January 2013

# EMR Program – Privacy and Security Policy and Procedure Requirements

**Clinic Name: _____ Date: _____**

Physicians in private practice in Saskatchewan are responsible for meeting the requirements of *The Health Information Protection Act* (HIPA). The EMR Program requires and the College of Physicians and Surgeons of Saskatchewan (CPSS) expects participating physicians to have written policies and procedures that show their adherence to HIPA. This list of requirements is the minimum set of policies and procedures a physician in the EMR Program should adopt.

| Policy & Procedure Requirement: Accountability | Guideline in Privacy & Security Reference Manual | |
|---|---|---|
| 1. Designate in writing a Privacy Officer in the practice location and describe the position's responsibilities.<br>*CPSS and EMR Program* | • Responsibilities of Privacy Office and Medical Office Administrator | ☐ |
| 2. A written privacy and security statement<br>*EMR Program* | • Privacy and Security Statement in sample policy manual | ☐ |
| 3. A policy and procedures on the obligations of physicians and staff to protect the confidentiality and security of personal health information.<br>*CPSS* | • Obligations of Employees, Health Professionals and Third Parties | ☐ |
| 4. A policy and procedures to obtain signed confidentiality agreements from staff, health professionals, third parties and other individuals who have access to personal health information, including the frequency of renewing the confidentiality agreement.<br>*CPSS and EMR Program* | • Obligations of Employees, Health Professionals, and Third Parties | ☐ |
| 5. A procedure is established to ensure all employees, health professionals and third parties who have access to personal health information for which the physician is accountable receive a copy of the privacy and security policies.<br>*CPSS* | • Responsibilities of Privacy Office and Medical Office Administrator<br>• Obligations of Employees, Health Professionals and Third Parties | ☐ |
| 6. A procedure that ensures the privacy and security policies are reviewed on a regular basis and are amended if required. *CPSS* | • Responsibilities of Privacy Office and Medical Office Administrator | ☐ |

| | | |
|---|---|---|
| 7. A policy and procedures on how staff, health professionals and third parties are educated on *The Health Information Protection Act* and the policies and procedures, and how a culture of privacy and confidentiality is maintained.<br>*EMR Program* | • Awareness, Education, and Training | ☐ |
| 8. A policy and procedures that addresses the steps to be taken when the physician ceases to practices or leaves a medical practice.<br>*EMR Program* | • Ceasing to Practice or Leaving a Medical Practice | ☐ |
| 9. A policy and procedure on how patients are notified of the information handling practices of the physician.<br>*EMR Program* | • Identifying Purpose and Openness | ☐ |
| 10. A policy and procedures on how patients may make a complaint regarding the adherence to the practice's privacy policies and procedures, or to notify the clinic of a breach.<br>*EMR Program* | • Challenging Compliance | ☐ |
| 11. Policies and procedures to protect the integrity, accuracy and confidentiality of patient health information<br>*CPSS* | • Accuracy and Integrity<br>• Safeguards<br>• Right to Request Amendment<br>• Collection of Personal Health Information<br>• Scanning and Destruction | ☐ |
| **Policy & Procedure Requirement: Patient Rights** | **Guideline in Privacy & Security Reference Manual** | |
| 12. A policy and procedures for patients to access and obtain copies of their records.<br>*CPSS and EMR Program* | • Patient Access to Their Own Information | ☐ |
| 13. A policy and procedures for patients to request amendment to their personal health information if it is incorrect or missing.<br>*CPSS and EMR Program* | • Patient Requests for Amendment of Their Record | ☐ |
| 14. Policies and procedures for third parties to access and obtain copies of patient records to which they have access pursuant to ***The Health Information Protection Act.***<br>*CPSS* | • Patient Designates and the Exercise of Rights by Others<br>• Disclosure of Personal Health Information | ☐ |

| Policy & Procedure Requirement: Collection, Use and Disclosure | Guideline in Privacy & Security Reference Manual | |
|---|---|---|
| 15. Policies and procedures to restrict access to personal health information unless access is required for a purpose authorized by *The Health Information Protection Act*.<br>*CPSS* | • Awareness, Education, and Training<br>• Acceptable Use of Technology<br>• User Account Management<br>• Auditing | ☐ |
| 16. A policy and procedures for the collection of personal health information.<br>*CPSS* | • Collection of Personal Health Information | ☐ |
| 17. Policies and procedures respecting the use of personal health information.<br>*CPSS* | • Use of Personal Health Information | ☐ |
| 18. Policies and procedures respecting the disclosure of personal health information.<br>*CPSS* | • Disclosure of Personal Health Information | ☐ |
| 19. A policy and procedures for responding to consent directives from patients, including masking.<br>*EMR Program* | • Managing Patient Consent and Masking | ☐ |
| **Policy & Procedure Requirement: Safeguards** | **Guideline in Privacy & Security Reference Manual** | |
| 20. A policy and procedures related to signed agreements:<br>- Information sharing agreement,<br>- Clinic Exit Agreement or similar expectations in a legal agreement related to the group practice,<br>- IMSP and other third parties.<br>*EMR Program* | • Sample Agreements | ☐ |
| 21. Policies and procedures to protect against reasonably anticipated threats to the security, integrity or loss of personal health information.<br>*CPSS* | • Safeguards | ☐ |
| 22. Policies and procedures to protect against unauthorized access to, use, disclosure or modification of personal health information.<br>*CPSS and EMR Program* | • Auditing<br>• User Account Management<br>• Awareness, Education, and Training | ☐ |
| 23. A policy and procedures regarding the response to a | • Management of Breaches | ☐ |

| | | |
|---|---|---|
| suspected or actual breach of privacy.<br>*EMR Program* | | |
| 24. Documented procedures for managing patients when the EMR is not functioning, as part of a Business Continuity/Disaster Recovery Plan.<br>*EMR Program* | • Developing a Business Continuity and Disaster Recovery Plan | ☐ |
| 25. A policy and procedures on the retention, storage and destruction of paper and electronic records.<br>*EMR Program* | • Retention of Personal Health Information<br>• Storage of Personal Health Information<br>• Destruction of Paper Records | ☐ |
| 26. A policy and procedures regarding the backing-up of EMR data.<br>*EMR Program* | • Backups including Storage of Backup Tapes | ☐ |
| 27. A policy and procedures for the management of user accounts, including the requirement that each user have his or her own account.<br>*EMR Program* | • User Account Management | ☐ |
| 28. A policy and procedures to establish and maintain an auditing program of all activity associated with the EMR.<br>*EMR Program* | • Auditing | ☐ |
| 29. A policy and procedure regarding how to securely dispose of devices that may contain personal health information..<br>*EMR Program* | • Destruction of Devices | ☐ |
| 30. A policy and procedures to protect personal health information, including encryption, anti-virus software, firewalls, and Virtual Private Networks..<br>*EMR Program* | • General Security Software | ☐ |
| 31. A policy and procedure for the secure location of office equipment, such as fax machines and monitors, so that personal health information is not visible or accessible to those not authorized to see it.<br>*EMR Program* | • General Office Security | ☐ |