

EMR Privacy and Security

Business View

September 30, 2021

Document Version & Status: 1.0 – Final



Table of Contents

1. INTRODUCTION	3
1.1 PURPOSE	3
1.2 OVERVIEW	3
1.2.1 <i>How to Read this Specification</i>	3
APPENDIX A: GLOSSARY OF KEY TERMS AND DEFINITIONS	4
1.3 ACRONYMS AND ABBREVIATIONS	4

1. INTRODUCTION

1.1 Purpose

This specification describes a common set of functional and non-functional requirements that are fundamental to maintain the privacy and security of patient data used and stored in local and hosted EMR Offerings.

1.2 Overview

As points of services such as EMRs continue to connect with different systems including provincial EHR products and services, it is essential to ensure that the privacy and security expectations of maintaining health data. Personal health information (PHI) needs to be treated as confidential and be protected from unauthorized access whether the EMR resides and is used at a clinic practice, or if it is a service hosted by a vendor in a data centre. This specification defines a minimal set of requirements to meet the privacy and security expectations for both local and hosted EMRs in the healthcare industry in general where patient data is managed, such as primary care, secondary care or ambulatory care.

1.2.1 How to Read this Specification

The requirements in this specification cover:

- EMR Baseline – Encompass privacy and security of the EMR application and functionality. This set of requirements apply to both Local and Hosted EMR models.
- EMR Hosting – Encompass privacy and security of the managed services offered by a Hosted EMR. This set of requirements additionally apply to Hosted EMRs and do not apply to Local EMRs.

APPENDIX A: GLOSSARY OF KEY TERMS AND DEFINITIONS

1.3 Acronyms and Abbreviations

The following table lists abbreviations and acronyms used in this specification.

ACRONYM	DEFINITION
CIO	Chief Information Officer
CISSP	Certified Information Systems Security Professional
CNO	College of Nurses of Ontario
COTS	Commercial off-the-shelf
CPSO	College of Physicians and Surgeons of Ontario
CSEC	Communications Security Establishment Canada
FTP	File transfer protocol
HTRA	Harmonized TRA
NTP	Network time protocol
ODBC	Open Database Connectivity
PHI	Personal health information
PHIPA	Personal Health Information Protection Act
PIA	Privacy Impact Assessment
TRA	Threat Risk Assessment
VPN	Virtual private network
WAN	Wide area network