4 Keys to Developing Privacy Culture in Multidisciplinary Clinics

October 28, 2020

In multidisciplinary clinics, protecting the privacy of patient information is everyone's business. But most clinics are thinking about privacy all wrong.

Here are some of the privacy risk factors affecting the healthcare industry:

1. **Change.** Healthcare technologies and environments are never stagnant. Their privacy needs are evolving constantly. From interdisciplinary models of care to interoperability, clinics themselves are complex ecosystems that have many variables to keep track of.
2. **The human factor.** It is unavoidable, and still one of the most common causes of healthcare data breaches. Examples include stolen or lost assets, insider and privilege misuse (1), and miscellaneous errors, such as improper device disposal or mishandling PHI.
3. **New technologies need time to mature.** Whether it's the latest medical device or a cloud-based health app, most new products enter the market with an inadequate level of security.
4. **Laws also need time to catch up with privacy risks.** The rapid technological and structural changes catalysed by the COVID-19 pandemic have outpaced Canada's privacy laws, leaving the healthcare sector inadequately protected. (2)
5. **Lacking the right resources.** Compared to large hospitals, multidisciplinary clinics and other smaller organizations may lack the resources and ability to support secure system architecture.

As we've seen, healthcare providers have customer, regulatory, and legal incentive to invest in developing a culture of privacy awareness and protection.

Understanding PHIPA

Ontario businesses, including all disciplines of health clinics and solo practitioners, are required to handle personal information in accordance with the Personal Health Information Protection Act (PHIPA).

In Ontario, personal health information (PHI) includes any and all information related to the provision of health care for an individual's physical or mental health. This includes:

- Family history
- Personal identification information
- Plans of service
- Payment information
- Eligibility for care
- Information regarding body parts or substances
- Health numbers

PHI also includes any other information that can identify either the individual or a substitute decision maker who acts on the individual's behalf. (3)

4 Keys to Developing Privacy Culture in Multidisciplinary Clinics

1. Conduct an assessment:

The first key is to assess the organization's current PHIPA compliance infrastructure. This could involve a few measures:

- Conducting an inventory of the organization's current privacy and security programs, policies and procedures; general staffing levels; and overall resourcing. This allows the organization to map out its current situation and determine how it wants a privacy culture to look like.
- Taking an inventory of past security incidents and compliance monitoring. This will help identify gaps in terms of training, privacy and information security.

Once an assessment is conducted, the organization can then determine its goals and how it wants to integrate a privacy culture into the workplace.

2. Make a budget:

The organization needs to Identify what will be required in terms of time, money and resources to carry out the integration of a privacy culture. Considerations include:

- What will be needed to help any staff member, contractor, or other non-healthcare provider who lacks basic privacy frameworks to get off the ground, either on their own or in partnership with the health team.
- What it will take to address any significant variations that may exist among the health team's PHIPA compliance programs.

3. Set realistic procedures and timeframes:

A plan and a timeframe for privacy integration should consider items such as:

- The specific tasks and responsibilities associated with the integration effort and the available resources that can be allocated to it.
- Which members of the organization will lead the various components of the integration effort, taking into account their expertise, resources and other relevant considerations.
- How this privacy integration timeframe will mesh with the organization's other priorities.
- Defining the scope of access to health records and other medical information.
- Determining how the organization will deal with violations with a discipline policy that reflects the goals of the organization.

4. Foster communication with managers, staff and physicians:

For many organizations, this means providing training opportunities in privacy. Types of training could include:

- New hire orientation training that covers PHIPA requirements and other policies and procedures of the organization
- In-person training to address specific organizational needs
- Remedial training for privacy violators
- Establishing communications (e.g. a website, email address, and hotline) for a "privacy office" where privacy issues can be reported and addressed.

Conclusion

A single data breach can destroy an organization's reputation. As medical futurist Bertalan Meskó has noted, "there is no digital health without sacrificing a part of our privacy." Investing in data privacy is no longer a question of "why", but of "how". (4)

MedThree can help protect your healthcare clients. For more information about our insurance products, visit our website.

Content is current as of the date of broadcast and is subject to change without notice.

Sources:

1. *Read about a recent case of insider misuse here:* https://www.canadiansecuritymag.com/toronto-hospital-network-says-info-of-about-150-patients-allegedly-stolen/?utm_source=rss&utm_medium=rss&utm_campaign=toronto-hospital-network-says-info-of-about-150-patients-allegedly-stolen
2. https://www.canadianunderwriter.ca/insurance/covid-19-pandemic-accelerating-digital-privacy-risks-federal-watchdog-warns-1004198224/
3. https://jane.app/guide/privacy-and-security/privacy-compliance-for-clinics-in-ontario
4. https://www.linkedin.com/pulse/your-privacy-digital-health-era-medical-futurists-mesk%C3%B3-md-phd/?trk=eml-email_series_follow_newsletter_01-hero-1-title_link&midToken=AQEYNWs0gW9DrQ&fromEmail=fromEmail&ut=1_bhs5E2GdA9s1