



Healthcare Materials Management Services

Privacy and Confidentiality Requirements for Suppliers

Dear Supplier:

Healthcare Materials Management Services (hereafter referred to as HMMS) with offices located at 188 Stronach Crescent, London, Ontario is a joint venture between the London Health Sciences Centre (LHSC) and St. Joseph's Health Care, London (SJHC), created to integrate and consolidate the functions of Purchasing, Contract Management, Accounts Payable, and Inventory Management. HMMS also provides services to other organizations (Affiliates) including other joint ventures of LHSC and SJHC. HMMS has the authority to negotiate and sign contracts on behalf of LHSC, SJHC, and Affiliates.

The Ontario government enacted the Personal Health Information Protection Act (PHIPA) on November 1, 2004. PHIPA is a provincial law that governs the collection, use and sharing of personal health information and patients' right to have that information kept private, confidential and secure. HMMS, London Health Sciences Centre, St. Joseph's Health Care, London and associated Affiliates are required to comply with PHIPA.

HMMS on behalf of LHSC, SJHC, and associated Affiliates expects its suppliers to comply with the Supplier Compliance Statement that includes expectations related to privacy and confidentiality. Patient privacy is of paramount importance to us and we recognize that our responsibilities extend to the Suppliers with whom we conduct business.

Please review the following Supplier Compliance Statement

If your firm is compliant with the Supplier Compliance statements, it is not necessary to respond to HMMS.

If your firm is not in compliance with the Supplier Compliance statements, you must immediately notify Toby O'Hara, General Manager, HMMS, indicating the specific area(s) of non-compliance including a timeline and process for remediation.

Mailing Address:
Healthcare Materials Management Services
188 Stronach Crescent
London, ON
N5V 3A1

Email:
toby.o'hara@sjhc.london.on.ca

Ontario Health Privacy Legislation

All Suppliers of equipment and services to HMMS and its Customers (see listing at www.hmms.on.ca) must comply with the following statements:

All Suppliers must:

1. Be in compliance with all applicable Privacy laws, including PHIPA.
2. Keep current a Privacy policy, which assigns a key contact person for your company for privacy issues, outlines a process for dealing with privacy complaints, and defines a breach management process in the event of inappropriate use of personal health information by their staff and/or subcontractors.
3. Upon request, share your privacy policy with HMMS and/or notify HMMS of any changes made to your privacy policy during the term of any contract.
4. Educate your employees on privacy laws and policies and take reasonable steps to ensure employee compliance through staff training, confidentiality agreements and employee sanctions. Ensure those employees who resign or are terminated return all information belonging to HMMS and its affiliates and that they are prevented from accessing facilities physically and/or this information electronically.
5. Comply with permitted uses of identified or personal health information as specified by contractual agreement and PHIPA and its Regulations.
6. Use effective administrative, technological and physical safeguards to protect and secure the information to reduce risk of loss, theft, and unauthorized access. Measures may include anti-virus protection software, backup security, encryption software and the development and maintenance of acceptable business recovery plans.
7. Ensure the accuracy of records of personal health information under the Supplier's custody and control as specified by PHIPA and its Regulations.
8. Comply with any special requirements that may be required by the contractual agreement related to audits, privacy impact assessments, threat risk assessments.
9. Only use and disclose the information HMMS shares or is made available as needed to fulfill the contract, subject to PHIPA.
10. Give subcontractors access to personal health information belonging to HMMS/affiliated only with HMMS prior approval and if the subcontractor agrees to maintain the same privacy and security provisions as outlined in your agreement with HMMS.
11. Upon request, provide HMMS reasonable access to inspect your premises, security practices, books and records to ensure you are in compliance with the terms for the Supplier Statement of Compliance and/or PHIPA legislation.

12. Notify HMMS promptly and in writing if it becomes aware of a security threat or breach relating to HMMS or its affiliates' information, which includes, but not limited to theft and/or inappropriate use of personal health information.
13. Immediately revoke any user's access if security is breached and/or on HMMS' request.
14. Comply with any stipulated sanctions for breaching the contract, including ending the contract.
15. Return or securely destroy, as specified by contractual agreement, all information received or created in performance of the agreement when the contract ends, and where this is not possible, keep the contract's privacy and security measures in place to protect the remaining information.
16. Agree that HMMS and its affiliates retain custody and control of all personal health information and can not be denied access due to late or disputed payment for services.
17. In consultation with Area Leadership, ensure any patient-identifying information is removed from medical equipment/device(s), which was brought into the organization for evaluation, or any equipment sent off site for repair, prior to this equipment/device leaving the hospital premises.

Healthcare Materials Management Services reserves the right to:

1. Take legal action against Suppliers for violating privacy and confidentiality provisions of the contract and an acknowledgement that HMMS has been irreparably harmed.
2. Hold vendor responsible for any and all costs incurred by HMMS due to the supplier's failure to sufficiently protect HMMS' PHIPA related information.
3. Terminate the contract, order, or agreement, without penalty, for any breach of privacy or confidentiality of confidential information or serious breach of the terms of these Privacy and Confidentiality Requirements for Suppliers.

When storing or sharing personal health information in electronic format, HMMS requires its Suppliers to provide, upon request:

1. An electronic record of all access, use and disclosure of information including time and source of access, and
2. A Privacy Impact Assessment and/or a Threat Risk Assessment.