

HEALTHCARE COMPLIANCE

Build customer
loyalty, protect
your bottom line,
prevent hefty fines.

cliniconex

TABLE OF CONTENTS

UNDERSTANDING COMPLIANCE	2
Reasons to care	7
Building your compliance program from the ground up	9
Understanding the pitfalls of non-compliance	13
NEW NATIONAL STANDARDS	16
USING TECHNOLOGY TO EMBRACE COMPLIANCE	17
What is RegTech anyway?	20
Challenges and opportunities	21
Lack of industry and technical experts	23
Cybersecurity threats major challenge	23
THE FINAL WORD	26



Canada Health Act, The Personal Health Information Protection Act (PHIPA) and Guiding Principles of Compliance are a complex set of provincial and territorial rules and regulations that must be strictly adhered to. These are just some of the regulations keeping Canadian senior care home administrators and healthcare service providers moving toward compliance, safety and continuous quality improvement.

The price of not meeting these strict compliance regulations can be steep. When there is a proven violation, companies open themselves up to everything from hefty fines and legal fees to reputational damage and the resulting loss of business.

In 2021, Ontario announced new fines, ranging from \$200,000 for an individual to \$ 1 million for a corporation, as part of its overall rules governing long-term care. The license of a home can be suspended if its officers and directors are found not competent to operate it in a responsible manner, if they risk the health and safety of residents or provide false statements to the ministry.

This potential financial impact and subsequent loss of reputation is why more healthcare providers are turning their attention and dedicating budget to putting solid compliance programs in place. It just makes good business sense and gives staff, shareholders, patients and residents, and their families an added sense of security.



UNDERSTANDING COMPLIANCE

At its most basic level, compliance is defined as the ongoing process of meeting or exceeding the legal, ethical and professional standards that apply to a particular organization or provider.

The scope for compliance programs covers everything from patient care, billing, reimbursement, managed care contracting, research standards, Occupational Health and Safety, preventive care and PHIPA privacy and security.

It calls for a compliance culture to be ingrained within an organization. This means promoting preventing, detecting and resolving issues that do not comply with government and ethical guidelines.

Benefits of building a compliance-first culture

It's important to involve stakeholders from all departments to build a solid compliance program:

- Patients, residents and families/caregivers have a role to play because they know if the quality of care they were promised and outlined in their care plan is being delivered. Involving them early on also ensures they have a clear understanding of their personal responsibility when it comes to compliance practices. Some institutions establish resident councils to get feedback on compliance and other care-related issues.
- All staff from medical office assistants, nurses, support workers to the cleaning and kitchen staff know the risks most likely to arise in their roles and responsibilities; they can help you determine compliance gaps and recommend which measures need to be taken to avoid risks.
- Measure your compliance practices against industry best practices which gives you a competitive advantage that can be promoted to potential clients.



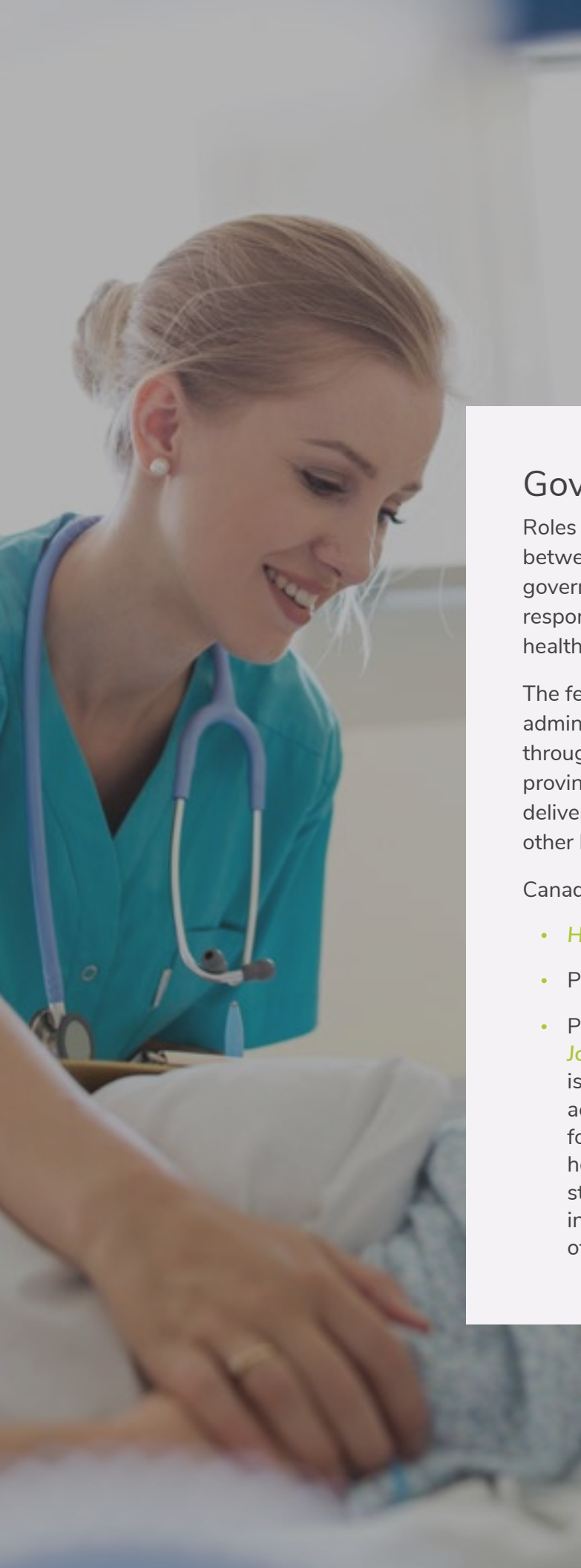
Having a say will ensure that all internal stakeholders buy into the policies and procedures and champion them among their co-workers and fellow residents. This ownership creates a compliance culture, not one that just blindly follows a set of rules without understanding the critical importance of ‘why.’

Despite the increases in compliance costs because of the number of regulations that must be followed and the need to prepare for heightened scrutiny, studies show that it is more costly not to meet compliance standards, by at least 2.7 times. The cost of compliance, on average, is approximately \$5.5 million whereas the cost for noncompliance is approximately \$15 million—almost three times as much.

The need for compliance experts is also on the rise. According to Deloitte’s [compliance survey 2021](#), 35% of those surveyed said they expect an increase in compliance headcount, citing maturing compliance frameworks, broader organizational growth and an increase in regulatory requirements.

“ **An increase in the volume of regulatory change over 2021 has driven a reduction in their ability to meet all of the demands placed on them by the business. 61% of respondents noted that the recent level of regulatory change has had an adverse impact on the compliance function’s ability to perform its role effectively.** ”

Having a strong compliance program in place and the budget to back it, is a strong motivator for compliance experts to join your team.



Government oversight

Roles and responsibilities for healthcare services are shared between provincial and territorial governments and the federal government. The provincial and territorial governments are responsible for the management, organization and delivery of healthcare services for their residents.

The federal government is responsible for setting and administering national standards for the healthcare system through the Canada Health Act, providing funding support for provincial and territorial healthcare services, supporting the delivery of healthcare services to specific groups and providing other health-related functions.

Canadian governing and regulatory bodies include:

- **Health Canada**
- Provincial and territorial governments (see chart below)
- Professional certifications such as that provided by the **Joint Commission**. Founded in 1951, The Joint Commission is the nation's oldest and largest standards-setting and accrediting body in health care. As an independent, not-for-profit organization, it seeks to continuously improve health care for the public, in collaboration with other stakeholders, by evaluating healthcare organizations and inspiring them to excel in providing safe and effective care of the highest quality and value.



PROVINCE/ TERRITORY	LONG-TERM CARE TERMS USED	LEGISLATION/REGULATION	ACCOMMODATION COSTS TO THE RESIDENT
<i>British Columbia</i>	Residential care facilities, long-term care homes	<i>Community Care and Assisted Living Act</i> (2002) and <i>Residential Care Regulation</i> <i>Hospital Act</i> (1996), and its <i>regulations</i>	Income-based up to 80% after tax, \$1,189 to \$3,444/month (2020)
<i>Alberta</i>	Long-term care homes, nursing homes, auxiliary hospitals	<i>Nursing Homes Act</i> (2000), <i>Nursing Homes General Regulation</i> and <i>Nursing Homes Operation Regulation</i> <i>Continuing Care Health Service Standards</i> govern publicly-funded facilities, and the <i>Long-Term Care Accommodation Standards</i>	\$1,743-2,120/month (2020)
<i>Saskatchewan</i>	Special care homes, nursing homes	<i>Provincial Health Authority Act</i> <i>Program Guidelines for Special Care Homes</i>	\$1,152 + 57.5% of income over \$1,579/month up to a maximum of \$2,859/month (2020)
<i>Manitoba</i>	Personal care homes	<i>The Health Services Insurance Act</i> (1987) and <i>Personal Care Homes Standards Regulations</i> and <i>other regulations</i>	\$39-95/day based on income. Minimum retained monthly income of \$370 (2020-21)
<i>Ontario</i>	Long-term care homes	<i>Long Term Care Homes Act</i> (2007) and its <i>regulation</i>	\$1,891 -2,700/month (2019)

Quebec [in French]	CHSLD (« centre d'hébergement et de soins de longue durée »)	Act respecting Health and Social Services and its regulations related to long-term care. Private CHSLDs that are not under contract with the provincial government are not subject to the same regulations as CHSLDs that receive public funding but are expected to follow provincial standards.	\$1,211-1,946/month (2020)
Nova Scotia	Residential care facilities, nursing homes	Homes for Special Care Act (1989) and its regulation Required operating standards are issued ministerial guidance .	Income-based up to 85% of after-tax up to \$110/day. Minimum left to resident \$260/month.
New Brunswick	Nursing Homes	Nursing Homes Act and its regulation	Average \$3437/month depends on services required. (2014)
Prince Edward Island	Nursing homes, manors	Community Care Facilities and Nursing Homes Act (1988) and its regulations .	\$92/day (2019)
Newfoundland and Labrador	Long-term care facilities	Health and Community Services Act (1995) and the Personal Care Homes Regulations .	Income-based to a maximum of \$2,990/month. Minimum left to resident \$150/month
Yukon	Long-term care homes, continuing care facilities	Health Act (2002) Yukon Continuing Care: Bill of Rights for Residents Living in Yukon Continuing Care Facilities	\$35/day (2019)
Northwest Territories	Long-term care homes, supported living	Not addressed in legislation or regulation but standards have been published.	\$844/month (2020)
Nunavut	Continuing Care centres, nursing homes, elder homes	Not addressed in legislation or regulation	No charge to the resident

Source: Table prepared by the author from provincial and territorial and stakeholder websites and Royal Society of Canada, **Restoring Trust: COVID19 and The Future of Long-Term Care – A Policy Briefing by the Working Group on Long-Term Care**, Table 1, p.53-54, June 2020.



REASONS TO CARE

When it comes to choosing the right senior residence, potential clients do their due diligence.

One widely used tool is [Your Health System: In Depth](#), an interactive database that compiles data from close to 1,300 long-term care organizations and 600 Canadian hospitals. In Depth allows potential clients to filter homes based on indicators such as person-centeredness and healthcare; healthcare access, efficiency, appropriateness and effectiveness; social determinants of health; healthcare safety; and, health status. Users can view results for individual facilities, health regions, provinces or territories, or for all of Canada.



Case in point: Ontario's long-term care home quality inspection program

The Retirement Homes Regulatory Authority (RHRA) regulates all retirement homes and is responsible for enforcing care and safety standards and supporting the rights of residents through:

- **Licensing**
- **Conducting inspections**
- **Investigating complaints**

During inspections, inspectors will ask for documentation such as a list of residents and staff and reports on how they responded to incidents such as falls, complaints, incidents of behaviour management and reports of alleged abuse. They do a full walkthrough and talk to residents and observe care services.

These reports can be found on Ontario's [Retirement Homes Database](#), the official database of all 750+ licensed retirement homes in the province. It gives potential clients a complete history of a retirement home's track record in meeting its obligations under the law. Clients can search the data to get information such as licence status, inspection reports, size of the home and care services available. How you fair during an inspection, impacts how people judge the reputation of your organization.



Why reputation matters

Clearly, reputation matters when it comes to attracting new business.

A quick look at the facts:

5%

of Google searches are health-related

79%

of prospects run searches before booking an appointment at a senior home

94%

of prospects use online reviews to evaluate providers

1-6

Online reviews needed for potential clients to form an opinion about your company

A strong compliance program can help you attract the more than 80% of potential clients checking you out online.

Then there are potential investors. Why would any investor want to associate themselves with your brand if you have a less-than-stellar reputation? You can bet that an important aspect of an investor's due diligence is determining any reputational risks they may face by investing in your business.

Need another compelling reason? Today, more than 90% of companies use social media for recruiting. Statistics show that 83% of respondents to a [survey](#) said they're influenced by reviews when making application decisions, and almost half reported that company reputation influences their job offer decisions. 75% said they would not be willing to work for a company with a bad reputation—even those without jobs.



BUILDING YOUR COMPLIANCE PROGRAM FROM THE GROUND UP

The starting point for any world-class ethics and compliance framework starts at the top, and the sense of responsibility they share to protect the shareholders' reputational and financial assets. The board and senior management need to do more than pay lip service to ethics and compliance. A strong compliance program to protect reputation and maintain financial stability, requires that they empower and properly resource those with the day-to-day responsibilities to mitigate risks and build organizational trust.

“ People are suspicious of leaders who are closed about their values or standards. Stakeholders assume if you value nothing, you'll value anything.” *Thomas Rollauer, executive director, Deloitte Center for Regulatory Strategies.*

The program has to support and enhance the existing corporate culture which typically covers standards regarding patient care, a code of conduct and ethics, personnel matters and policies to comply with government standards. A strong, measurable compliance program can positively contribute to the corporate culture as long as it's not seen as an impediment to driving change.



Hire or appoint a Chief Compliance Officer (CCO)

The CCO has day-to-day responsibility for managing compliance and reputational risks. A skilled CCO can create a competitive edge for organizations and oversee the creation of or modifications to an existing plan.

Assess your risk

A risk assessment is designed to detect, monitor, assess, mitigate and prevent risks to residents. Areas to assess for risk include accreditation compliance, resident safety and quality (e.g. infection control, medication practices), emergency and disaster readiness and vendor risk management. Assessing these risks helps you to develop a comprehensive program that everyone can buy into, protects your reputation and ensures compliance with government regulations.

Ethics and compliance risk assessments are not just about process—they are also about understanding the risks that an organization faces. The risk assessment focuses senior management on those risks that are most significant within the organization, and provides the basis for determining the actions necessary to avoid, mitigate or remediate those risks.

Plan it out

Develop a detailed framework and plan to clearly spell out how your program is going to work at a practical level. For example, ensure it incorporates policies and procedures, education, communication and action steps to follow if offences occur. Get employees and residents involved in the planning so that all aspects of care are taken into consideration.

Training and retraining essential

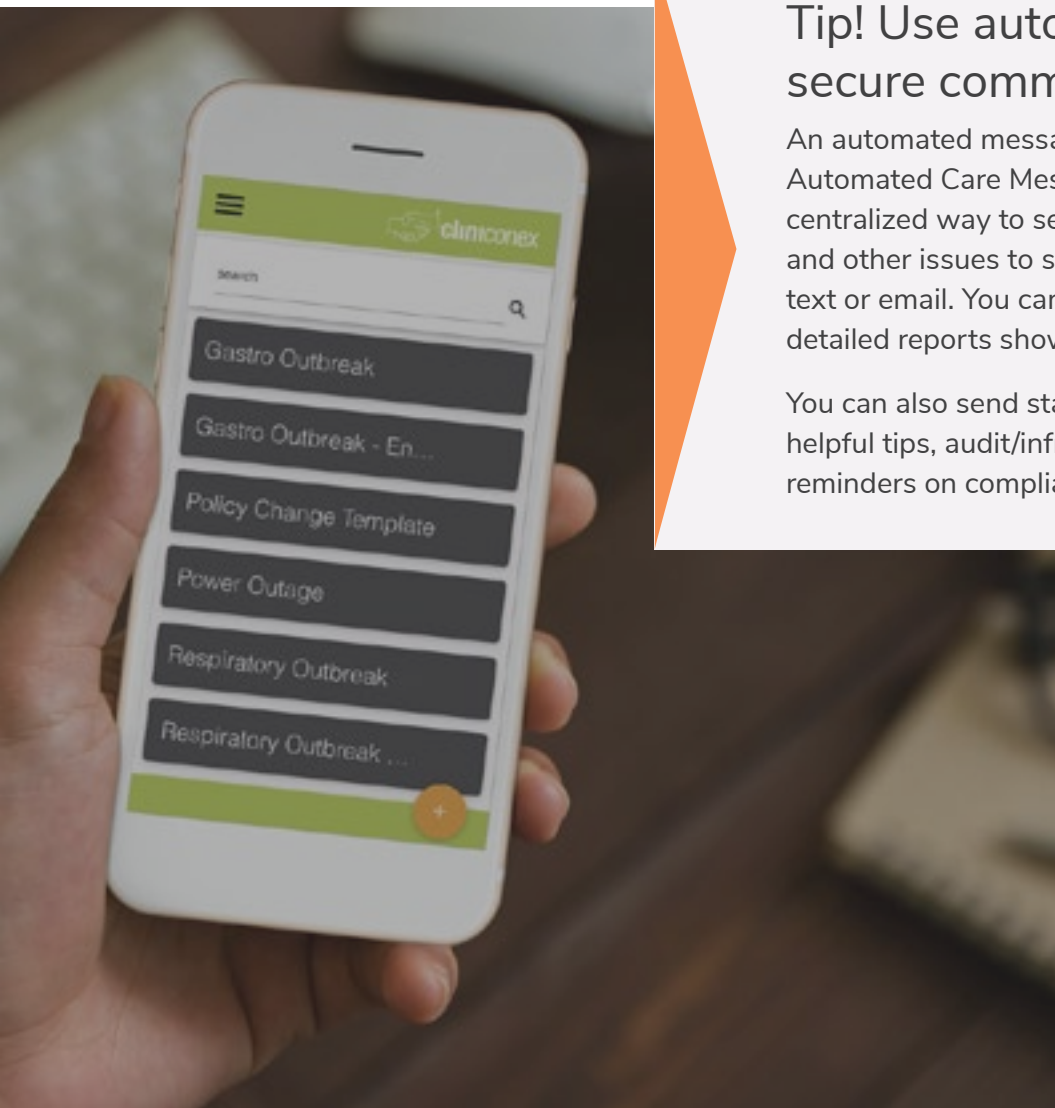
The plan is only a piece of paper until it's ingrained into the culture of your organization. This requires a training program that is designed for those who need the training, how they like to receive information and how often and how much training is required for each specific function.

Clear reporting process

Processes on how to report non-compliance need to be clear, easy and, more importantly, protect those reporting the suspected violation. Take every opportunity to remind employees and residents about when, why and how they should take action if necessary.

Communicate and then communicate again

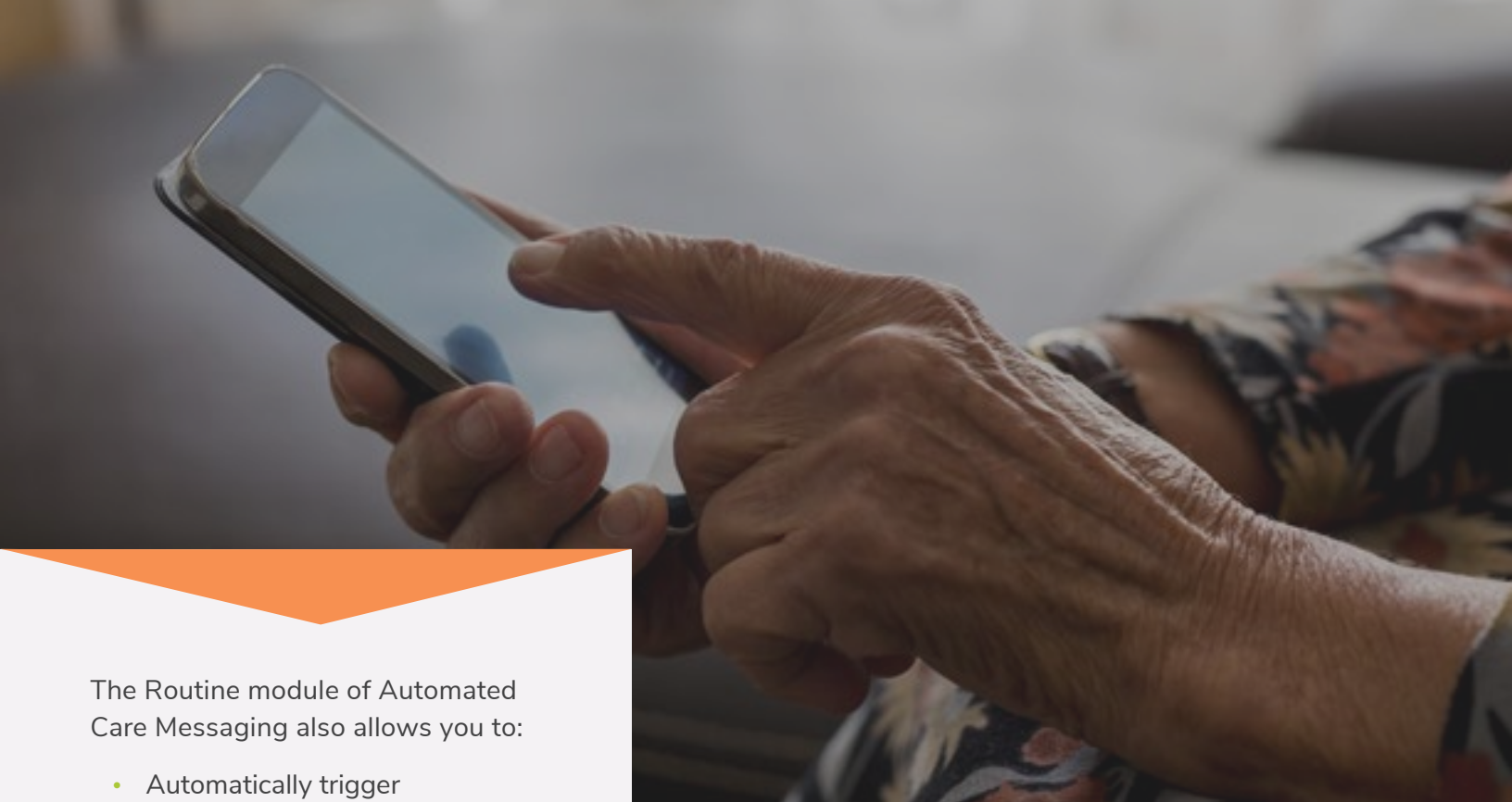
Use every available tool to remind staff and residents of their compliance rights and responsibilities.



Tip! Use automated messaging for secure communications

An automated messaging system such as [Cliniconex's](#) Automated Care Messaging system provides a centralized way to send secure messages on compliance and other issues to specific targeted groups via voice, text or email. You can view the messages sent and get detailed reports showing outcomes.

You can also send staff reminders for training programs, helpful tips, audit/infraction updates and helpful reminders on compliance-related issues.



The Routine module of Automated Care Messaging also allows you to:

- Automatically trigger notifications to families when an event is added to a resident's calendar
- Respond to a family's request to confirm, cancel or request a callback
- Create custom workflow rules to trigger messages
- Trigger workflows based on responses
- Customize messaging by facility, event type
- Log communications and outcomes in resident charts.

Clear measurements and audits

There's an old adage that you can't manage what you don't measure; this is clearly the case with compliance. Otherwise, how could you know if your program is working? You can rely on your internal audit department or hire an auditing company to support your efforts. Use the information to refine your plan and share it so everyone knows exactly where they stand. Results should be built into your communications outreach.

Respond to detected offences

Enforcement and disciplinary provisions are needed to build credibility into your compliance program. They need to be consistent and appropriate, including termination. At the same time, you need to ensure flexibility for mitigating circumstances. Everyone needs to understand their role in this process.

Stay current with regulatory change

Laws, regulations and standards change and you need to be able to change with them. Your compliance program is not a one-and-done. It needs to be updated at least annually (or more depending on if new regulations are announced) to ensure that you are meeting your compliance requirements.



UNDERSTANDING THE PITFALLS OF NON-COMPLIANCE

Now that you know what compliance is and how to build a plan, what exactly is *non-compliance*? In general, non-compliance is when individuals do not follow the rules, regulations and laws that relate to healthcare practices.

While non-compliance can cover both internal and external rules and regulations, most healthcare non-compliance issues deal with patient safety, the privacy of patient information and billing practices.

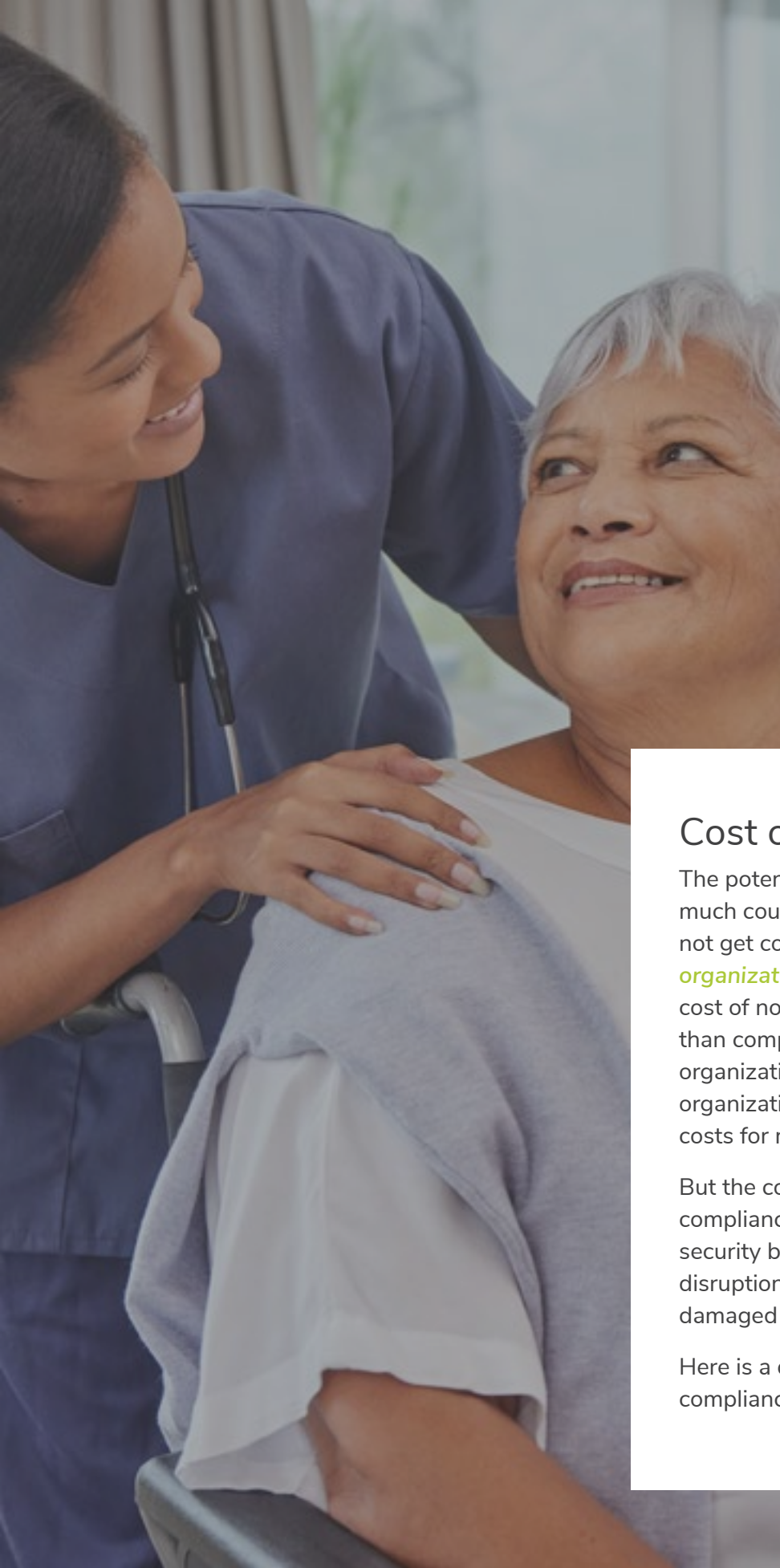
Ordinary vs. gross negligence

It's important to understand the difference between ordinary non-compliance versus gross negligence.

The key difference is based on whether the healthcare organization willfully or voluntarily knew they were putting their clients in danger.

Putting strong policies and procedures in place can help safeguard you against this risk because it demonstrates that you have put processes in place, even if they were not followed exactly. Simply put, establishing systems, protocols and safeguards from the start will reduce your liability.

While PHIPA compliance is often thought of as the only real concern, the consequences of non-compliance are a much broader topic than just meeting PHIPA or PIPEDA requirements. Your organization must also comply with an array of other requirements, including federal and provincial regulations, accreditation standards, internal policies and procedures and financial requirements, just to name just a few.



Cost of non-compliance

The potential risk involved is far-reaching. How much could it cost your organization if you do not get control of this issue? [This study of 46 organizations by the Ponemon Institute](#) put the cost of non-compliance to be about 3.5 times higher than compliance (\$820/employee for non-compliant organizations vs. \$222/employee for compliant organizations), with an average of \$9.6 million in costs for non-compliant organizations.

But the costs go beyond just dollars. Non-compliance leaves you at risk for financial losses, security breaches, license revocations, business disruptions, poor patient care, erosion of trust and a damaged reputation

Here is a quick overview of the impact of non-compliance.



Security breaches

With more healthcare providers switching to digital systems, and as information is increasingly shared between networks, electronic data breaches are on the rise and becoming a major problem.

Ontario has one of the highest penalties for a privacy breach. An individual found guilty of committing an offence under PHIPA can be liable for a fine of up to \$200,000 or up to one year in prison, or both. An organization or institution can be liable for a fine of up to \$1,000,000.

If a corporation commits an offence under PHIPA, every officer, member, employee or agent of that corporation found to have authorized the offence, or who had the authority to prevent the offence from being committed but knowingly refrained from doing so, can also be held personally liable.

In Quebec, failure to comply with its requirements for the collection, storage, communication or use of personal data may result in a fine of up to \$10,000 and \$20,000 for a subsequent offence. The same fines apply to anyone who hampers an inquiry or inspection by communicating false or inaccurate information.

In Alberta and British Columbia, the fines can be as high as \$100,000.



NEW NATIONAL STANDARDS

Recently, Canada released a new set of national standards focused on improving long-term care homes. The Health Standards Organization (HSO) published 60 pages of comprehensive standards, complimenting the release of 115 pages of standards from the Canadian Standards Association Group (CSA).

The two sets of standards are designed to work in tandem with one another, and address everything from preventing falls and maintaining flexible meal schedules, to end-of-life-care and emergency preparedness planning.

Taking lessons learned from the pandemic, the standards include recommendations for more flexible visitation policies that consider residents rights with health and safety, as well as updated recommendations on infection prevention and control.

For the physical long-term care homes themselves, there are new guidelines pertaining to bathroom access, outdoor access and dedicated hand hygiene sinks for every level of a long-term care home, as well as guidance on waste management, video monitoring, signage and the design of staff rooms.

It should be noted that these standards are currently voluntary.



USING TECHNOLOGY TO EMBRACE COMPLIANCE

A recent [OECD Report Empowering the healthcare Worker: strategies to make the most of the digital revolution](#) points out that failure to leverage digital technologies to deliver the right information and knowledge at the right time is a significant missed opportunity to improve care.

“**For instance, 10% of patients are unnecessarily harmed during care, most frequently due to information and knowledge not reaching the right person at the right time. The health burden of this shortcoming in OECD countries is on par with that of diseases such as multiple sclerosis and some cancers.**

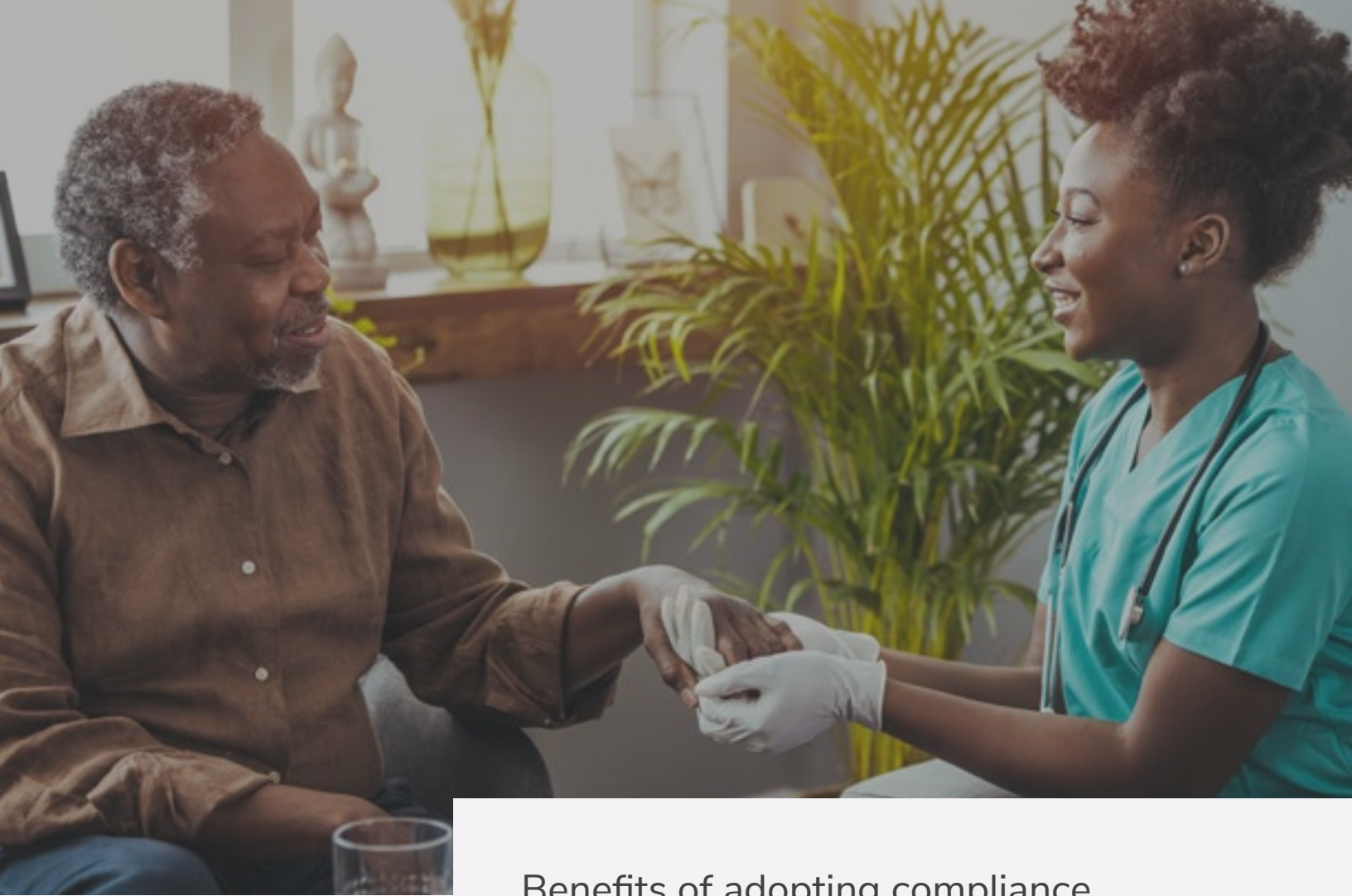
Given this backdrop, and the hefty fines that can result, the imperative for embracing compliance technology has never been more imperative.

In general, compliance technology is anything that helps you meet data security, cybersecurity and any other regulations you are expected to follow. Compliance technology was initially nothing more than secure storage. Today, it consists of various tools that allow you to keep up to date with new and evolving regulations.

While you can deliver compliance management and assistance without relying on technology, you will find this an increasingly unsustainable approach.

Using technology to improve compliance can involve several processes, including:


- Automating processes and workflows, such as the checking of documents or the monitoring of security systems
- Organizing data in line with the regulatory frameworks
- Storing and managing data
- Streamlining reporting processes
- Making the compliance processes more accessible, enabling residents to be more engaged in their compliance activities.



Benefits of adopting compliance technology outweigh the costs

Adopting compliance technology:


- Demonstrates to regulators your commitment to compliance
- Increases staff productivity and returns the time spent on manual processes to care; this improves overall resident and staff satisfaction which is directly linked to your reviews
- Reduces risks, ensures compliance and helps you pass audits which, again, improves your reviews
- Better detects a compliance risk or breach and notifies you automatically that a response is required
- Automates manual processes (such as record keeping) that can automatically prevent non-compliance in areas that were once rife with infractions
- Cross-functional reporting helps you find, prioritize and respond to the risks, streamlines performance and drives business.



Tip! Financial support to implement compliance technology

The **Canada Digital Adoption Plan** may be able to provide loans and advice if you are ready to move forward on your digital adoption plan, and similar provincial programs exist. The **Business Development Bank of Canada (BDC)** can help with a 0% interest loan of up to \$100,000. BDC supports small and medium-sized businesses in all industries and at every stage of development.

The Boost Your Business Technology grant gives you up to \$15,000 to get advice and up to \$100,000 in interest-free loans to implement the technologies that can propel your business forward.



As part of its commitment to promote quality resident care in Ontario's long-term care homes, the Local Health Integration Networks (LHINs) allocates long-term care (LTC) home funds through a mechanism known as the **Level-of-Care (LOC) envelope funding system**. Under this system, computer hardware and software specifically dedicated to supporting NPC resident care services such as the development of care plans, electronic patient files, medication administration records and related records and documents are eligible.

WHAT IS REGTECH ANYWAY?

One term you are going to be hearing a lot about is RegTech. RegTech is **a class of software applications for managing regulatory compliance**. It employs various technologies, including machine learning and artificial intelligence, to build enterprise-wide data governance and reporting. RegTech companies use cloud computing technologies through SaaS to help companies comply with regulations. SaaS or Software as a Service is a way of delivering applications over the Internet—as a service. Instead of installing and maintaining software, you simply access it via the Internet, freeing your company from complex software and hardware management.

RegTech was born after the 2008 financial crisis that resulted in stricter financial sector regulation. It is a subset of FinTech—a group of technologies designed to automate the use and delivery of financial services. It stands for companies looking to solve challenges of a technology-driven economy as a result of increased data breaches, cyber hacks and other fraudulent activities. RegTech makes use of machine learning and big data technologies to reduce risks and support compliance.

These new technologies are intended to replace the current manual analysis and reporting methods. Companies invest in RegTech as a way to save time and money, allowing resources that were once devoted to regulatory compliance to be diverted to patient-centred care.

Global RegTech spend will exceed \$204 billion by 2026; accounting for more than 50% of all regulatory compliance spend for the first time. This spend will grow from \$68 billion in 2022; representing growth of some 200% over the next four years.

Ontario's 626 licensed long-term care homes are estimated to spend between \$20 to \$23.8 million on compliance which translates to about \$38,000 per home.

With healthcare being a highly-regulated industry and the time, cost and potential errors in a manual compliance process, healthcare is ripe for RegTech innovation. The automation of processes could significantly increase the efficiency and effectiveness of healthcare services, along with promoting a healthy bottom-line.

CHALLENGES AND OPPORTUNITIES

Like financial services, healthcare is a highly-regulated industry where non-compliance can result in severe financial and reputational consequences. Unfortunately, there is not a lot of data and research available on the maturity of RegTech in the healthcare industry. However, limited parallels can be drawn between the two industries, particularly when it comes to the challenges and opportunities.

Although some of the steps toward establishing a compliance program through RegTech may be clear based on lessons learned from the financial industry, there's a long road ahead.

Tip: IT compliance checklist

IT compliance refers to the guidelines you must follow to ensure your processes are secure. Each guideline refers to rules for data, digital communications and infrastructure. When it comes to building infrastructure, the end goal is to safeguard data.





Before hiring a vendor, consider the following in your evaluation criteria:

- **Monitoring and reporting:** does it give you a real-time assessment of your systems?
- **Ease of use:** any software will fail if it's difficult to use or if the training is minimal and not built into your overall training and onboarding programs. If you want buy-in, involve the people who understand the requirements better than anyone—your staff.
- **Accessible software:** software must be accessible from any device—laptop, desktop, tablet, or phone.
- **End-to-end security:** it must be built and authenticated by a third party to make sure your data is protected.
- **Secure storage:** cloud-based solutions are widely considered more secure than locally hosted systems.
- **Reliability:** with staff shortages and other challenges facing the industry there should be virtually no wait time for queries, searches or analytics.
- **Easily updateable:** make it easy for staff to add fields, customize page layouts and modify the configuration to accommodate changing regulations, new requirements or evolving priorities—without the help of IT or your software vendor.
- **Easily accessible:** allows you to access all relevant documentation, see the current status, and communicate across departments, functional areas and locations without leaving the platform. Every activity needs to be automatically logged for a clear audit trail.
- **Automation:** needs to automate workflows, assessments, alerts and action plans.
- **Integrate with other functions:** such as third-party risk management, internal audit and other risk management functions to give you an accurate picture of your total risk.
- **Customizable dashboards:** to give you a clear picture of the metrics you care about most.
- **Click and point reporting:** critical for regulatory submissions, a comprehensive overview for executives and drill-down capabilities for tacticians.

Most standards fall into these categories:

- **Access and identity control** defines authentication and authorization rules.
- **Strict control protocols for data sharing** with the public and residents.
- **Incident response** guidelines on how you will mitigate, report and investigate a data breach.
- **Disaster recovery** defines your disaster recovery plan if your infrastructure fails.
- **Data loss prevention** spells out what you will do to protect business revenue and productivity, including backups, recovery and redundancy.
- **Protection against malware** across your IT environment, including servers and user devices.
- **Corporate security policies** to outline steps that staff must follow to protect data.

LACK OF INDUSTRY AND TECHNICAL EXPERTS

Like many other areas in the field, there is a critical lack of compliance officers in healthcare with RegTech experience, developers and project managers with the requisite skills, inconsistent regulations from jurisdiction to jurisdiction, cybersecurity threats and a dependence by many companies on legacy or manual systems.

Prophecy Market Insights, a specialized market research, analytics, marketing and business strategy and solutions company, said in a **recent article** that heavily regulated industries equals a complex industry.

“**The general elements of a successful compliance officer in this field might well be similar to other industries, i.e experience in public policy, law, loss prevention, and strategic management, coupled with an agile workstyle and innovative mindset,**” Prophecy says. **“However, the specific knowledge is not as easily transferable and experience built up in the sector is extremely valuable**

CYBERSECURITY THREATS MAJOR CHALLENGE

According to the **Chief Healthcare Executive** cyberattacks continued to target hospitals and health systems. Cybersecurity refers to today’s defences of networks, data systems and programs from outside digital attacks. Holistic cybersecurity maintains safe and secure computer networks and all their accompanying data, files and programs while protecting against breaches, leaks or unauthorized access.

Cyberattacks are proving to be very costly to hospitals and healthcare settings. **The average healthcare breach now costs more than \$10 million**, according to an analysis by IBM Security. Cyberattacks also pose **serious risks to patient safety**, and security experts have implored health systems to bolster their defences to protect patients.

Packetlabs, a Canadian cybersecurity firm, says security weaknesses are costing organizations billions of dollars in losses and that the cybersecurity landscape continues to be unrelentingly risky. According to the **Canadian Chamber of Commerce**, 35% of Canadian businesses are planning to implement new cybersecurity measures but that “leaves 65% with the mindset that they are not impacted by cybersecurity or don’t know how to address increased cyber risk.”

Packetlabs says that 80% of global companies reported they suffered from a **cybersecurity skills gap**. “However, there are some positive developments. For example, cybersecurity product developers have started to incorporate machine-learning capabilities into the endpoint and network detection and response agents which reduces the burden on human analysts.”


Strong compliance management can help to manage this threat because it is the process of ensuring all workflow, internal policies and IT initiatives align with specific industry cybersecurity regulations. Your compliance efforts must be ongoing because the digital attack surface is always expanding.

According to builtin, a career site dedicated to matching industry experts with industry needs, one of the difficulties with regulating [cybersecurity](#), and a deterrent up until this point, is that it is [an industry founded in](#) rule-breaking. How do you regulate a sector built to protect computer systems when the groups it is offering protection from operate outside of any rulebook, and constantly devise new means of breaching the systems they're targeting? Any regulatory framework can never be truly current; it's a question of being as up-to-date as possible, rather than absolutely so.

In the United States, the government has used its discretion in penalizing HIPAA noncompliance "occurring in good faith" during the pandemic (a public health emergency) and beyond. This meant that the provision of telehealth services, for example, "allowing providers to deliver care through a broad range of devices and technology platforms," according to [this article](#) by attorneys at Faegre Drinker Biddle & Reath.

The Office of the Inspector General says it used the pandemic as a time to [investigate illicit areas of telehealth](#), such as scams that leverage aggressive marketing (for instance cold-calling patients) or provide fraudulent telemedicine services. The government will use these findings to [prioritize enforcement](#), with the Department of Justice's Healthcare Fraud Unit explicitly stating it is "dedicated to rooting out schemes that have exploited the pandemic."

As such, it will be important for healthcare providers to provide records of their historical and ongoing marketing communications, including email campaigns and websites, in order to prove compliance.



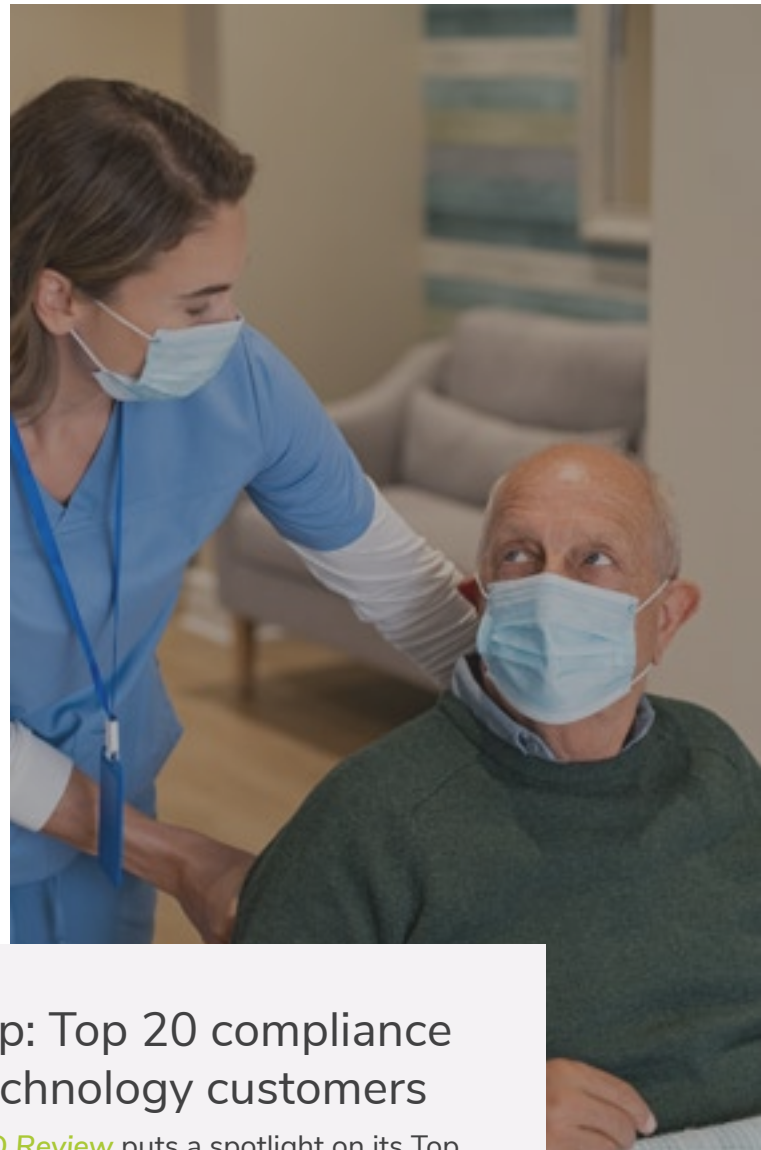
Tip: Automated Care Messaging keeps all historical messaging safely stored and easily retrievable

With [Cliniconex's](#) Automated Care Messaging (ACM) you can track all historical records. ACM sends out targeted messages to residents, families and staff in minutes via voice, text or email; logs all communications in resident's charts; syncs family contacts with a company's EHR; and, automates day-to-day messaging with workflow rules.

The Routine Module of this automated care messaging also allows companies to automatically trigger notifications to families when an event is added to the resident's calendar. Families can then confirm, cancel or request a callback and workflows can be triggered based on responses.

You can also:

- Create custom workflow rules to trigger messages
- Customize messaging by facility, event type
- Families can confirm, cancel or request a call back
- Workflows can be triggered based on responses
- Communications and outcomes are logged in resident charts



Tip: Top 20 compliance technology customers

CIO Review puts a spotlight on its Top 20 Compliance Technology Solutions Companies for 2022.

It points out that AI and ML-based chatbots are being steadily adopted to eliminate time-consuming manual compliance-related activities. Robotic process automation (RPA) is another advanced technology that can streamline workflows, and reduce manual effort. RPA software tools can automate report generation and delivery, e-mail circulation, status updates, notifications, change tracking and different asset compliance programs.

In the wake of these developments, CIO Review reports that the global compliance technology market is projected to reach compound annual growth rates of 8.5% by 2025.



THE FINAL WORD

As outlined in this white paper, there are many challenges facing the future of compliance in the global healthcare industry such as lack of skilled technical expertise, slow adoption of new technology with its associated costs, ensuring interoperability for data sharing, reimagining the way work is done and putting the legal, regulatory and security frameworks in place.

It's a new endeavour for many healthcare providers and, in fact, for the industry itself looking to deliver the technology and expertise needed to grapple with the complexity of differing regulatory rules, cybersecurity and ways to integrate with legacy systems.

Whether you are compelled by:

- Ever-changing rules and regulations
- The need to cut costs and improve efficiency
- Recruit and keep your staff
- Attract investors and new clients...

It is clear that the cost and effort associated with embracing healthcare compliance using digital technology, far outweighs the risks of failing to put a strong compliance program in place.

It gives you:

- Security knowing you are doing everything you can to protect your bottom line and improve efficiency
- Tools to meet your regulatory requirements
- Safety guards and protocols to deal with cybersecurity threats
- An enhanced reputation which, in turn, helps you to attract new residents
- The ability to retain and recruit staff; and most important of all
- Liberate your care staff to do what they do best—provide patient-centered care.