# CSS HINP Statement of Practices

## HINP Statement of Practices

The Personal Health Information Protection Act (PHIPA), describes a Health Information Network Provider (HINP) as someone that provides services to two or more Health Information Custodians where the services are provided primarily to enable the Custodians to use electronic means to disclose Personal Health Information (PHI) to one another. HINPs are required to comply with requirements under Ontario Regulation 329/04, including making available information about its services and information practices.

CSS has created the MendMD system to benefit physicians and other providers of care all across Ontario. This provides the organizations with the ability to access their patients' PHI at the point of care. As a result, CSS is classified as a HINP in the context of hosting this system and administering access to it. As part of CSS's obligations under the Regulations, this page represents our statement of information practices in relation to these offerings:

## CSS HINP Statement

CSS is a HINP under the regulation, in relation to its hosting, development and administration of the MendMD system.

MendMD expands the patient record across system boundaries enabling a more seamless flow of information between the hospital and their departments, ensuring continuity of care between hospitals and caregivers through a fully-integrated patient record. The web-based platform brings the patient's medical information into one unified health record, giving clinicians the fulsome picture of a patient's health and medical history anywhere at any time.

## Organizational Safeguards

As HINP, CSS employs a combination of technical, physical and administrative safeguards to help protect the security, confidentiality and integrity of systems and the information on them:

- A documented Disaster Recovery/Business Continuity Plan;
- Anti-virus solutions;
- Regular audits, Privacy Impact Assessments (PIA) and Threat Risk Assessments (TRA);
- Automated systems logging and monitoring of patient information;

- The use of complex passwords are enforced on all systems;
- Regular backup of data and a robust off-site storage system;
- Data Sharing Agreements with all participants;
- Employees receive regular education and training on privacy, confidentiality and security;
- Firewall systems guard our network perimeter;
- Formal agreements in place with maintenance and service providers;
- Network traffic is monitored continually, helping identify threats;
- Policies, procedures and standards govern related operations;
- Servers are housed in a secure space, with redundant and backup power supplies;
- Servers are patched on an ongoing basis; and
- Third parties and their authorized staff are subject to control processes such as data sharing agreements, privacy agreements and contracts.

## Policies, Practices and Standards

In general, with regards to the system it maintains as HINP, other than as may be permitted or required by law, CSS does not:

- Use any personal health information to which it has access in the course of providing the services for the health information custodian except as necessary in the course of providing the services;
- Disclose any personal health information to which it has access in the course of providing the services for the health information custodian; or
- Permit its employees or any person acting on its behalf to be able to have access to the information unless the employee or person acting on its behalf agrees to comply with the restrictions that apply.

## Accountability to Partner Organizations

As HINP, CSS is accountable to its partner organization and takes the following steps:

- Notifies participating health information custodians (HICs) of any privacy breaches detected;
- Provides each participating HIC with a copy of the HINP statement of information and, where requested, a copy of the partner agreement including its statement of network services;
- Completes a Privacy Impact Assessment (PIA) and, where requested, provide a copy;

- Makes this statement available to the public on our website;
- Maintains appropriate logging and monitoring of PHI that will be made available to participating HICs on request;
- Performs regular privacy and security assessments of the operation of in-scope systems and provides summary copies of the results of those assessments to participating HICS; and
- Binds third parties providing services to these programs to these requirements.

For more information about CSS's privacy and security practices, please contact Victoria Tolls by calling 613-767-8864 or by sending an email to privacy@clinicalsupportsystems.com.