Privacy and Security

Business View

November 3, 2023

Document Version and Status: 2.1 – Final

Table of Contents

1. INTRODUCTION 3

1.1 PURPOSE 3

1.2 OVERVIEW 3

1.2.1 Privacy 3

1.2.2 Security 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 align with provincial expectations for the privacy and security of patient data used and stored in EMR Offerings.

1.2 Overview

As EMRs continue to connect with different systems including provincial EHR products and services, it is essential to ensure the privacy and security expectations of maintaining personal health data (PHI). PHI needs to be treated as confidential and secured from unauthorized access whether the EMR resides at a clinical practice or is a service hosted 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 Privacy

Privacy of PHI ensures that controls are in place, including processes and technologies, to allow authorized individuals to appropriate and timely access the data. In other words, privacy is about providing the right access to the right people at the right time for the right purpose.

1.2.2 Security

Security ensures that the information is safeguarded from unauthorized access typically from cybersecurity attacks from threats and vulnerabilities. Access can relate to viewing, modifying, or deleting data, or denying authorized and appropriate access to the data. Protections may leverage processes, technologies, tools or knowledge. Both privacy and security measures often overlap each other and are needed to work together to protect patient data.

APPENDIX A: GLOSSARY OF KEY TERMS AND DEFINITIONS

Terms identified in this section relate to concepts within this Specification. Terms that apply generally across OMD specifications are defined in the glossary available here: https://www.ontariomd.ca/emr-certification/library/guides-and-references.

1.3 Acronyms and Abbreviations

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

ACRONYM	DEFINITION
CIO	Chief Information Officer
CNO	College of Nurses of Ontario
COTS	Commercial off-the-shelf
CPSO	College of Physicians and Surgeons of Ontario
DFC	Draft for comment
DFU	Draft for use
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 and Risk Assessment
VPN	Virtual private network
WAN	Wide area network