Mississauga Halton **LHIN** | **RLISS** de Mississauga Halton

GOVERNANCE GUIDELINE

FOR

COMMUNITY HEALTH SERVICE PROVIDERS

December 2015

Ontario
Local Health Integration Network
Réseau local d'intégration des services de santé

Table of Contents

Preamble

This checklist is to be used by the Board and Management of Not-For-Profit Community and Mental Health and Addiction Health Service Providers to demonstrate to the Mississauga Halton LHIN proper oversight and management of their enterprise, ensuring they are exercising their fiduciary duties. It is a tool for the Board and Senior Management to conduct a self-assessment of governance and business practices in order to identify gaps and/or opportunities for improvement. It also may be used to track action items coming out of the analysis. Governance best practices are continually evolving and this checklist represents current practices.

The term "Executive Director" (ED) used in the document signifies the Agency's most senior manager reporting directly to the Board. However the title of that staff member may vary from Agency to Agency, e.g., CEO.

#	BASIC STANDARD	COMPLY NOW? (Y/N)	IDENTIFY ACTION ITEM(S)	LEAD	DUE DATE
1.0	**Governance** *				
1.1	**General** The organization complies with the approved, signed Board By-Laws including how directors are recruited; its obligation to the LHIN (M-SAA), nominated, elected; how the appointment/election of officers occurs; officers' roles, frequency and process for advertising annual meetings; and approved Board Committees.				
1.2	The Board is responsible for: • Setting the strategic directions of the organization • Monitoring organizational performance under M-SAA and other obligations • Ensuring fiscal viability and sustainability • Monitoring the CEO/ ED's performance and conducting a formal CEO/ED performance review. Accordingly the organization's performance management program and measurement system must connect the strategic plan to the annual operating plan. Metrics must be developed and implemented so the Board can routinely monitor how effectively the organization is performing in all areas, e.g. services to clients, financial performance, ED performance, and other areas. The Board has a system in place to ensure that they are meeting all of their responsibilities and that all aspects of the organization are monitored within a twelve month time frame.				

#	BASIC STANDARD	COMPLY NOW? (Y/N)	IDENTIFY ACTION ITEM(S)	LEAD	DUE DATE
1.3	The Board requires the Executive Director to provide a formal ED Compliance Declaration (see attached LHIN Board version as an example) at each Board Meeting stating that the organization is compliant with approved policies, relevant legislation and regulations, directives from the funders and that all statutory deductions have been remitted on time.				
1.4	The Board approves the annual capital and operating budget for the organization.				
1.5	**External Audit** The Board approves the audited financial statements for the organization.				
1.6	Ensure the external auditors have an opportunity to meet without management with the Board/Board Committee overseeing the annual financial audit.				
1.7	Where the auditors have issued a Management Letter, the Board must be able to get it directly and ensures that the Executive Director adequately follows up on all items.				
1.8	**ED/CEO Role & Performance** The ED job description is current, reflects the Board's expectations and the responsibility and authority delegated to the ED.				
1.9	The Board Chair /Executive Committee approves the ED's attendance at professional development/conferences prior to costs being incurred.				
1.10	Performance evaluation criteria for the ED has been developed, documented and shared with the ED and approved by the Board.				
1.11	Increases in the ED's salary or benefits are only processed on receipt of written documentation from the Chair of the Board directly to the H.R. Department and copied to the ED.				
1.12	The Board reviews and approves all staff salary and bonuses in accordance with the most current public sector wage restraints, the capacity of the agency to fund any increase recommended by the ED, prior to payment being issued to employees as to its reasonableness and compliance with government policies.				
1.13	**Client Complaints** The Board approves the organization's Client Complaints Policy and Procedures.				
1.14	Client complaints are monitored and reported to the Board/Board Committee as per the Policy.				

#	BASIC STANDARD	COMPLY NOW? (Y/N)	IDENTIFY ACTION ITEM(S)	LEAD	DUE DATE
1.15	The organization is in compliance with Public Sector Compensation Restraint requirements.				
1.16	**Risk Management** An enterprise risk assessment (ERA) has been completed within the last two years and the results and action plan have been presented to the Board.				
1.17	Risks identified as a result of the ERA have been mitigated and the relevant Board/Board Committee has been updated.				
1.18	Does your organization carry Directors and Officers (D&O) Insurance? Does it cover Directors from day 1? Does it cover prior Directors? How often do you review its coverage?				
2.0	**Human Resource Management** *				
2.1	Human Resources Policies and Procedures have been developed for all non-unionized staff and have been reviewed and updated within the last eighteen months. A hard copy of the signed, dated H.R. P & Ps is available in Human Resources.				
2.2	There is an anonymous submission process to receive and evaluate employee concerns regarding questionable practices in the agency.				
2.3	A staff opinion survey has been conducted within the last two years.				
2.4	The major issues identified through the staff opinion survey have been reviewed with the Board and an action plan put in place.				
3.0	**Procurement/Contract Management** *				
3.1	There is a Board approved policy related to the procurement of goods and services. Where Agencies achieve the required threshold (public funding of $10M or more), they comply with the Broader Public Sector (BPS) Directive on Procurement.				
4.0	**Financial Management/Financial Reporting** * In some instances the Agency may not be able to meet specific internal controls listed, but is expected to have compensating controls in place to ensure the validity, completeness and accuracy of its financial statements and the continued financial viability of the organization.				
	There are Board approved policies, that as a minimum, relate to banking, financial investments, fundraising, sponsorships, donations, financial reporting, assets including capitalization thresholds and amortization rates, procurement, compliance with GAAP, etc.				

#	BASIC STANDARD	COMPLY NOW? (Y/N)	IDENTIFY ACTION ITEM(S)	LEAD	DUE DATE
	There is Board policy specifying signing officers and limitations, e.g., the Board may determine that all cheques/payments in excess of a defined amount must first be signed by an officer of the Board.				
	The Board approves the Annual Capital and Operating Budget				
	Where cheques are issued, the entire accounts payable voucher must be presented to both signing officers, i.e., no signing officer shall sign a cheque without first reviewing and initializing the supporting documentation. Where payment is by EFT signing officers must still review and initial the supporting documentation prior to funds being transferred				
	An accounts payable list showing vendor, cheque/EFT#, amount and account charged is produced from the accounts payable system each month and signed off by the ED and is available to the Finance Committee for review as needed.				
	The ED's expenses and credit card purchases must be approved by the Board Chair or Treasurer prior to payment being processed.				
5.0	**Data Security** **				
5.1	Policies and Procedures for the administration of security are documented, approved and communicated.				
5.2	Security policies are acknowledged and documented by new employees upon hire.				
5.3	Duties of security personnel do not include programming or IT management.				
5.4	User profiles and menus on the system are restricted to IT security personnel.				
5.5	There are access controls in place that require unique user IDs and minimum lengths for passwords. The system locks out the user after a reasonable number of unauthorized entry attempts.				
5.6	All information shall be protected by physical security features				
5.7	Programming changes are restricted to IT personnel and administrator rights are limited appropriately.				
5.8	Access for terminated employees is disabled on a timely basis. The Organization has documented procedures for disposal or transfer of media and hardware, which ensure the protection of sensitive data.				
5.9	Remote users are identified and authenticated before access is granted and information is transmitted.				

#	BASIC STANDARD	COMPLY NOW? (Y/N)	IDENTIFY ACTION ITEM(S)	LEAD	DUE DATE
5.10	Management ensures that all laptops and desk tops are backed up to the organization's server, daily. Any data that is stored on a portable media should be encrypted.				
5.11	Management ensures that electronic records are backed up on a daily basis and that the weekly back-up copy is stored off site with a reputable company. In the event of a server problem, this minimizes data loss to the current week's updates.				
5.12	The organization's electronic systems are protected by a firewall.				
5.13	The organization has a document management system in place to file and retrieve critical documents. The Organization maintains an inventory of all media containing unencrypted information, including location and status.				
6.0	**Privacy** ***				
6.1	The Organization should designate a senior member of the team to be accountable for ensuring ongoing compliance with legislated privacy requirements (e.g. Chief Privacy Officer).				
6.2	The Organization should have a documented Privacy Policy that is easily accessible by the Public. The Privacy Policy should include: • a general description of the administrative, technical and physical safeguards and practices that the organization employs with respect to safeguard privacy • a description of processes for handling a suspected breach of privacy and provisions for notifying the individual(s) concerned. • a description of data retention limits and rules • documented procedures for data disposal according to retention schedules defined in the Privacy Policy. • documented procedures for handling complaints and inquiries, including users' requests for changes to their data.				

#	BASIC STANDARD	COMPLY NOW? (Y/N)	IDENTIFY ACTION ITEM(S)	LEAD	DUE DATE
6.3	Public Communication of Privacy Policy should include, but not be limited to, a description of the information held by the Organization, including: • a general account of the process by which the organization confirms the authority or consent of the data custodian to collect the information • the purposes and limitations for collecting, using, retaining and disclosing information; and • information about how the Organization maintains the accuracy of this information.				
6.4	The Organization's training and orientation program includes content relating to the Privacy Policy and its implementation in operational processes.				
6.5	The Organization has performed a Privacy Impact Assessment (PIA) for appropriate solutions. The PIA identifies the risks to the privacy of individuals arising from *normal operations* of the system or service, specifies controls designed to mitigate identified risks to personal privacy and is available to members of the public, on request.				

* From MH LHIN Audit and Finance Committee
**The International Organization for Standardization's Code of Practice for Information Security Management – ISO 17799:2005
*** Government of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA); and
The Canadian Standards Association's Model Code for the Protection of Personal Information – CAN-CSA-Q830-03