HealthCareCAN
Leading. Innovation. Together.

DECLARATION OF COMMITMENT TO CYBERSAFE HEALTHCARE

In the 21st Century, patient safety depends on cybersecurity. Cyberattacks can affect patient care systems and medical devices. They can disrupt communications and supply networks and threaten the integrity and confidentiality of health records, as well as other foundations of modern healthcare. On the other hand, digital solutions can be an important source of resilience for critical infrastructure, enabling access to care even when local health services are disrupted.

We, as representatives from the organizations listed below, recognize the importance and urgency of protecting critical infrastructure systems and data against cyber threats in Canadian health care organizations. Our approach is consistent with the National Strategy for Critical Infrastructure endorsed by federal, provincial, and territorial governments, as well as the Action Plan for Critical Infrastructure.

In moving ahead, we are mindful of the potential of digital solutions to promote broader critical infrastructure resilience and of the challenges in safeguarding health care against cyber threats in a continuously-evolving security environment. We also recognize that cyber incidents can affect critical health care systems worldwide with catastrophic consequences, including the availability of information and communications technology systems, and the integrity and confidentiality of data, all of which the health care sector is increasingly reliant on.

Advancing cybersecurity in Canada's health sector requires collective, collaborative action. Together, we commit to taking six tangible actions to increase cybersecurity preparedness and resiliency:

1. **Champion:** Championing cybersafety in Canada's health sector;
2. **Inform**: Ensuring that our leaders, staff, and partners are informed about the scope of the challenge and opportunities to mitigate risk;
3. **Contribute**: Contributing to shared action plans that build collective resilience to cyberattacks;
4. **Advance**: Progressing cybersafety in ways consistent with our mandate, considering opportunities for prevention, mitigation, preparedness, response, and recovery;
5. **Share**: Sharing information, best practices, and tools with others within and beyond the health sector to build collective capacity and resilience; and
6. **Transparency**: As each organization's circumstances and capacity are unique, we will confirm by Cybersecurity Awareness Month in October 2018 how we will apply these commitments in our unique context and/or with our community.

Through these actions, we are committed to fostering a robust, safe, and effective health system that benefits those we serve.

_____ _____

Name Organization