integro

WHITE PAPER

FIVE HOT TOPICS AFFECTING THE HEALTHCARE RISK INDUSTRY TODAY

Opioids, Batch Claims, Cyber Threats and More

This year has been a banner one for events, issues and outcomes that percolate to the highest level on a healthcare organization's risk radar screen. Five of the hottest topics affecting the healthcare industry this year include:

- The Opioid Crisis in Healthcare
- The Severity of Batch Claims
- Workplace Violence
- Medical Devices and Cyber Threats
- TeleHealth as a Virtual Reality Platform

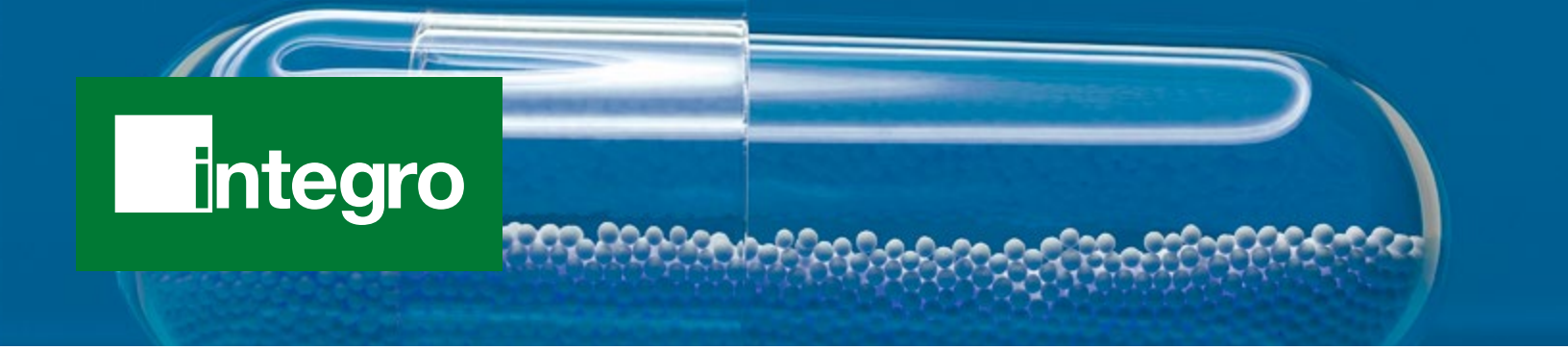
In addition to the above topics, which are addressed here, we commenced a review of the following topics deserving further analysis and which we plan to discuss in future white papers:

- The Complexity of Sepsis Related Claims
- Medical Marijuana Challenges for Providers
- An Active Shooter in the House
- Bad Bugs and Pandemic Infections
- A Collision Course – Medical Necessity and Case Management

These hot topic issues should be placed on a healthcare organization's current risk management agenda for review with both clinical and administrative leadership. Developing a baseline or status report of how an organization has embraced these topics for executives and captive board members is an important and helpful first step in providing a thoughtful response to these issues.

HOT TOPIC #1: MEDICAL LIABILITY AND THE OPIOID CRISIS

Over the past several years, the opioid epidemic has caused horrific problems for many organizations across the country, including healthcare providers. In 2015, the U.S. Department of Health and Human Services estimated that 12.5 million people misused prescription opioids, causing over 33,000



overdose deaths. The most recent financial data related to opioid "mis-use" (from 2013) suggests the opioid epidemic resulted in $78.5 billion in economic losses across all industries and all regions of the United States.

In response to the tragic outcomes many individuals have faced, as well as the economic strain on healthcare organizations, state and local governments, and employers in general, there has been a major uptick in the number of claims and lawsuits. The following information (from 2015 data) is important as healthcare providers continue to learn more about battling this crisis:

- 12.5 million people misused prescription opioids in 2015[1]
- 33,091 people died from overdosing or "mis-using" opioids[2]
- 2 million people had prescription opioid use disorder[3]
- 15,281 deaths were attributed to overdosing on commonly prescribed opioids[4]
- 135,000 people used heroin in the U.S. for the first time[5]

Targets for claims and lawsuits have included, for example, pharmaceutical companies, healthcare organizations, and physicians. For purposes of this review, we will focus on healthcare organizations and prescribing physicians.

ABOUT OPIOIDS

Opioids are synthetic or semi-synthetic forms of opiates (like morphine). Opiates are derived directly from the poppy plant while opioids are manufactured chemicals that are very similar to opiates. Opioids are used as painkillers and are prescribed to patients to treat a variety of medical conditions where moderate to severe pain is a concern. Commonly prescribed opioids in the U.S. include:

- Oxycodone (OxyContin)
- Hydrocodone (Vicodin)
- Fentanyl

1 2015 National Survey on Drug Use and Health (SAMHSA)
2 MMWR, 2016: 65(50051); 1445-1452 (CDC)
3 Prescription Overdose Data (CD)
4 IBID
5 2015 National Survey on Drug Use and Health (SAMHSA)

Opioids are effective at relieving pain, but unfortunately, they are extremely addictive and can lead to overdoses and the use of stronger (and more dangerous) illicit drugs. The causes of the opioid epidemic are complex, and there are no easy solutions. One approach that some individuals, organizations or even municipalities are pursuing is to seek relief in the courts by going directly after the opioid makers and prescribers.

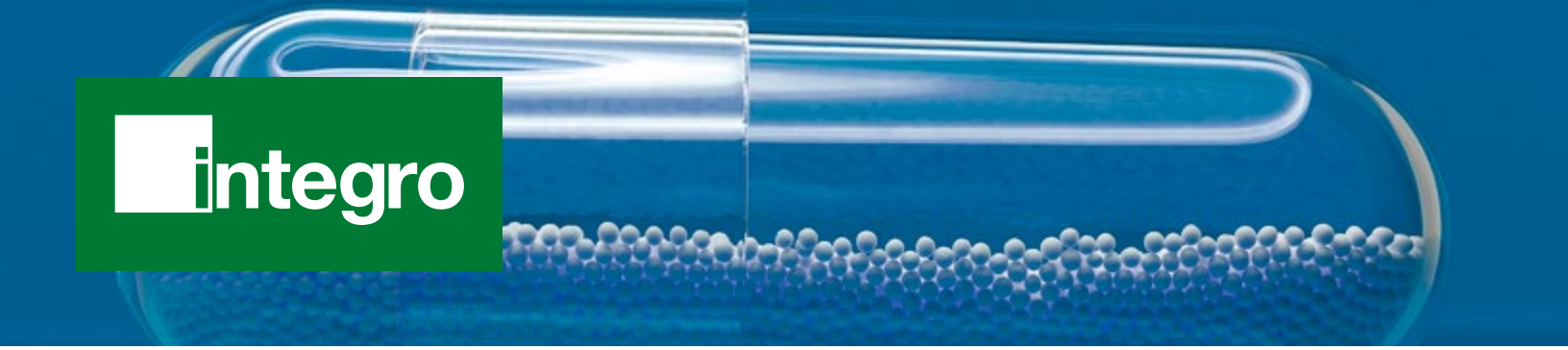
THE CURRENT LANDSCAPE

While many providers/physicians refuse to prescribe opioid medications, most will, due to a lack of other viable options for complex pain management for their patient populations. Many providers/physicians suggest that drug manufacturers and distributors have not made reasonable efforts to provide healthcare providers generally with alternatives to opioids, or to educate physicians and healthcare organizations about the serious health conditions that can occur due to opioid addiction.

RISK MANAGEMENT TIPS

With this crisis at hand and the focus on patient safety and appropriate strategies to avoid harm resulting from opioid usage, risk management professionals and providers should consider the following strategies to manage their risk exposure:

- Educational materials should be regularly updated and made readily available to patients and families.
- Patients with complex medical histories and needs will benefit from ongoing coordination among caregivers. The use of case studies and "lessons learned" from either internal and external "opioid" medical malpractice cases or poor patient outcomes should be emphasized. Reliance on pharmacy colleagues and clinical educators can benefit treatment plans for all patients seeking pain management through opioids.
- Selection of opioids for specific patient treatment requires patient-specific clinical scrutiny, including



ongoing review of the need for and management of pain medication.

- When prescribing opioids, assessing the risks of all medications or other stimulants (e.g., alcohol) the patient may be taking as well as close team monitoring is critical to patient safety as well as to the avoidance of poor outcomes. There are multiple tools and guidance available to providers, including guidance from state agencies which should aide in the improved management of this sensitive population.
- Clinicians may want to consider the clinical risks and time frames for a prescription renewal and expectations for return office visits given the evidence of abuse of opioids, plus the challenges many patients exhibit with these drug regimens. Ongoing toxicology testing may also be an important intervention to consider.
- Healthcare organizations should design and implement tracking systems that identify outliers (i.e., providers who exceed standard prescription frequency per patient or in the aggregate) within the physician/prescriber population as doing so may facilitate quick intervention and prevent poor outcomes including overdose and/or death.

CASE IN POINT

A St. Louis jury awarded $17.6 million in damages to a couple who had filed a medical malpractice lawsuit against a doctor for overprescribing opioid pain medication. The plaintiff, Brian Koon, was awarded $1.4 million and Michelle Koon, his estranged wife, was awarded $1.2 million. The remaining $15 million was awarded as punitive damages against the physician who prescribed the medication and the plaintiff's employer.

HOT TOPIC #2: BATCH CLAIMS EVENTS REVISITED

Batch Claim(s) events continue to be a top concern for both risk management professionals and underwriters. Categories of "batch" typically fall into one of the following areas:

- Contamination and/or Sterilization
- Unnecessary Surgeries
- Serial Infectors
- Abuse/Molestation
- Property or Catastrophe

While the majority of significant "batch" claims tend to settle relatively quickly and fall in the $20,000,000 - $100,000,000 range, there are published events that have ultimate costs greater than $200,000,000 in other industries. In addition to being costly, these events can damage reputations and result in complex insurance coverage disputes.

RISK MANAGEMENT TIPS

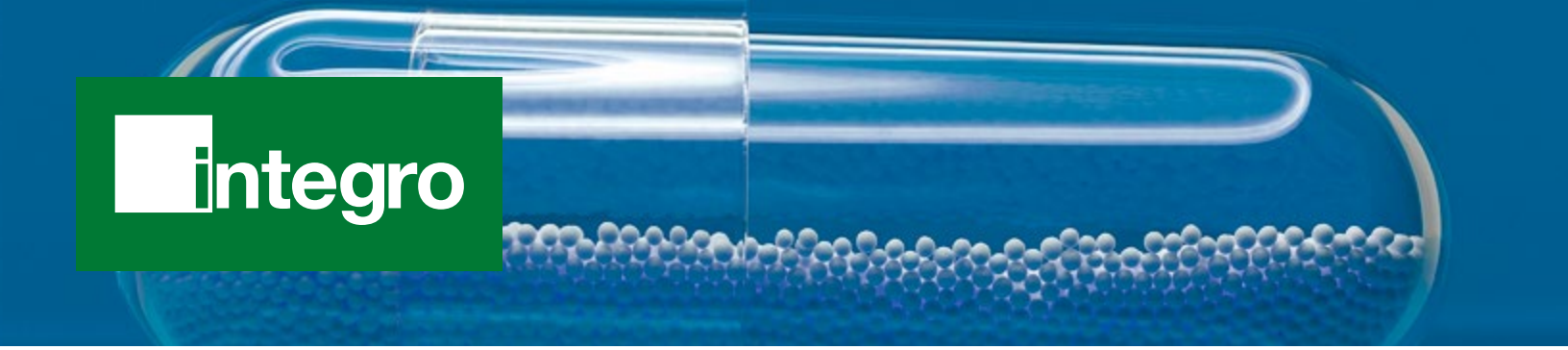
When addressing and mitigating exposure to "batch", risk management professionals should consider the following:

1. Review your coverage to confirm that it will address and respond to "Batch" as expected.

- Is the policy wording unambiguous as to "related acts" and "related claims" regardless of which coverage might be triggered (e.g., CGL, Professional Liability, Products)?
- Are retentions and limits clearly defined if there was a "batch" event?
- Have you adopted embedded "batch" wording versus wording via endorsement?
- Have you assessed all insurance (or reinsurance) policies to make sure there is consistency of treatment throughout entire coverage towers?

2. Take measures to mitigate the potential of a very costly "Batch" event.

- Keep careful watch on FDA and CDC alerts and advisory letters and have a plan in place to take prompt action when appropriate.
- Know your vendors, their specific products and insurance coverage/limits and contractual provisions.



- Employ robust hiring/screening measures and ensure that outside staffing agencies have appropriate screening protocols.
- Be coordinated and communicative with your Legal/ Regulatory team to ensure that Risk Management is aware of all its compliance obligations with respect to required disclosures and otherwise.

3. Know your claims reporting conditions, and have a clear protocol around investigating and declaring a "Batch" event.

- Ensure that all staff involved with claims are educated about what makes "batch" events unique and might present complex coverage issues.
- Know whether your insurer (or reinsurer) has the right to declare "batch" events.
- Understand any specific provisions as respects reporting "batch" or "related acts."
- Understand any timing issues as respects "batching" claims as well as whether there are coverage provisions regarding "mitigating" risks.

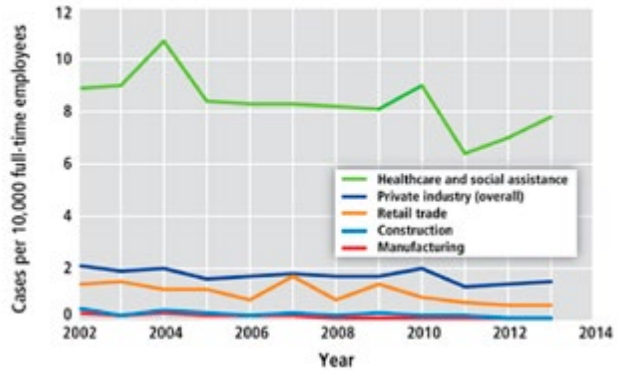
CASE IN POINT

In 2014, a large health system agreed to a $37 million settlement, to be divided among more than 270 patients who were told that their blocked arteries required the insertion of coronary stents. Four years earlier, the hospital had agreed to a related $22 million False Claims Act settlement within the U.S., sending patient notifications that their procedures may not have been necessary.

HOT TOPIC #3: WORKPLACE VIOLENCE

Staff in hospitals, nursing homes, behavioral health facilities and other healthcare settings are exposed to significant workplace violence risks. The usual source of the violence and or verbal abuse is either patients or family members. In addition to the clear impact on healthcare employees, this risk can also impact innocent patients and bystanders.

Violent Injuries Resulting in Days Away from Work, by Industry, 2002–2013



According to the Bureau of Labor Statistics and as depicted in the graph on this page, healthcare employees are at least four times more likely to lose time away from work due to workplace violence than most industries.

According to recent statistics from OSHA and the CDC, the increasing trend of workplace violence in the healthcare setting has been fueled by:

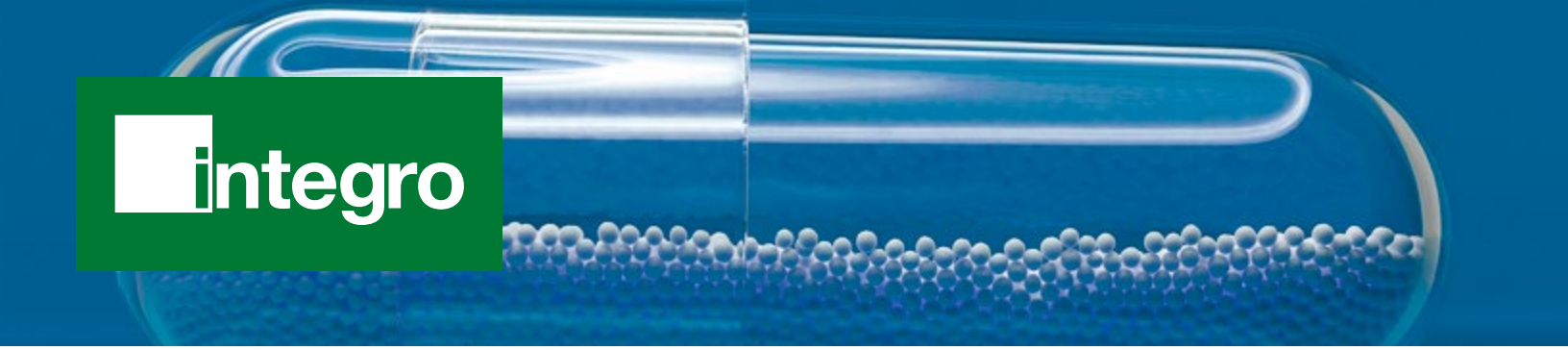
- Drug and alcohol abuse
- Social media (e.g. "bullying")
- Reduced funding for behavioral health services

The problem has grown larger given that many times, caregivers are reluctant to report violence or abuse at the hands of their patients.

RISK MANAGEMENT TIPS

Healthcare facilities can reduce the incidence and costs associated with workplace violence by developing and executing a prevention program, which includes:

- **Raising employee awareness and ensuring management commitment:** All employees need to be made aware of the risks and costs associated with workplace violence. Managers need to demonstrate their commitment to a comprehensive prevention program, and continue to stay engaged in all aspects of the program.



- **Conducting a worksite hazard assessment:** Interview experienced staff in each area/department; review incidents; and gain input from Security and local law enforcement as they are all important facets of assessing and identifying both the frequency and potential severity of risks.
- **Implementing education and training:** All employees should receive education and training on hazard recognition, their responsibilities, escalation protocols, and what to do in an emergency. There should be additional focus and ongoing efforts at those locations/departments that have a higher potential for workplace violence.
- **Developing specific policies:** Programs like "Zero Tolerance (for Workplace Violence)" and "Safe Reporting" can go a long way towards reducing incidents of workplace violence without a high expense.

There might be crossover with existing protocols that address high severity or "batch" exposures (e.g., "Active Shooter"). It is important that facilities develop and utilize programs that will work best for their culture and community.

CASE IN POINT

In July 2013, a patient was admitted to a special psychiatric unit at a New Hampshire hospital. Two days later, while awaiting involuntary commitment, the patient attacked two employees in an attempt to leave. One of the employees, a nursing assistant, suffered critical injuries to his face and head. He was never able to return to work. Several months later, another patient at the same facility attacked a security guard, punching him repeatedly in the face before being subdued with pepper spray.

HOT TOPIC #4: MEDICAL DEVICES- THE NEXT SECURITY NIGHTMARE

Hacked medical devices make for scary headlines. The Guardian reported (8/31/17) in an article titled, "Hacking Risk Leads to Recall of 500,000 Pacemakers Due to Patient Death Fears," that the FDA is overseeing a crucial firmware update in the U.S. to patch security holes and prevent the hijacking of pacemakers. In 2013, Dick Cheney ordered changes to his pacemaker to better protect it from hackers. Johnson & Johnson warned customers about a security bug in one of its insulin pumps last fall, and St. Jude Medical has spent months dealing with the fallout of vulnerabilities in some of its defibrillators, pacemakers, and other medical electronics.

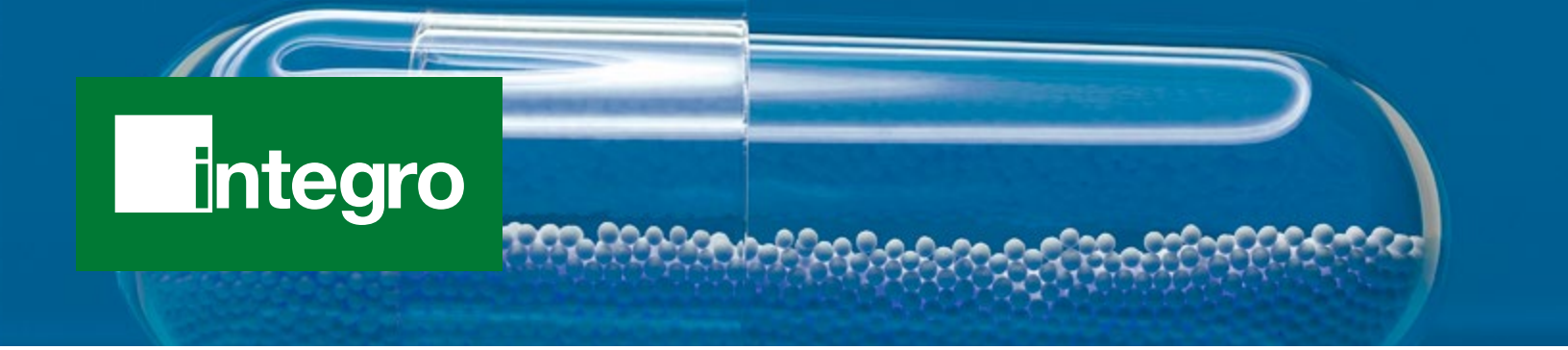
The fear is that the lax cybersecurity makes the devices vulnerable to attacks from hackers that could debilitate the batteries or change patients' heartbeats. St. Jude Medical does not have evidence that any devices are compromised at this time; the concern is that if a hacker does take control, it could lead to patient deaths.

By now multiple invested parties suggest that medical device companies should have invested in technology to improve medical device security based on the lessons they've learned from multiple hacking incidents. Published security experts suggest there may be more work to be done in this area.

As hackers increasingly take advantage of lax security on embedded devices, defending medical instruments has taken on new urgency on two fronts:

- A need to protect patients from their devices being hacked, such as attackers hacking an insulin pump to administer a fatal dose.
- Vulnerable medical devices connected to a huge array of sensors and monitors, making them potential entry points to larger hospital networks, which could lead to the theft of sensitive medical records or a devastating ransomware attack.

Medical devices with features like wireless connectivity and remote monitoring allow health professionals to adjust the devices without invasive procedures, which while progressive, also creates potential points of exposure.



While implanted devices draw the most attention, the broader universe of medical care creates exposure and potential danger in the healthcare industry. According to Wired magazine (March 2, 2017), "U.S. hospitals currently average 10 to 15 connected devices per bed, according to recent research from IoT security firm Zingbox."

May Wang, Chief Technology Officer of Zingbox said, "We tend to think healthcare is very conservative, healthcare is very slow because of regulations and liabilities, but because of the huge benefits they're seeing by using IoT devices, hospitals are deploying more and more of them. For the past three years the healthcare sector has been hacked even more than the financial sector. And more and more hacking incidents are targeting medical devices."

Another concern is that many healthcare systems use outdated operating systems, which make them vulnerable to hackers. In one hacking attack known as MedJack, malware was injected into medical devices to spread across a network. The medical data discovered in this attack can be used for tax fraud or identity theft, as well as to track active drug prescriptions, enabling hackers to order medications online and then sell them on the dark web.

As hackers probed and compromised the system, the attackers used malware to target their assaults at medical devices running outdated operating systems with known vulnerabilities, like Windows XP and Windows Server 2003. By attacking legacy technology, hackers more easily avoid detection, especially since other parts of a network running current operating systems do not flag the activity. Newer services are already patched against the older malware, and automatically classify it as a minor threat.

Once hackers have a foothold, they can exploit their position for a number of different types of network assaults, such as ransomware attacks. This type of assault victimized Rainbow Children's Clinic in Texas Hollywood Presbyterian Medical Center last year.

RISK MANAGEMENT TIPS

As with other IoT devices, there are two components to address the device security issue.

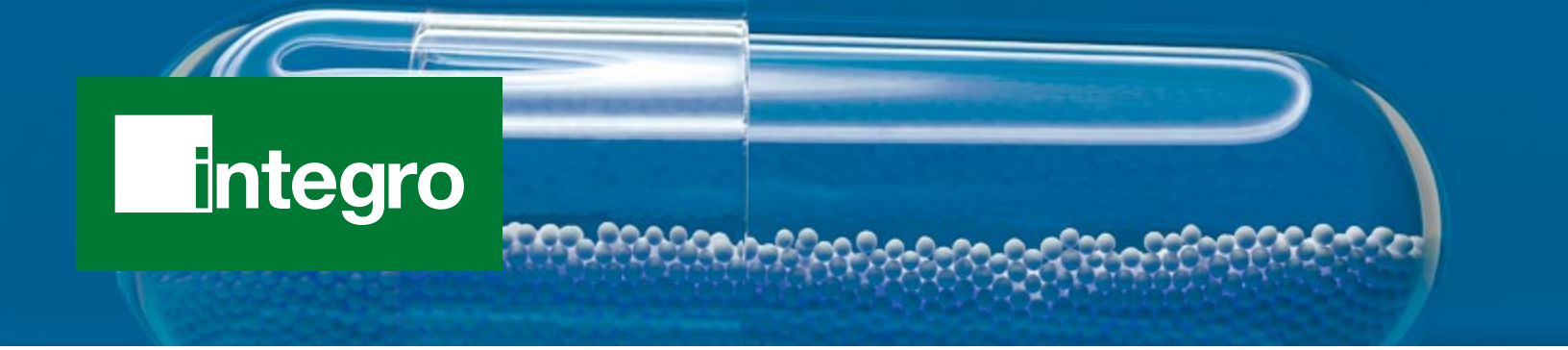
- Medical devices that have been on the market for years need defenses, such as security scanning, and an easy mechanism for downloading patches and updates.
- There need to be incentives for future generations of devices to include more robust security protections at the onset. Many manufacturers ignore security in the early planning stages or rely on third-party components that may be vulnerable.

There is some progress as the Food and Drug Administration (FDA) began evaluating device cybersecurity as a criterion for product approval in 2013 and has since updated it. The FDA has delayed or even blocked medical devices from coming to market if they do not meet the agency's cybersecurity standards. As a result, the FDA has seen improvement in the foundational cybersecurity protections that are encoded on new products coming under review. Since a device can take years to develop and the FDA has only been focused on cybersecurity concerns in the past few years, the tangible results are slow.

It is clear that securing existing devices and working towards protecting new devices is a gradual process. In the meantime, both patients and the healthcare industry as a whole remain exposed.

CASE IN POINT

In October 2016, Johnson and Johnson sent letters to 114,000 patients warning them about a potential bug in its Animas OneTouch Ping insulin pumps, which could be targeted by hackers. In a more recent development (August 2017), Siemens announced that it would be updating software to its PET scanners, which otherwise could be vulnerable to cyber attack.



HOT TOPIC #5: TELEHEALTH - VIRTUAL REALITY

In some rural hospitals, a human-size robot wanders the halls with cameras and a tablet mounted at eye level. By using this device, physicians from outside the hospital can remotely view and treat patients. In other areas, medical groups use Skype to communicate and evaluate patients remotely.

Recent hurricanes highlight the fact that extreme weather makes it difficult for people to access healthcare services. According to MobiHealthNews, reporter Jeff Lagasse stressed how telemedicine companies are mobilizing to fill the void, offering physician consultations remotely to those who may be trapped by flooding and extreme winds.

While these remarkable technologies hold great promise for specific patient populations, they also create significant risks. The concept of and platforms for delivering telehealth has evolved over the last 20 years and is now a part of everyday vernacular. More private insurers are now paying for telehealth services—a trend experts say will boost utilization levels, especially as states enact laws with rules addressing telehealth coverage.

Nearly all payers now believe telehealth will help rural members gain access to providers and may attract companies wishing to offer modern conveniences to employees who expect on-demand services. Insurers are also hoping telehealth will live up to its hype by keeping people out of more expensive healthcare settings.

TELEHEALTH DEFINED

Telehealth involves the delivery of healthcare to patients in remote locations and to underserved patient populations through a variety of electronic modalities, including audio-visual, online, and wireless applications. Depending on the need, telehealth can provide remote monitoring, as well as real-time interactions with physicians and mid-level practitioners. The advantages of telehealth include improved access to medical care and consultation in rural areas, more efficient treatment plan implementation, cost-savings for patients, and increased patient satisfaction. Many medical specialties—including cardiology, pathology, psychiatry, and radiology, among others—have embraced the concept on a national basis.

SECURITY AND PRIVACY ISSUES

Despite the obvious advantages of using various forms of telehealth, the medical community must become knowledgeable about and comply with federal and state regulatory policies and requirements that affect its practices as it relates to provide care and treatment with these platforms.

LICENSING ISSUES

Historically, physicians and other healthcare professionals have been licensed exclusively by state boards of practice (i.e., medicine, nursing, pharmacy). Physicians who engage in telehealth across state lines, therefore, face a number of challenging considerations beyond the scope of this paper as the laws governing the practice of medicine vary significantly among the states.

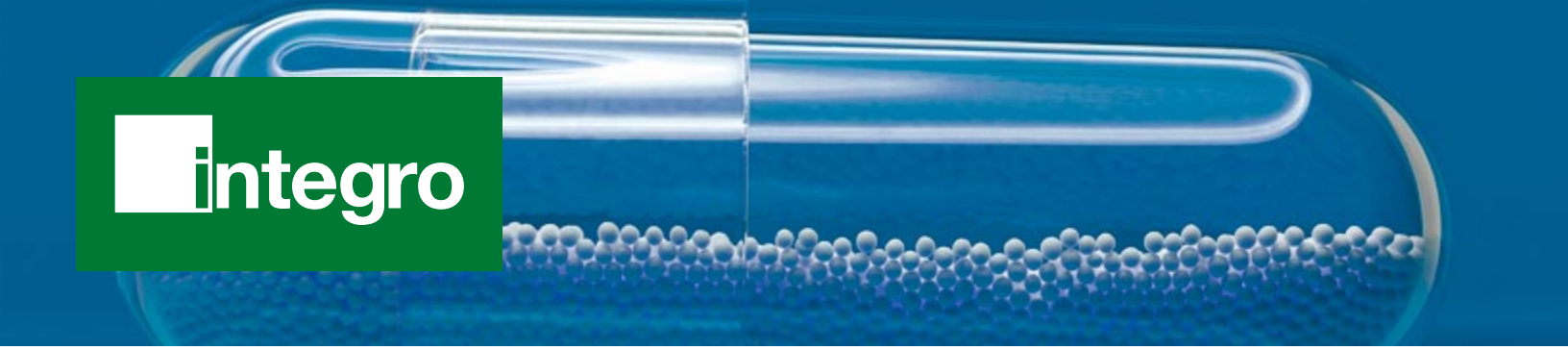
PROFESSIONAL LIABILITY

Traditional professional liability policies generally specify that indemnity coverage is only available for a claim that occurs in a specific territory or jurisdiction. A physician sued in a state other than the covered territory may find that no coverage is available to either defend the claim or pay indemnity if there is an adverse judgment. Also, flaws or malfunctions in the delivery of telehealth could lead to multi-plaintiff or "batch" scenarios, which would need to be properly defined under the coverage.

RISK MANAGEMENT TIPS

If you are practicing telemedicine, there are several things you can do to encourage secure consumption of this emerging medical practice. Those actions include the following:

- Ask your system vendor, compliance department, legal counsel, etc. to provide training to you and your staff on how to protect and secure your data.



- Ensure robust and reliable high-speed broadband connectivity to support clinical functions.
- Check practice requirements and consult with legal counsel regarding limitations in states where you anticipate providing care to patients. Understand reimbursement practices for telehealth services.
- Use telehealth carefully and understand any limitations on the reliability and accuracy of the information.
- Communicate directly with your professional liability insurer to make certain that your policy extends coverage to all jurisdictions where you provide services.

ABOUT INTEGRO'S HEALTHCARE PRACTICE HOT TOPICS

Members of Integro's Healthcare Practice team prepared this series of "hot topic" risk management issues that healthcare organizations across the continuum are dealing with on a daily basis. The topics are based on questions from our clients, colleagues and underwriting partners; trends from both the healthcare risk management landscape and those resulting from the delivery of care generally; claims activity in the U.S.; review of the literature; and communication with risk management professionals, clinicians, captive board members and others to identify those issues or topics which are most concerning to them.

If you need help with any of these issues or topics, please reach out to your Integro Executive Broker or a member of your client management team. Please let us know about other "hot topics" you would like to see addressed in future white papers.

ABOUT THE AUTHORS

This hot topics edition was authored by Audrey Greening, Bill McDonough and Shep Tapasak, leaders within the firm's national Healthcare practice.