

Privacy and Confidentiality Requirements for Suppliers

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 (St. Joseph's), created to integrate and consolidate the functions of Purchasing, Contract Management, Accounts Payable and Inventory Management. HMMS provides services to other organizations (Affiliates) including other joint ventures of LHSC and St. Joseph's. HMMS has the authority to negotiate and sign contracts on behalf of LHSC, and St. Joseph's.

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, St. Joseph's and associated Affiliates expects its suppliers to comply with the following requirements that include 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.

CONFIDENTIALITY AND PRIVACY

- 1.0 For purposes of this section the term "Confidential Information" shall mean information or data in any format relating to the business and affairs of HMMS, an Affiliate, or of their respective employees, officers, directors, and customers, and includes confidential business information, personal health information (PHI) and personal information (PI) as those terms are defined in both Ontario and Canadian privacy or information protection laws.
- 2.0 The Terms and Conditions of this Agreement are confidential to HMMS and the Supplier, and are not to be disseminated, distributed, or otherwise conveyed to third persons, other than those officials and employees of either party whose duties require knowledge thereof, without the expressed written consent of both parties, except in the pursuit of legal redress in the courts of law or in pursuit of the direction of any competent legal authority. The Supplier shall not issue any public announcement or news release pertaining to this Agreement, without prior written approval from HMMS. If a Supplier makes a public statement in breach of this requirement HMMS shall, in addition to any other remedy it may have, be entitled to take all reasonable steps as may be necessary, including disclosing any information about the Supplier's Proposal or Quote, to provide accurate information and/or to rectify any false impression which may have been created.
- 3.0 Where applicable, the Supplier may, by means of their business relationship with HMMS, have access to confidential information about staff and/or patients and/or business of HMMS.
- 4.0 On signing this Agreement, the Supplier confirms that it is compliant with requirements of both Ontario and Canadian Privacy Laws and anti spam legislation, in that it will use confidential information strictly for the purposes agreed upon by HMMS, and the Supplier. The Supplier confirms that it has a program for education of its staff on privacy, confidentiality and security of information, ensures that employees are

aware of their privacy and confidentiality obligations. The Supplier confirms that employees who resign or are terminated must return all confidential information belonging to HMMS, are reminded of their continued responsibility to maintain the information's confidentiality, and cannot access applications, hardware, software, networks and facilities belonging to HMMS or the Supplier.

- 5.0 On signing this agreement the Supplier confirms that any confidential information regardless of format, obtained by the Supplier or any agent or employee of the Supplier will be kept confidential and secure. The Supplier must use effective administrative, technological and physical safeguards to protect confidential information against such risks as unauthorized access, use, disclosure, copying, modification, disposal, loss or theft. Security measures must include, but are not limited to, antivirus/anti-malware protection software, backup security, encryption software and the development, documentation and maintenance of acceptable data destruction and business recovery plans.
- 6.0 The Supplier agrees that HMMS and its affiliates retain custody and control of all confidential business information, personal health information and personal information and cannot be denied access to the information requested by HMMS due to late or disputed payment for services.
- 7.0 In consultation with area leadership, the Supplier will ensure any patient-identifying information is removed from medical equipment/device(s), brought into the organization for evaluation, or any equipment sent off-site for repair, prior to this equipment/device leaving the hospital premises.
- 8.0 The Supplier will keep current a privacy policy, which assigns a person responsible for privacy compliance, outlines a process for dealing with privacy complaints, and defines a breach management process. Upon request, the Supplier will share its privacy policy with HMMS and/or notify HMMS of any changes made to your privacy policy during the term of any contract. This Agreement confirms that HMMS is authorized to audit the privacy policies and practices and security measures of the Supplier at the discretion of HMMS, and on reasonable notice, HMMS or its representative will be allowed access to inspect your premises, security practices, books and records to ensure compliance with this Agreement.
- 9.0 The Supplier agrees to notify HMMS within one (1) business day and in writing if it becomes aware of a privacy, confidentiality or security breach relating to HMMS confidential information. In that event, the Supplier will consult with HMMS in identifying the root cause of the breach and the affected information, assessing the consequences of the breach, undertaking and implementing possible mitigation measures for the breach such as assistance in recovering lost or disclosed information, and determining appropriate measures to prevent the recurrence of such a breach. Supplier will immediately revoke any users' access if security is breached and/or on HMMS' request. Supplier will comply with any stipulated sanctions for breaching the contract, including ending the contract.
- 10.0 In the event of a breach, HMMS reserves the right to:
 - 10.1 Hold vendor responsible for any and all costs incurred by HMMS due to the supplier's failure to sufficiently protect HMMS' personal and personal health information.
 - 10.2 Terminate the contract, order, or agreement, without penalty, for any privacy breach or serious breach
 - 10.3 Take legal action against Suppliers for violating privacy and confidentiality provisions of the contract and an acknowledgement that HMMS has been irreparably harmed.
- 11.0 When storing or sharing confidential business information, personal or personal health information in electronic format, HMMS requires its Suppliers to provide, upon request:
 - 11.1 An electronic record of all accesses of information including time and source of access, and

- 11.2** A written assessment of how the service the supplier offers may threaten, make vulnerable or risk the security and integrity of the information (Threat Risk Assessment), and how they impact privacy (Privacy Impact Assessment).
- 12.0** On expiry or termination of this Agreement, or upon request of HMMS, the Supplier will cease any and all use of the confidential information and will return it to HMMS, at no cost, including any copies, or will destroy it in a manner designated by HMMS, with proof of destruction.
- 13.0** The Supplier agrees to notify HMMS 30 days prior to and in writing if it will be moving, hosting/storing or backing up data or confidential information relating to HMMS at a facility not identified in this agreement.