London Health Sciences Centre Systems Access Agreement

This document summarizes your obligations when using the London Health Sciences Centre (LHSC) computer network, and its information systems and data. Failure to comply with these obligations may lead to the discontinuation of your hospital network privileges. It is the responsibility of Information Management to monitor and enforce the conditions of this agreement. Any inappropriate use of the network may also result in disciplinary action up to and including termination/loss of privileges.

1. Use of Computer Resources

a. Acceptable Use

LHSC computer resources are allocated to groups and individuals for patient care, research, educational, and administrative purposes only, and should be used in accordance with established policy.

b. Unacceptable Use

Specifically, the following are considered unacceptable:

- accessing, modifying, deleting, copying, printing, disclosing, restricting access, or otherwise tampering with files and/or data to which you have not been given authorization to access. Electronic patient records may be accessed only if there is a direct patient care or approved research relationship with patient consent.
- sending or arranging to receive email in a manner that violates hospital policies or legislation, e.g. Harassment, Ontario Human Rights Code.
- accessing pornographic Internet sites
- usage that is disruptive to the operations of the hospital, such as:
    - chain letters
    - sending to all e-mail users for communicating information other than of a corporate nature and important to the broad audience
    - playing games (except for training purposes)
- theft of, or any other criminal activity related to equipment, and/or software, and/or data use of personal software on the hospital's hardware
- use of hospital computer resources to run or support a private business

2. System User's Confidentiality Obligations

You will be assigned a unique identifier and a confidential password to access the appropriate systems for which you have approval. It is your responsibility to maintain the confidentiality of that password. The hospital systems maintain an internal record of all transactions carried out by you through the use of your password. This internal record of your activity may be audited as part of the hospital's security management practices. You are responsible and accountable for all transactions associated with your password.

If, at any time, you suspect that the confidentiality of your password has been compromised, you should immediately change your password and inform your direct supervisor as well as Information Services.

Any patient-related information accessed through the hospital systems is strictly confidential and should be used only in the performance of necessary duties and in accordance with hospital policy. Individuals accessing electronic patient records for research purposes must document the reason for access in the comments section of the electronic patient record.

I have read, understand, and agree to abide by the responsibilities outlined in this document:

Applicant's Full Name (please print) _____Signature _____

Position/Job Title: _____ Date (dd/mm/yy)_____

Hospital: _____ Dept/Program/Location:_____ Phone#/Ext _____