EMR/Cyber Privacy & Security Agreement

WEST CHAMPLAIN
FAMILY HEALTH TEAM

General

- All employees who use WCFHT office computers and EMR must read, understand and sign this Policy.
- As an employee, your computer system and EMR use may be monitored at any time.
- Any intrusion or suspected breach of security should be privately and immediately reported to the Administrator.

Authorization

- No employee, vendor, or IT personnel may install software or download "inappropriate files" on a computer or local network device in this office without prior, written permission from the network Administrator.
- Knowledgeable consent, whether implied or express (oral or written), must be acquired before patient information is shared through EMR.

Communication

- All emails from patients will be copied in the chart. Employees are not permitted to email patients in response. Instead, employees should promptly contact the patient by telephone.

Authentication

- All desktop computers in this office will run the most recent version of Windows, according to the Administrator.
- Each machine will have an "Administrator" account that is set up and accessed only by the Administrator. For security reasons, employees may not use the Administrator account.
- Each EMR account must be set to auto-logoff after 5 minutes. Computers in patient rooms must be logged off immediately after use.
- Patient information and records will be maintained as accurate, complete, and up-to-date in a timely manner.

System Integrity

- Employees may be responsible for updating service packs, antivirus updates, firewall updates, and vendor patches whenever they are reminded. Reminders typically come via pop-up message on the screen, by verbal reminder, or by an email memo.
- Web browsing is not permitted unless required for patient care or otherwise approved by management.
- Each machine will have auto-updating enabled for Windows patches.

Confidentiality

- Patient data may not be stored, removed or transmitted from the office by any media, without prior written permission from the Administrator.
- Employees must leave the built-in hard drives of scanners, copiers, fax machines disabled.
- Patient data may not remain in computer recycle bin. Employees will delete all reports from this file daily.

Mobile Security

- External drives (USB, SD cards, etc) of any kind or size are forbidden, unless approved in advance by the Administrator.
- All wireless and/or mobile devices may not be synced to office computer systems.

Disaster Recovery

- Employees who are responsible for the patient database must be back up the database once each work day.

_____	_____	_____/_____/_____
EMPLOYEE NAME	EMPLOYEE SIGNATURE	DATE