CLINIC SECURITY CULTURE

DTO Doctors Technology Office
A GPSC initiative

What is security culture?

Security culture in physician offices relies on employee work habits that consider the safety, confidentiality, and security of patient information. Security is not a one-time event; it is an ongoing practice that can be integrated into day-to-day clinic operations. Effective security culture requires involvement from the entire team. An appointed Privacy Officer, the clinic physician, is in charge of overseeing and maintaining this work culture by documenting proper work procedures, handling proper security training, and implementing measures to mitigate security risks.

Common security threats

Security is often perceived as an IT issue when it is in fact a patient care issue. While security threats are not always malicious, they can cause information damage or loss, disrupt patient care, and violate the privacy and confidentiality of patients and/or employees. To ensure the security of private patient information, physicians and staff must understand potential threats.

Privacy breach

A privacy breach is when unauthorized access, collection, usage, disclosure, or disposal of patient personal information occurs.

Security incident

A security incident is an unwanted incident with the potential to harm people, information systems, and the clinic.

Why is security culture important?

Everyday clinical tasks have the **potential** to be a privacy or confidentiality violation. Workarounds that seem minor can have a big impact in maintaining the security of patient information.

When an incident results in information loss or damage, or becomes a privacy breach, the outcome can be painful. Possible harm can impact patients, doctors, clinic staff and families.

Potential impacts

- Medical harm
- Loss of patient trust
- Financial loss
- Legal liability
- Criminal acts like identity theft, fraud, or blackmail
- Failure to meet professional or certification standards
- Damage to a clinic's reputation

How can we begin to implement it in our clinic?

Discuss with your clinic staff

By bringing awareness to security culture, it encourages active participation. This engagement allows for your clinic to be on the same page, leading to opportunities for developing security training routines.

Perform a preliminary assessment

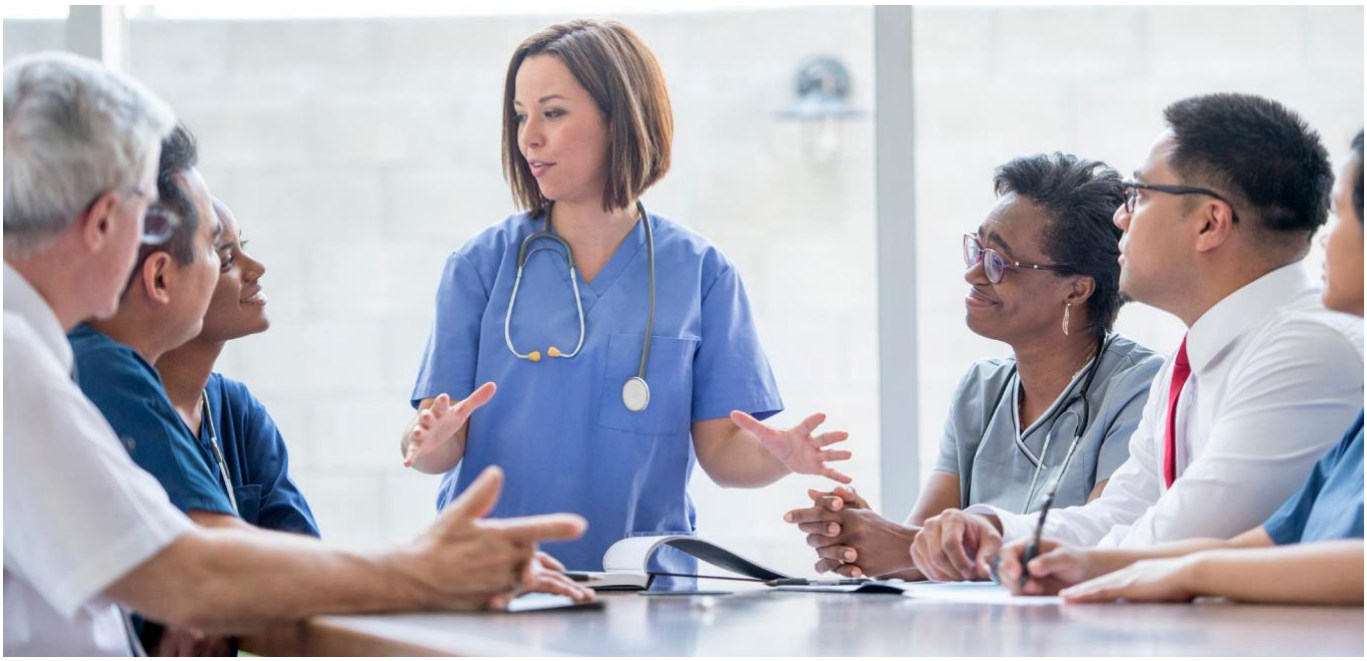
Take the time to go through everyday tasks and habits to see if there are any flaws that could lead to a security incident. Being mindful of your clinic's practices will help establish a starting point for where to begin.

Create written documentation

From the preliminary assessment, implement guidelines for topics such as password and device management. This pro- vides a foundation and resource for your clinic to access for any questions or uncertainties.

Unsure how to start?

See our Physician Office Security Tools and Resources catalogue for guides your clinic can follow and adopt.



Security culture thrives when teams exercise that:

It belongs to everyone

Everyone in the clinic takes responsibility for creating a safe and secure environment for patients and staff

It is a mindset

Each individual has access to private information and they are accountable for keeping that in- formation safe.

It is an ongoing effort

Security practices should be integrated into daily thinking and decision-making processes.

For more information, guidance, or support contact:

Doctors Technology Office

604 638-5841
DTOinfo@doctorsofbc.ca
www.doctorsofbc.ca/doctors-technology-office