

TO: Chair and Members of the Finance & Facilities Committee

FROM: Christopher Mackie, Medical Officer of Health / CEO

DATE: 2018 November 1

---

## **CYBER INSURANCE**

### **Recommendation**

*It is recommended that the Finance & Facilities Committee receive Report No. 039-18FFC re: “Cyber Insurance” for information.*

### **Key Points**

- Cyber insurance coverage in the amount of \$5 million, to address cyber, network, and data exposures not specifically covered under the current comprehensive insurance policy, was initially sought as a requirement for entering into a particular data-sharing agreement.
- Cyber insurance covers invasion-of-privacy loss involving personal or confidential data in electronic form stored both on MLHU’s computer systems and on third-party-controlled shared computer networks.
- Three bids were received, and the lowest acceptable quote, in the amount of \$10,250, has been accepted.

### **Background**

The Middlesex-London Health Unit was asked to seek appropriate privacy breach (or “cyber”) insurance to be eligible to participate in ClinicalConnect, a secure on-line Shared Network Arrangement to access or share health-related data administered by the Hamilton Health Sciences Corporation. The Health Unit was asked to confirm that it has appropriate cyber insurance in the amount of \$5 million.

Through subsequent investigation, it was determined that for MLHU, privacy breach exposure extends well beyond participation in an SNA. Recent Ontario privacy breaches in the news, including cases of unlawful access to and public disclosure of sensitive confidential information, have raised significant concerns about how institutions in the public sector safeguard client data. By canvassing other health units and investigating best practices in the health sector, MLHU has determined that acquiring appropriate cyber insurance is an important component of an overall strategy to secure and safeguard client records and confidential information, and protect MLHU from financial risk.

Cyber insurance provides coverage for the following situations:

- Privacy breach due to technological failure, as costs involved in restoring MLHU’s reputation;
- Privacy breach where data is supplied to a third-party service provider and/or under an SNA;
- Media exposures, such as defamation and breaches of intellectual property rights, arising from on-line disclosures;
- Failure of network security to protect against unauthorized access;
- Failure to safeguard sensitive personal information entrusted to MLHU;
- Extortion threats from a hacker;
- Crisis management expenses after a network compromise; and
- Business interruption costs during a period of network restoration.

## **Risk Mitigation Requirement**

Currently MLHU's risk of cyber/privacy breach is heightened by several factors, which include (but are not limited to):

- An increasingly mobile workforce, resulting in more remote-accessing devices (e.g., rollout of Activity-Based Workspaces and Alternative Work Arrangements);
- Data-sharing arrangements with other organizations (e.g., ClinicalConnect);
- Introduction of new technology programs (e.g., Electronic Medical Records and an Enterprise Resource Planning system that includes employee self-service components); and
- Evolving technology platforms, such as moving toward cloud computing and an increased capability to collect online payments.

As an organization that stores and maintains personal client information, and with large and growing numbers of devices that connect to MLHU networks, opportunities for malicious parties to access the organization's assets are increasing. The growing risk of ransomware is a threat that, if realized, would have a negative impact on public relations, compromise data security, and present challenges from a data-recovery perspective. Therefore, in order to mitigate the risks in this area, it is recommended that MLHU enter into a cyber insurance contract.

## **Cyber Insurance Quote and Application Process**

In order to obtain quotes, Finance, Information Technology, and Operations worked together to complete applications to three prospective insurers identified by other parties within the industry they service (public health). MLHU's current comprehensive insurance policy broker was included in this process. Three quotes were received, with Holman Insurance Brokers Ltd. submitting the lowest acceptable bid, at \$10,250 plus applicable taxes. The insurance company that this broker represents, CFC Underwriting Ltd., is an experienced insurance provider serving the health sector on a global scale. In a survey of other health units, several respondents confirmed that they had recently added cyber insurance as part of their enhanced risk-mitigation programs, while others indicated that they were in the process of adding cyber insurance to their overall coverage in light of sensitivity over unauthorized access to personal records and confidential data maintained by institutions within the public health sector.

This report was prepared by the Healthy Organization Division.



Christopher Mackie, MD, MHSc, CCFP, FRCPC  
Medical Officer of Health / CEO