Clearwater

Whitepaper

How Physician Groups Can Overcome Common Cybersecurity and HIPAA Compliance Challenges

Table of Contents

Introduction

Across the healthcare industry, large physician groups are becoming increasingly common, as investors bring disparate physician practices together to keep up with healthcare challenges and ever-more complex treatment and service delivery needs.

Today, there are about 155,000 physician groups across the United States, generating about $354 billion in annual revenue with close to 2 million employees.

Physician groups are no longer a quaint niche in the industry. They're viable market competitors playing significant roles in healthcare delivery, and as such, they need to address a range of business issues, including cybersecurity and HIPAA compliance, as they grow and expand.

First, what is a physician organization?

For much of the industry's history, physicians were generally single owner, private practices that, over time, could grow to include a number of doctors working in the same practice together.

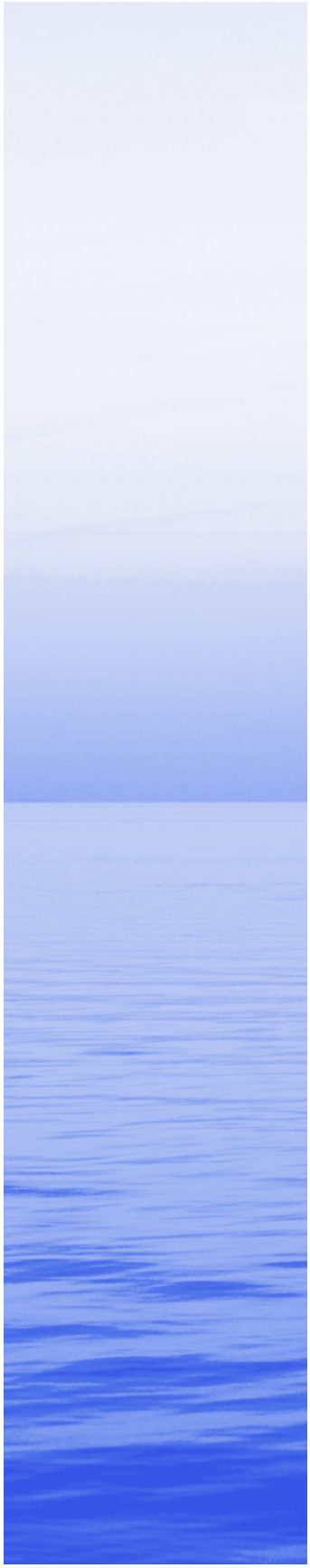
Today, we're seeing more independent providers uniting as physician groups in an effort to be more competitive, manage costs, improve efficiencies, and serve more patients. As mergers are occurring in different sectors, Physician Practice Management Groups have also come on the scene as the entity that handles business operations while physicians focus on care delivery.

Why are physician organizations growing?

The number of physician groups is not only increasing, but so are the size of these organizations and their complexities. Why is this happening?

Here are three issues fueling the proliferation of physician organizations across the U.S.:

1. Community hospitals are evolving into larger integrated delivery networks and as a result, many are now purchasing and merging with physician practices



2. We're seeing payers venture into the provider business and buying large physician practices and/or consolidating them
3. Private equity groups are playing bigger roles in healthcare, backing start-ups that are leading to larger physician organizations, particularly in specialty areas

Why would a provider move into a physician group?

Moving from a private practice into a physician group helps providers because they can reap the benefits of scaling in ways many could never do on their own.

- Larger physician groups have increased negotiating power with payers. The more negotiating power they have with those payers, the better situated they are to get reimbursements, so there's definitely a financial motivation behind these mergers.
- Physicians groups also have increased purchasing power with their suppliers, which effectively helps lower their costs relative to those of private practices or smaller groups. This helps them be more competitive by offering services at less cost than others.
- Moving into a physician group also helps organizations save money by removing a lot of the operational overhead and management costs most private practices or smaller groups struggle to manage.
- By moving day-to-day operational management into the group setting, providers can focus more on patient care and, what might be a huge personal benefit to these physicians, is improved quality of life because someone else handles operations giving them the opportunity to decrease hours and stay focused on patient care.

The pandemic effect

The pandemic effect has a significant impact across the industry. Patients, especially those in at-risk groups, were less likely to leave home for in-person treatments and stay-at-home and social distancing orders made that ever-more challenging for those who could.

During the pandemic, both private and group providers saw a significant decrease in patient visits, with in-person visits decreasing from 97 per week to a little more than half of that at 57.

Between February and October 2020, on average, physicians experienced a loss of about 32% in revenue, with at least 1 in 5 doctors saying their revenue decreased by 50% or more.

Not only did providers face revenue shortfalls, but they were also expected to rapidly adapt to meet changed demands and many, for the first time, had to adopt new technologies to deliver telehealth services and electronically streamline many office and patient functions that had previously been handled hand-to-hand, paper-to-paper, by on-site staff.

More tech, more challenges

As healthcare organizations of all types adjusted to our new pandemic normal, the proliferation of new technologies created a range of new challenges. Top among them were an increase of cyber breaches and compliance scrutiny.

Ransomware and phishing attacks continue to lead as common attack vectors, and there are also increasing risks and successful breaches affecting healthcare organizations originating with third-party vendors and business associates.

Along with these increased breaches, we're also seeing a big spike in the number of incidents reported to the Office for Civil Rights (OCR) and, in turn, a record number of OCR settlements. Healthcare leads other industries as the costliest for breaches, where on average, the cost of a healthcare breach in 2020 is more than $7 million.

Real-world breach impact

Here are some examples of breaches that affected physician organizations in 2020:

But it's not just OCR attention that's problematic for physician groups. There is also an increasing number of civil and class action lawsuits against organizations that fail to prevent breaches or don't meet compliance mandates, and these settlements can vastly exceed OCR fines and penalties. Here are a few of note:

Tennessee Orthopedic Alliance

The lawsuit is related to a phishing attack that affected more than 80,000 individuals and potentially exposed patient names, dates of birth, contact information, health insurance information, treatment or diagnostic information, and/or treatment cost information. As part of the settlement, class action members may be able to collect up to $2,000 in reimbursements and a year of credit monitoring.

Florida Orthopaedic Institute

This class action lawsuit originated over the ransomware attack mentioned earlier, potentially exposing names, dates of birth, Social Security numbers, and health insurance information. This lawsuit seeks $99 million in damages.

Athens Orthopedic Clinic

This lawsuit centers around a 2016 breach that potentially exposed records of about 200,000 individuals, including health insurance information, Social Security numbers, addresses and dates of birth. This case ended up before Georgia Supreme Court. In 2020, OCR announced a settlement on this breach for $1.5 million.

On top of investigations and lawsuits, the financial impacts of breaches on physician groups are sometimes so vast, they can't continue to operate.

For example, when a ransomware attack took down Brookside ENT and Hearing Center, owners decided to close their doors in 2019 after refusing to pay the ransom and attackers deleted all of their data. Wood Ranch Medical faced a similar fate and closed doors after a ransomware attack that same year.

The challenge for physician organizations

If you're a physician group, these real-world examples of breach impact can feel overwhelming. How do you keep scaling, meet patient demands, adhere to all your compliance and regulatory mandates, and build a mature cybersecurity program to support it all?

When we talk about developing and managing an effective cybersecurity and HIPAA compliance program, there are a number of challenges.

- Right out of the gate, what is reasonable and appropriate for your organization?
- And will what works for you today work as you scale and change in the future?
- How do you keep up with changing mandates, standards, and requirements?

Not only are these issues complicated by the speed at which physicians groups are scaling and implementing new technologies today, but like other industries, healthcare faces challenges created by a lack of available skilled professionals. Existing teams are either buried under a mountain of tasks already, or they just don't have the skills or the financial resources to do what's needed, let alone build and scale a compliance and security program.

And what does “reasonable and appropriate” mean anyway?

When it comes to cybersecurity and compliance, when we talk about a reasonable and appropriate program, there are a few things we want to hone in on. For example:

- The size of your organization
- The nature of your organization
- Your business type
- Individuals you do business with
- Types of data you create, store, process, and transmit
- Which compliance and regulatory standards you’re subject to
- Geographical location of your facilities and patient location

Who: Florida Orthopaedic Institute

When: Reported July 1, 2020

Number affected: 640,000 individuals

Breach type: Hacking/IT incident of a network server (ransomware)

Who: Elkhart Emergency Physicians (and St. Joseph Health System)

When: May 28, 2020

Number affected: 550,000 individuals

Breach type: Improper disposal of files from third-party vendor Central Files

Who: The Baton Rogue Clinic

When: Reported Sept. 2, 2020

Number affected: 308,169 individuals

Breach type: Desktop computer/email/network server

Establishing a reasonable and appropriate program

Once you tackle those considerations and understand the type of security and compliance program you need, where do you start? How do you develop your program?

You may find efficiencies in building your program off an established, industry-recognized security and compliance framework instead of trying to build a program on your own.

While there are a number of frameworks across the industry, we recommend starting with a 10-point HIPAA Compliance and Cyber Risk Management Program. On the next page is an overview of what that might look like and how you can apply it to your organization.

10-Point HIPAA Compliance and Cyber Risk Management Program

1. **Have a set privacy and security risk management and governance program in place**

- (45 CFR §164.308(a)(1))
- Here are some questions to consider:
- Do you have a designated HIPAA security and/or compliance officer?
- Is there a governance structure in place?
- Is there a board to whom your security officer reports?
- Do you have a leadership structure to whom the officer reports?,
- Are you setting regular meetings for program governance?
- Are you tracking minutes of those meetings?
- Have you established HIPAA privacy, security, and breach notification policies and procedures?

2. **Develop and implement HIPAA privacy, security, and breach notification policies and procedures**

(45CFR §164.530 and 45CFR §164.316)

Be sure these policies and procedures are in place, are routinely reviewed and updated, and establish a document repository as they will serve as evidence if you face OCR scrutiny or investigation.

3. Train all members of your workforce

(45CFR §164.530(b) and 45CFR §164.308(a)(5))

Be sure to include training around HIPAA requirements, as well as security and privacy awareness. Conduct these trainings consistently and frequently. Include documentation of trainings and updates.

4. Complete a HIPAA security risk analysis

(45 CFR (§164.308(a)(1)(ii)(A))

From an OCR perspective, if you face investigation or inquiry, a security risk analysis may be the first thing OCR will ask to see. Unfortunately, nearly 90% of organizations facing monetary settlements or penalties for HIPAA violations related to electronic protected health information have not conducted a risk analysis correctly or have not done one at all.

5. Complete HIPAA security risk management

(45 CFR §164.308(a)(1)(ii)(B))

Once you complete your risk analysis, you'll need to have a risk management plan in place to deal with the risks that you've identified that require treatment or mitigation. You should also document if you've decided to accept, mitigate, or reject those risks, and document any additional safeguards you're planning to implement that will support OCR findings regarding gaps and risks.

6. Complete a HIPAA security evaluation (e.g. compliance assessment)

(45 CFR §164.308(a)(8))

This is often considered a non-technical evaluation under the HIPAA Security Rule. Think of it as a gap assessment and demonstrating your organization is being reasonably diligent in ensuring you're complying with the Security Rule.

7. Complete technical testing of your environment

(45 CFR §164.308(a)(8))

The HIPAA Security Rule also requires technical testing, which includes things like vulnerability scanning and internal and external penetration testing, web application testing, etc. In light of the number of increased ransomware and phishing attacks physician organizations face, this is also a good time to add related assessments to your testing processes to see where you may have gaps or issues that could put you at greater risk of a successful attack.

8. Implement a strong, proactive Business Associate management program

(45CFR §164.502(e) and 45 CFR §164.308(b))

Be sure you have business associate agreements in place. Physician organizations, now more than ever, need to ensure they have processes in place—and documented—to address and mitigate risks associated with business associates and other third-party relationships.

9. Complete Privacy Rule and Breach Rule compliance assessments

(45CFR §164.530 and 45CFR §164.400)

As a best practice, be sure to complete a compliance assessment to undercover any gaps in your Privacy and Breach Rule compliance measures.

10. Document and act upon a remediation plan

(45CFR §164.530(c) and 45CFR §164.306 (a))

Documentation is key for maturing your program and attesting to your program's effectiveness. But remember, it's more than documenting what you're doing correctly. You also want to identify your known gaps and weaknesses and document all the steps you're taking to mitigate or remediate those issues.

7 fundamentals of an effective compliance program

In addition to the 10-point HIPAA compliance and cyber risk management best practices, you may also find it helpful to adopt these seven fundamentals to ensure security and compliance program effectiveness, including:

1. Implement Policies, Procedures, Standards
2. Designate Compliance Officer and Committee
3. Conduct Effective Training and Education
4. Develop Effective Lines of Communication
5. Conduct Internal Monitoring and Auditing
6. Enforce Standards with Disciplinary Guidelines
7. Respond Promptly with Corrective Action

Building on frameworks

Earlier, we mentioned how helpful it is to use an industry-recognized framework as the foundation for your compliance and security program. It can be challenging, however, to know which framework is right for your organization. While there are a number of factors for consideration, here is a good starting point:

NIST Cybersecurity Framework

One of the best parts of adopting the **NIST Cybersecurity Framework** is it's all open source and all of the information associated with it is easily accessible (and free) from the **National Institute of Standards and Technology (NIST)**.

This framework was created through a government and private sector collaboration. It uses common languages to help you address and manage your cyber risks in a cost-effective way. It's scalable to meet your organization's specific needs and doesn't place additional regulatory burdens on your program.

The framework's core is divided into 23 categories and 108 subcategories across five main cybersecurity functions. It's also mappable to a number of other frameworks including NIST 800-53, ISO, CIS, HITRUST, and informally CSA 2015 405(d).

Your business decision

Now that you understand why building a cybersecurity and compliance program is critical for operational resiliency today, the question you may ask is … can we do this on our own or do we need to outsource program development and management?

Like choosing the right framework, the answer depends on a range of factors, but here's some insight that may help.

First, program set up and management can be just too taxing for some physician groups. As an example, if you're a large enterprise, this is what you might be able to expect financially to develop and maintain a reasonable and appropriate compliance and security program on your own: If those numbers don't seem too off the mark for your organization's capabilities, next consider:

Do we have all of the appropriate resources available—including sufficient staffing, funding, time, and technology resources—to work on this program on a continuous and ongoing basis?

Do we have knowledge or right professionals to understand the problems, challenges, and requirements?

Are we able to adequately address these issues and does our existing team have the time to do it?

If your answer to any of these questions is no, or you're not sure, then you might find it beneficial to work with an advisor or outside firm that can help. Even organizations that are able to successfully find the resources needed to establish a program find it challenging—if not impossible—to keep up with changing standards and mandates and successfully manage the program over time.

If you're a physician group and you're just beginning your journey for compliance and security, or your needs are changing and you need a more robust and mature approach, here are a few key takeaways to remember:

- Define what's reasonable and appropriate for your organization
- Determine where your organization is today in relation to those objectives
- Identify gaps and issues in relation to where you are and where you need to be
- Build a roadmap to close those gaps and achieve your objectives
- Understand all of your investments, commitments, and requirements to manage and deliver on that roadmap
- Build a reasonable and appropriate compliance and cybersecurity program using recognized frameworks
- Document your policies, processes, and procedures
- Continuously re-assess, review, and improve your program

There was a time, not long ago, when we may have thought that physician groups were immune to some of the common challenges that face larger healthcare organizations. But we see as these organizations become larger and pick up momentum, threat actors are honing in on them as valuable targets. The increasing number of systems, technologies, patients, and data make them as vulnerable as other entities.

You may find it helpful to engage in a partnership with an organization like Clearwater that has the industry knowledge, experience, and expertise to help you build and scale a program over time to meet your needs today and grow with you as you change, all the while helping to identify and decrease your risks and helping you remain compliant with evolving industry regulations.

Average Minimum Annual Cost of Security Program	
Expenditures	Annual Cost
Staffing	
1. Chief Information Security Officer / VP Security	$150K - $250K
2. Security Analyst	$60K - $80K
Subtotal Staffing	$210K - $330K
Consulting Support	
1. Policy and Procedures Support	$5K - $40K
2. Technical Testing	$15K - $50K
3. Risk Analysis / Risk Management	$30K - $50K
Subtotal Consulting Support	$50K - $140K
Software	
1. HIPAA and Security Awareness Training	$1K - $5K
2. Other Security Tools	$20K - $100K
Subtotal Software	$21K - $105K
Total	$281K - $575K

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact