is not focused on IT solutions, antivirus or firewalls. It is directed at specifically what

healthcare organizations' leadership team should be doing right away from an insider's view. Too many times I have read about solutions from those who have not had the opportunity to be inside a complex whirling healthcare organization to know where to focus cybersecurity efforts for the betterment of safety and patient care, I bring that perspective.

It is my view that a very different approach should be taken. I would suggest the following hypothesis:

Every day, healthcare organizations accept responsibility for patients who entrust their lives and information to us. In a very organic way, we accept it and "bubble wrap" that responsibility with numerous approaches to safety. Part of the paradigm shift in patient safety planning should be the organization's thorough review and protection of patient privacy and protection against cybercrime. This should be something we share with patients as we do our other safety efforts.

Given the fact that healthcare culture shifts occur only with the focused attention, I am positing that the following should occur:

1. Align the healthcare provider with cybersecurity experts and innovators.
2. Perform all the actions suggested by the experts – including a comprehensive assessment to determine your sensitive risk areas and your risk tolerance, create policies that will protect your patients, train your staff, educate your employees, etc.
3. Appoint a leader with only this responsibility who reports to the Chief Operating Officer or the Chief Quality Officer. This will sound edgy to many organizations, but in fact it is both a quality issue (consider hacking of medical devices), a safety issue (consider shut down of medical record system) and finally an operational issue (consider the most important factor in protecting patients by changing their approaches to technology and information).
4. Develop a routine tabletop exercise with clinicians and others to not only outline what should be done but to educate those folks. If drills are being done by IT, this will not change the culture, nor does it involve the actual people who will be involved when a breach occurs.
5. Routinely test downtime procedures for the potential of medical information not being available (certainly a drill where the staff is unknowingly unable to access medical information can be dangerous but creates an amazing learning

environment). I would recommend this be done with actual fake patients who perhaps suffer from a machine malfunctioning due to a cyberattack.

6. Implement a corrective action plan (CAP) from each tabletop exercise and training sessions to be taken to enhance the process. Assume your CAP is dynamic and organic in its development. Ensure you have the following categories in the CAP:
    a. Culture shifts required by department
    b. Employee education needs
    c. Insurance coverage assessment
    d. Safety rounds question additions
    e. Cybersecurity Council actions needed
    f. Policy enhancements
    g. Vendor risk assessments
    h. Added assessments to be done
    i. New education opportunities by department and job classification
7. Create a sense of urgency that cybersecurity is everyone's job every day.
8. Establish a cybersecurity reporting system where employees (much like patient incident reports) can report situations where they can see a problem exists.
9. Have secret shoppers try to access information they should not or even to try and hack into a system. This is known as a penetration test.
10. Do walk arounds and test how many times you gain access to health information and access you should not have as a leader.
11. Develop "town halls" where employees can hear recent "near misses" (a common approach with safety programs which will move them to change their own practices).

In establishing these types of actions, cybersecurity slowly, but surely, becomes something each person in a healthcare environment thinks about as they are working. This state is the place your organization should be. The place where someone in healthcare doing their work, recognizes a cybersecurity risk/vulnerability/threat and either corrects it and/or brings awareness. Only in this way can healthcare indeed make it safer for patients who entrust us with their information and their lives.

Recently, the articles I have been reading are focused on medical device hacking with the expansion of the Internet of Things (IoT). Even though the reality of this possibility is frightening, it has not yet happened and, although this would be the time to plan and prepare, healthcare is encumbered by so many other priorities that it has not made its way into the consciousness. Here is where a real-life drill would be key – to point out the

possibility but also to engage the clinicians in what they should do next. Remember, clinicians and employees at all levels in healthcare are trained for emergencies, fires, infection, code blues – they understand this is a reality. Building on this reality for cybersecurity issues is key. Currently, healthcare workers, without a doubt, view this as "someone else's" job and not theirs, much like safety was viewed before the Institute of Medicine (IOM) report came out. This is the 21st century's largest safety issue, whether healthcare employees see it or not.

4. Conclusion

This is not your grandfather's white paper, I am suggesting that healthcare executives are not paying full attention nor putting their attention in the right places. Instead, they may be "hoping" that the Chief Information Officer (CIO) is handling this issue. However, hope cannot be the strategy here. We are missing an opportunity to ensure that we are ahead of this curve like every other curve we have had to be ahead of. Cybersecurity is not an IT issue – it is an operational issue focused on patient safety. It is a safety hazard requiring full attention and innovative solutions. You cannot do this alone – you must have expert help from firms who specialize in creating and deploying a tailored cybersecurity program development for your organization. There are not many out there, I consult for one.

So, for those of you in healthcare who, like me, read the last page only and look for a summary and a few takeaway points:

1. Partner with a cybersecurity firm who has an innovative approach to the complicated problem.
2. Appoint one person whose only job is to do this (not part of their regular job). I would recommend it not be an IT person. They must have expert help from an outside company (like risk management has from a legal firm). They can get IT help inside. They should report to the COO or Chief Quality Officer.
3. Create educational teaching moments by telling real-life stories of patients being compromised. Require all employees to attend – do not tell them IT stories, tell them patient stories. Include a "what if" about technology hacking – make them feel it in their gut.

4. Do routine tabletop exercises with a specific action plan which includes all components mentioned above (otherwise you are not looking at it holistically or from a safety perspective).
5. Perform a penetration test with your expert firm and see what they can find then show these at events mentioned in number 3 above.
6. Have a Cybersecurity Council (just like a safety council populated with similar people). Include clinicians, nurses and the Chief Operating Officer in that council.
7. Ensure executives have a full understanding of the risks (not a cybersecurity education). That ensures they understand the risks of reputation, or patient endangerment in real time, of how their inaction can be viewed as the potential abandonment of known issues, etc.
8. Bring it to the board – ensure the board knows the risks (not from the IT perspective) but from the perspective of patient safety and reputation. Either include it part of the Board Performance Improvement Council or part of the President's report.
9. Know the risks in your organization and examine them closely – use an outside firm to tell you the issues – as we all know internal folks may, appropriately not have the clear eye to see all the risks.

In summary, I am challenging healthcare leaders to take a different approach than most other articles suggest. I am suggesting you leave the IT solutions to IT but your approach is one of organizational risk, organization operations and organizational safety – all things healthcare executives are responsible to think about. Healthcare executives continuously rise to the challenges of complex solutions, this is no different.

5. About Dr. Bertine Colombo McKenna

Dr. Bertine Colombo McKenna, FACHE, has worked in healthcare for over thirty years, most recently as the Executive Vice President and Chief Operating Officer for the Bassett Healthcare Network. Dr. McKenna is currently a consultant in Healthcare Issues.

Dr. McKenna has her bachelors, MBA and Ph.D. and is also a Fellow in the American College of Healthcare Executives. At

Bassett, she was responsible for the day-to-day operations and programmatic performance of the over $700 million organization. Dr. McKenna was the COO for the entire system which encompassed a 700-employed practitioner Medical Group, five hospitals, 35 clinical outpatient centers, three ambulatory surgery centers, two long term care facilities, a DME company and Home Care Company. In this role Dr. McKenna was a Corporate officer and was responsible for Board relationships, compliance, quality/safety, hospital and medical group operations, budget, integration strategies, strategic planning and much more.

Her expertise covers the healthcare landscape from physician relations, safety quality and service, regulatory and compliance and healthcare operations of all levels – hospital, physicians practice, long term care and managed care.