MHI Internship Report:

Certification and Requirements Writing

at

Allscripts Canada

By:
Nischal Paudel

Performed at:
Allscripts Canada
13888 Wireless Way Suite 110
Richmond, BC V6V 0A3

In Partial Fulfillment of the Requirements for the Master of Health Informatics Program,

Dalhousie University, Halifax, NS

Report of Internship for the Period May 15 – August 11, 2017

Date Submitted: August 11, 2017

Acknowledgment and Endorsement

This report has been written by me and has not received any previous academic credit at this or any other institution.

First of all, I would like to thank Allscripts Healthcare Inc. for offering this valuable exposure and learning opportunity to Master of Health Informatics Students at Dalhousie University.

I am really fortunate to be supervised by Mr. Jaimes Blunt, Sr. Solution Manager, his exemplary guidance, knowledge, effort and careful monitoring throughout the internship have enhanced my informatics abilities. A deep sense of gratitute and appreciation to Jennifer MacGregor, Managing Director of Allscripts Canada; John Lee Barret, Senior Executive at Allscripts Canada, and the Allscripts sales team members as well as technical and administrative team members working at Richmond office.

I would also like to thank Julie Strachota for her guidance and support through the hiring, onboarding and internship period.

Also, I would like to thank Mara Maljanovic, MHI intern, for being a great team member.

Finally, I would like to thank Dr. Raza Abidi, Dr. Samina Abidi, Dr. Samual Stewart, Dr. Persuad and Dr. Ashraf Abushekhar for providing health informatics wisdom without which this internship would not be possible.

(signature)

Nischal Paudel

Executive Summary

This document is a reflection of MHI internship performed at Allscripts Healthcare Inc., Canada, from May 15 – August 11, 2017. Allscripts Healthcare Inc. is an innovative company that provides healthcare solutions and services to help organizations achieve better clinical, administrative, financial and operational results. The author was supervised by Mr. Jaimes Blunt, a very knowledgeable and experienced Senior Solution Manager at Allscripts Healthcare Inc.

The report consists of background information on two key topics used in the report, introduction on Allscripts business, goals and achievements, learning opportunity and exposure during the internship, objectives and deliverables of the projects assigned, analysis of a problem that can be solved using informatics science and a conclusion and recommendation drawn at the end of internship.

Within this internship period, the author contributed to two major projects and a couple of minor projects supervised by Mr. James Blunt. At the end of the internship, he successfully met the objectives and deliverables of the two assigned projects, which are: Privacy and Security Requirements Gathering for FollowMyHealth (Infoways Certification Services) and Requirements for CIHI's RAI-MDS 2.0 Canadian Version. The end deliverables of both projects are business and system requirements documents (word, excel and Visio files) submitted to the supervisor in a timely manner throughout the internship.

The internship was highly valuable to understand and use the knowledge and skills gained in MHI courses. It is a great exposure to the field of Health Informatics and is highly recommended to students on MHI internship track at Dalhousie University.

Table of Contents

1. Introduction

1.1 FollowMyHealth

FollowMyHealth® (FMH), an online application developed by Allscripts, is a patient engagement platform build to connect patients with their care provider, to give immediate access to their personal health information and engage them in their well-being. Using FMH, users can review their medical records, communicate privately with their physicians, update health information, view test and lab results, read care provider notes, request Rx refills, schedule or change appointments, view and pay bills etc.

FollowMyHealth is a candidate for Consumer Health Application Certification with Canada Health Infoway. When FMH is Infoway certified, it becomes a pan-Canadian standard compliant solution. This is very useful for care providers and patients who want to use the solution but are unsure of the local, national and international standards and the changing health IT market and business needs.

FMH has a cloud based architecture, runs on Microsoft Azure - Software as a Service (SaaS), making it scalable and secure and can be rapidly deployed and configured as per population needs. Due to its open architectural concept, it can integrate with Allscripts as well as third-party EHRs to collect and harmonize care plans and patient data. Further, it comes with advanced functionality such as remote monitoring, telehealth, and engagement and optimization.

One of the projects presented below is Canada Health Infoway's self-assessment requirements writing to certify FMH as a bi-directional Consumer Health Application.

1.2 RAI-MDS 2.0 Canadian Version

Resident Assessment Instrument Minimal Data Set 2.0 (RAI-MDS 2.0) is a standardized set of clinical and administrative data elements that helps care providers to gather definitive

information on a resident's strength and needs within a continuing care facility (i.e. hospital based extended care, nursing home, long-term care, personal home care etc.) (CIHI, 2012). RAI-MDS 2.0 was developed and is maintained by an international collaborative of researchers working in more than 30 countries (CIHI, 2012). The Canadian version of RAI-MDS is revised, maintained and distributed by Canadian Institute for Health Information (CIHI).

MDS assessment form is initiated when a resident is admitted to a continuing care facility (CIHI, 2012). Care providers fill in an admission/re-entry form when a resident is admitted to the facility, a full assessment form within 14 days of entry into the facility, a quarterly assessment every 92 days, an annual assessment every 365 days and a discharge record when the resident leaves the facility. The clinical and administrative data collected is then compiled into submission files using data submission specification and submitted to CIHI through CIHI's electronic Data Submission Services(eDSS) application. The information is then stored within Continuing Care Reporting Services (CCRS) database and CCRS reports are produced which is used by the facility to support their clinical, management and funding decision. The RAI-MDS 2.0 also consists of Decision Support Algorithms to calculate Quality Indicators (QI), Resource Utilization Groups(RUGs), Resident Assessment Protocols (RAPs), Outcomes Scales and to create care plans for the resident (CIHI, 2012).

The second project presented below is high-level requirements writing to build the assessment form for use in one of Allscripts' renowned clinical solution (Sunrise Clinical).

2. Allscripts Healthcare Inc.

Founded in 1986 as a medication management company, Allscripts is a publicly traded international company that delivers innovative solutions and services for hospitals and health systems, physician and community practice, life science and health plans, and ePrescibing. Their vision is to build a connected and coordinated community of healthcare (Allscripts, 2017). Their

mission is to provide solutions that enable smarter care, delivered with greater precision, for healthier patients, populations and communities (Allscripts, 2017).

Their solutions are used in United States, Canada, United Kingdom, Australia, Singapore etc. Some hospitals using their solutions in Canada includes St. Joseph's Health Centre, Toronto; Fraser Health Authority, B.C.; Hospital for Sick Children, Toronto; provinces of Manitoba, Saskatchewan; Horizon Health, New Brunswick etc. (Allscripts, 2017).

Allscripts offers comprehensive suite of Electronic Health Record (EHR) solutions for clinical, administrative and operational, and financial management. Their EHR solutions (Sunrise Clinical, TouchWorks EHR, Professional EHR) are built on an open platform with clinical decision support system capable of providing immediate analysis and insights. One of their renowned EHRs, Sunrise EHR Platform, is available for acute care, mobile care, ambulatory care, surgical care, anesthesia, emergency care, pharmacy, oncology, laboratory, radiology, rehabilitation, wound care etc. Further, they have separate EHR suites for large and multi specialty physician practices (TouchWorks EHR Platform) as well for large to small family practices and specialty groups (Professional EHR Platform).

Allscripts CareInMotion is a solution for population health management. These solutions are built for care coordination, patient engagement, connectivity, data aggregation, and analytics. Their care coordination solutions (Allscripts Care Manager, par8o, etc.) enable providers to manage patient care as they move from one stage to the next stage of care. Patient engagement solution (Allscripts FollowMyHealth) provides a single point of access to patient's health record while engaging them with their care providers and care plans. Connectivity, data aggregation and analytics solutions (Allscripts dBMotion, Allscripts Fusion) helps collect data from disparate source systems, harmonizes those data and delivers in a useable and actionable form at the point of care. Further, they also have a solution (2bprecise) that brings the intelligence and insights of precision medicine into the workflow of physician and enhances health and genomic research.

Their financial management solutions (Allscripts EPSi, Allscripts RCMS) are designed to change clinical processes to improve patient flow and outcomes, increase quality, and reduce costs with budgeting, strategic planning, capital management, accounting, labor productivity and decision support modules. These solutions also have revenue cycle management that can be used to improve efficiencies and to ensure users get most out of their business and information technology investments.

Allscripts is recognized for excellence in health IT innovation, some of their achievements are (Allscripts, 2017):

- 2017 #1 Top Core EHR with a Population Health Management Solution from Black Book Rankings.
- 2016 #1 Top Ambulatory EHR Vendor in user satisfaction poll from Black Book Rankings
- 2015 #1 Top Ambulatory EHR Vendor in multiple categories from Black Book Rankings
- 2014 #1 Best Global Acute EMR and KLAS Category Leader
- 2014 #1 Top Ambulatory EHR Vendor – Rheumatology Black Book Rankings
- 2013 KLAS Category Leader etc.

3. Work at Allscripts

3.1 Internship description

In 2015, Allscripts partnered with Dalhousie to provide paid internship opportunity to two health informatics students. The internship is 13 weeks long, project based, during the summer term, located at their Richmond office, British Columbia. The intern must be a current student at Dalhousie University in MHI Program on an internship track. The author is honored to be part of this great learning experience at Allscripts Canada.

Allscripts' Canadian team is led by the managing director and consists of senior executives, solution managers, product managers, service managers, sales team members, developers, etc. They provide their solutions as well as expertise on hosting, consulting, optimization and management of revenue cycle services to their Canadian and International customers. The author along with another MHI intern worked on various projects under direct supervision from Senior Solution Manager during this internship period.

3.2 Project description

Reporting directly to the Senior Solution Manager, the author was assigned to two major projects:

- May 15 – June 23: Responsible for gathering, analyzing and writing FollowMyHealth Privacy and Security requirements for submission to Canada Health Infoway Certification Services.
- June 26 – August 11: Use informatics science to model time-sequence and behavior of RAI-MDS 2.0 Assessment form in a structured and clear way for solution development.

3.3 Infoway Certification Services

Canada Health Infoway (Infoway) is a federally funded organization tasked to increase the use of digital health solutions in Canada. Infoway Certification Services provides certification for health information solutions per technology classes in Canada as (Infoway, 2017): Ambulatory Electronic Medical Records (aEMR), Electronic Medical Records (EMR), Drug Information System (DIS), Client Registry, Immunization Registry, Provider Registry, Consumer Health Application, Consumer Health Platform.

The goal of the first project was to gather, analyze and map requirements, also known as self-assessment, for submission to Infoway's Certification services. Under guidance from Mr. Jaimes and FMH team, the author along with an intern completed the self-assessment process explaining and highlighting how privacy, security, management and interoperable requirements

are met. The requirements document is derived from top-quality standards like ISO Privacy and Security standards, PIPEDIA, EHRi, COBIT, ITIL, HL7 v2/v3 CDA and so on. Since FMH runs as a SaaS on Microsoft Azure, both FMH and Microsoft Azure compliance documents had to be gathered, read and assessed since they both share Privacy and Security responsibilities for Personal Health Information.

Table 1 and Table 2 below are highlights of privacy and security requirements that FollowMyHealth (FMH) meets to protect the privacy of patients and maintain integrity confidentiality and availability of data as required by the Canada Health Infoway's Self-Assessment document (Infoway, 2017). The final business document is an excel spreadsheet submitted to the supervisor for review and submission to Canada Health Infoway Certification Services.

3.4 RAI-MDS and Health Informatics Solution

3.4.1 Problem

MDS 2.0 Canadian Version is filled out when a resident is admitted to a continuing care facility. Care providers fill in an admission/re-entry form when a resident is admitted to the facility, a full assessment form within 14 days of entry into the facility, a quarterly assessment every 92 days, an annual assessment every 365 days and a discharge record when the resident leaves the facility. In the current process, the nurse fills out a paper version of MDS 2.0 Assessment Form which consists of 23 different sections and around 500 clinical and administrative data elements. The elements are then coded using CIHI specification into a clinical application and submitted. This takes away valuable time and resources within a care facility having to fill in a paper form first and then their EMR and use XML/ASCII coding specifications to submit and resubmit to CIHI's.

3.4.2 Health Informatics Solution

A solution to this problem is integrating the assessment record within the care facilities EMR such that data elements can be collected from diverse sources, harmonized and delivered in a useable and actionable form saving both time and resources within the care facility. With the help of CIHI's data submission specification, it can then be submitted with appropriate XML/ASCII coding specification.

Using health informatics knowledge and skills, the author gathered high-level requirements necessary to mimic the paper version to an electronic version. The final business document, submitted to Allscripts, consists of high-level requirements, decision tree, tables and MS Vision diagrams. Below is a summary of requirements divided into time-sequence requirements and behavior of RAI-MDS assessment form.

A. Time-Sequence of the Assessment Form

The MDS Assessment Form is filled at pre-determined and specific times within a resident's stay at the care facility. There are four different assessment forms: Full and quarterly clinical assessment forms and admission/re-entry and discharge forms. The full assessment form needs to be completed at admission, annually and when there is a significant change in the status of a resident. The quarterly assessment form is completed within every 92 days or if there is a need to correct previously completed quarterly form. The admission/re-entry is completed after a resident is admitted to the facility and a discharge form when the resident leaves the facility.

Table 3 is an instance of clinical workflow scenario for an Annual Full Assessment Form. Full Annual Assessment must be opened and completed within the last 366 days of the Assessment Reference Date(A3) of the last Full Assessment. However, it can be initiated at any point prior to the one year follow to date.

Scenario: An existing resident, a Full Assessment performed on June 8th, 2016.
Requirements: 1. Patient's last Assessment Reference Date (A3) for their last Full Assessment is June 8th, 2016. 2. The one-year follow-up date for the patient's next Full Annual Assessment can be any point prior to June 9th, 2017. 3. Full Annual Assessment commences, the Assessment Reference Date is set to June 4th, 2017 (A3). 4. Full Annual Assessment status: open. (Primary Reason for Assessment AA8: 02) 5. The Assessment Coordinator sets the date for completion of the full assessment on June 8th, 2017. – (Date Assessment Coordinator signed as complete R2b) 6. Assessment is closed on June 8th, 2017. (Full Annual Assessment status: closed) **7.** Assessment is locked after the 7-day period on June 22nd, 2017. No alterations can be made to the record past this date. (Full Annual Assessment status: locked).

Table 3: Time-sequence requirement for Annual Full Assessment

B. Behavior of the Assessment Form

Rai-MDS consists of five different record types (Admission Full Assessment, Annual Full Assessment, Quarterly Assessment, Admission/Re-entry, Discharge) and 23 different sections from AA to U as seen in Table 4.

Section AA	Identification Information
Section AB	Demographic Information
Section AC	Customary Routine (Only 1st admission)
Section AD	Administrative Information
Section A	Identification & Background Info
Section B	Cognitive Patterns
Section C	Communications /Hearing Patterns
Section D	Vision Patterns
Section E	Mood and Behaviour Patterns
Section F	Psychological Well-Being
Section G	Physical Functioning & Structural Problem
Section H	Continence in Last 14 Days

Section I	Disease Diagnosis
Section J	Health Conditions
Section K	Oral/ Nutritional Status
Section L	Oral/ Dental Status
Section M	Skin Condition
Section N	Activity Pursuit Patterns
Section O	Medications
Section P	Special Treatment and Procurers
Section Q	Discharge Potential and Overall Status
Section R	Assessment Information
Section U	Medication List

Table 4: Overview of MDS Sections

Section AA, AB, and AD are primarily used in Admission, Re-entry and Discharge forms. Section AC is only filled on first Full Admission Assessment Form. Section B to U consists of clinical indicators specific to Full and Quarterly Assessments forms.

Below, the author describes one of the sections and specifies how the assessment form should be designed for end users.

Section J (Health Conditions):

Section J is one of the 23 sections within the assessment form. It consists of 5 data elements to be captured – Problem Condition(J1), Pain Symptoms(J2), Pain Sites(J3), Accidents(J4), Stability of Conditions(J5). It needs to be filled out in Annual Assessment and Quarterly Assessment.

Item ID	Item Type	Description	Priority	Trigger	Validation	Item Required on Record Type Y = Yes N = No				
						Full Assessment		Quarterly Assessment	Tracking	
						Admission Assessment	Comprehensive Assessment		Discharge	Re-Entry
J1	PROBLEM CONDITION	To record specific problems or symptoms that affect or could affect the resident's health or functional status, and to identify risk factors for illness, accident, and functional decline	Mandatory for full and quarterly assessment	Subset of J	Check all conditions that occurred within the past seven days unless otherwise indicated (i.e. lung aspirations in the last 90 days). If no conditions apply, check J1p. NONE OF ABOVE **INDICATORS OF FLUID STATUS:** a. Weight gain or loss of 1.5 or more kilograms in last 7 days (3 lbs.) b. Inability to lie flat due to shortness of breath c. Dehydrated; e.g. output exceeds intake d. Insufficient fluid; did NOT consume all or almost all liquids provided during last 3 days **OTHER** e. Delusions f. Dizziness/vertigo g. Edema h. Fever i. Hallucinations j. Internal bleeding	Y	Y	Y	N	N

Table 5: Decision Table for J1 Item (Problem Condition)

After reading CIHIs data submission manual, the author drew a decision table for each section. Decision table consists of 7 columns- Item ID, Item Type, Description, Priority, Trigger, Validation, and Item required on Record type. Item ID is the ID assigned by CIHI for data

submission, Item Type is the name of the information to be collected. Priority refers to when the item is mandatory, optional or not required. Trigger refers to when the item is required on the assessment form and its subset or superset descriptions if any. Validation column consists of the questions that the care provider must complete and coding specification provided by CIHI. Finally, "Item Required on record type" is a decision table that describes where the item is required. An example of one section of J (J1) is given in table 5 that specifies what is required of this item when the electronic version is built.

Full Annual Assessment: J1 → J2 → J3 → J4 → J5
Quarterly Assessment: J1 → J2 → J4 → J5

Figure 1: Flow of Items (Section J) on Annual and Quarterly Assessment

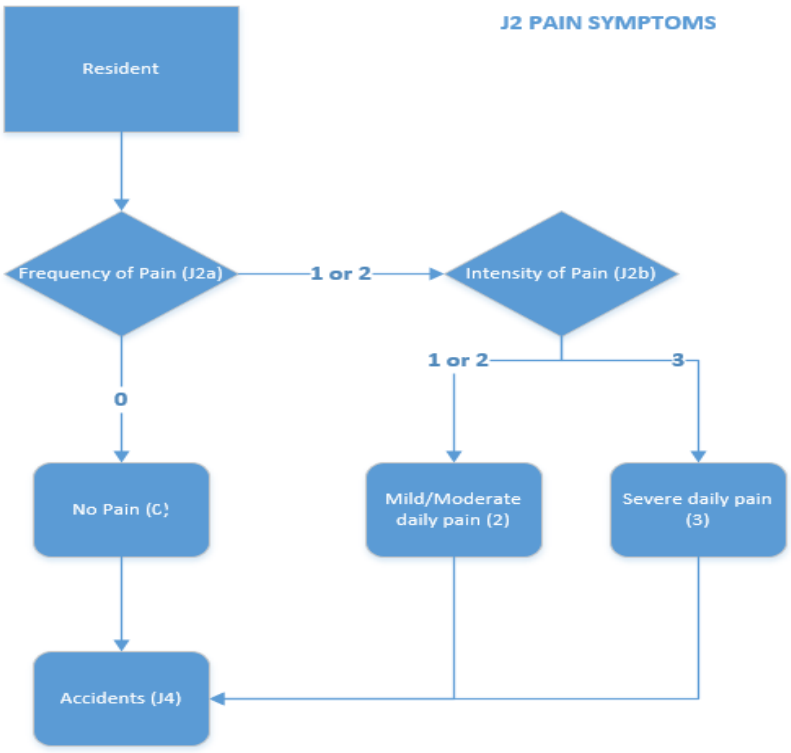

Figure 2: Decision Tree for J2 Pain Symptom (Quarterly Assessment)

Figure 1 is a workflow of items on annual and quarterly assessment end user needs to fill for Health Condition (Section J). When the user wants to fill in Health Condition (Section J) during a full annual assessment, all 5 data elements must be filled, while, J3 is skipped in Quarterly assessment. Figure 2 is a decision tree for Pain Symptoms (Section J2). If the user selects "No Pain/ 0" while filling out J2a then the application should skip J2b and go to "Accidents (J4)". If the user selects "Frequency of Pain" is either 1 or 2, then the system asks for the "Intensity of Pain (J2b)" before going to the next step.

Like the example provided above, he identified skip patterns within the assessment forms and drew decision tables and trees for all 23 sections and data elements contained within those sections.

4. Learning Opportunity and Exposure

Allscripts MHI internship was a great learning experience and an invaluable exposure to the field of health informatics science. It is highly recommended from the authors perspective for students in the MHI internship stream.

Below the author divides "Learning Opportunity and Exposure" into two sections: Privacy and Security Requirements learning opportunity and CIHI RAI-MDS learning opportunity.

1) Privacy and Security Requirements – Infoway

Some of the techniques used by the author to elicit, analyze and write requirements for FollowMyHealth certification includes:

— ***Understanding Infoway's P & S Requirements document***: Reading Canada Health Infoway's Certification Services documents, discussing the document details with the

supervisor and taking detailed notes were the foundation to identifying objectives for this project.

- ***Background Reading on Allscripts and FMH Policies***: Since the author was not familiar with Allscripts Policies and Procedures, reading Privacy and Security Policy documents, FollowMyHealth documents, Allscripts Corporate documents, hosting services documents (Microsoft Azure) familiarized him with Allscripts' policies and their solutions. The policy documents were the key source of information to understand, analyze and write the Privacy, Security and Interoperable self-assessment document for Infoway's Certification.
- ***Existing Requirements document***: Our supervisor provided us with similar existing documents that gave a clearer picture on how a requirements document is completed.
- ***Progress Meetings:*** Bi-weekly progress meetings were an important component of the MHI Allscripts internship. Meetings were used for summarization of findings, a collection of feedbacks, and to raise questions and concerns towards the objectives and progress of the project.
- ***Communication with Solution Experts***: Communication with FMH developers, product managers, and team members gave the author a rich set of information that uncovered opinions as well as hard facts about the solution.

2) Requirements – CIHI RAI-MDS 2.0

Some of the techniques used to model sequence and behavior of the RAI-MDS 2.0 assessment form includes:

- ***Understanding the Objectives***: Understanding Continuing Care Resource Submission procedure, discussing the contents with the supervisor and taking detailed notes were the foundation to this project.

- ***RAI-MDS Manuals:*** Reading RAI-MDS assessment forms, user manuals, data submission manuals, and CCRS reporting specifications gave the author insights on how health care providers and CIHI use this manual for patient care in Canada.
- ***A collection of Requirements:*** Iteratively while reading MDS manuals, the author gathered system requirements to define the new system. The original collection of requirements had to be analyzed and refined.
- ***Timeline for RAI-MDS:*** After gathering requirements, the author focused on the timeline of the MDS assessment requirements needed to build the new system.
- ***Decision Tables:*** Since the MDS form consists of more than 500 data elements, next, the author drew decision tables to identify conditional logics within the document to understand the behavior of the assessment.
- ***Decision Trees:*** Further, the author drew decision trees for each conditional logic to simplify and communicate the requirements to developers.

While working on the high-level requirements for CIHI's MDS assessment form, the author got the opportunity to:

- Learn about interRAI and CIHI services
- Licensing Requirements for the RAI-MDS 2.0
- Understand how RAI-MDS is used in Long Term Facilities
- Learn about data submission manual and CCRS specifications
- Data Elements of Admission, Annual, Quarterly, Discharge and Re-entry
- Understand the timeline for the MDS assessment form

5. Health Informatics Courses

Before this internship, the author had successfully completed all mandatory MHI courses (9 courses) plus 3 optional courses which gave him a keen and in-depth understanding of health

informatics science. While gathering requirements for FollowMyHealth, the author got hands on experience with Canada Health Infoway's Privacy and Security Conceptual Architecture and various data standards. While writing solution requirements for CIHI MDS 2.0 he learned how to write a business document and specification for solution development.

Below is a summary of how the internship relates to Health Informatics courses:

a) Health Information Flow and Use (HINF 6101)

This mandatory MHI course provides valuable insights into how health information flows and is used in a healthcare and population settings. The author used this knowledge and skills from the course to extract requirements and draw clinical processes on Microsoft Visio.

b) Health Information Systems and Issues (HINF 6110)

Knowledge used of this course includes: Canada Health Infoway, CIHI, Software Development Life Cycle, Clinical Information Systems were applicable on both major projects.

c) Health Information Flow and Standards (HINF 6102)

The course trained the author on Infoway's and CIHI's data flow and standards. Knowledge and skills from this course were very useful in completing the project.

d) Networks and the Web for Health Informatics (HINF 6220)

Coming from a non-IT background, this course taught principles of computer system architecture and database design which were useful in understanding the RAI-MDS assessment form requirements.

e) Data Mining for Health Informatics (HINF 6210)

Decision trees and decision tables learned in the course were useful in designing RAI-MDS conditional logics.

f) IT Project Management (HINF 6300)

The author used his project management skills and knowledge learned in the course to understand, organize and manage projects.

g) Healthcare Outcomes (HINF 6300)

This is a Master of Health Administration course consisting lectures on Long Term Care, CIHI, CCRS, and interRAI-MDS. This course made it easier to navigate through CIHI's CCRS documents.

h) Canadian Healthcare Law (HINF 6300)

HINF 6300 contains detailed topics on Healthcare Law in Canada and Government of Canada's Personal Information Protection and Electronic Documents Act (PIPEDIA). The course was very useful in navigating through health information collection and use, privacy policies, patient rights and obligations, provider rights and so on.

6. Conclusion

MHI internship at Allscripts was a great learning experience. It provided an exposure to the current health IT practices through Allscripts' perspective.

The first half, the author worked on Privacy and Security (P&S) Conceptual Architecture designed by Canada Health Infoway. This project taught him the certification process and the requirements needed to certify a consumer health product with Infoway. Second half, the author used informatics science to gather and model requirements to build an electronic assessment form. This project exposed him to writing requirements for time-sequence and behavioral aspect of the RAI-MDS assessment form. It also exposed him to CIHI data submission specifications.

Further, the internship increased his skills on various MS application including Visio, Office, Outlook, Exchange, Excel, Word etc. Finally, it exposed him to health IT solutions experts,

solution managers, executives, business analysts, developers, technical analysts, sales team, informatics intern etc.

7. Recommendation

Following this great learning opportunity, the author recommends:

- Requirements gathering is an iterative and complex process: going back and forth between solution experts and resources.
- Team work and clear communication with stakeholders are vital for navigating and gathering requirements.
- Informatics science is very useful in analyzing and designing user, system and business requirements.
- Using applicable Privacy and Security measures, patient engagement portals such as FollowMyHealth is a great way for patients to become an active member of their care team.
- Use of technology in healthcare can save valuable time and resources.
- Internship at Allscripts is very useful for MHI students.

8. Reference:

Allscripts Canada. (n.d.). Retrieved July 20, 2017, from http://ca.allscripts.com/

Morris JN, Hawes C, Mor V, Phillips C, Fries BE, Nonemaker S, Murphy K, Resident Assessment Instrument (RAI) RAI-MDS 2.0 User's Manual, Canadian Version, Washington DC: interRAI 2010

Infoway. (2017). Vendor Certification Services. Canada Health Infoway Certification Services. Retrieved July 20, 2017, from https://www.infoway-inforoute.ca/en/our-partners/vendors/vendor-certification-services.

9. APPENDIX A

TABLE 1 : P&S Documents Requirements that FollowMyHealth Meets

ID	Requirements	Details
1.	Privacy Policy Document	The purpose of this requirement is to ensure that applicants who may meet PHI as part of the delivery of services can support their client privacy obligations.
2.	Privacy Policy Document (Communication Plan)	The purpose of this privacy policy requirement is to ensure that applicants who may meet PHI as part of the delivery of services can support their client privacy obligations.
3.	Privacy Policy Document (Personnel Training on Communication)	Applicant personnel that provides support or interact directly with clients are trained at least annually in how to communicate the applicant's privacy policy, as well as the process for escalating client privacy inquiries, complaints, and challenges in a confidential manner.
4.	Privacy Officer Name	The applicant has designated an individual accountable for ensuring ongoing compliance with legislated privacy requirements and the applicant's privacy policy.
5.	Privacy Breach Handling Procedure/Manual	The applicant has a documented procedure for handling suspected privacy breaches, which includes steps to inform affected individuals and other relevant parties.
6.	Information Security Policy Document	The purpose of this policy requirement is to ensure that applicant staff who may meet PHI as part of the delivery of services can support their client security obligations.
7.	Information Security Policy Document (Plan Review Evidence)	The applicant reviews their Information Security Policy and Information Security Plan on an annual basis, or more frequently, as well as upon the occurrence of a serious security incident.
8.	Compliance Audit Report	The applicant has performed an audit of its own compliance with the Information Security Policy within the 18 months prior to the certification application date.
9.	Information Security Plan (How objectives will be met on Information Security Policy)	The applicant has a documented Information Security Plan which details how the objectives of the Information Security Policy will be met.

10.	Information Security Plan (Management Process)	The applicant has in place processes for continuous management of Information Security, including monitoring Information Security status and evaluating and responding to emerging issues.
11.	Security Incident Management Process	The applicant has in place a documented procedure for managing security incidents.
12.	Information Security Plan (Procedure to contact external authorities)	The applicant has in place procedures for contacting authorities or involved external parties, in the event of a privacy breach, or security incident in which criminal activity is suspected, or which may require action by an external party.
13.	Terms of Use Document	Sample or Template client contract, and/or Terms of Use agreement to be agreed by patients.
14.	Privacy Impact Assessment	A Privacy Impact Assessment (PIA) or equivalent privacy assessment has been performed for the product and/or service, using an industry-standard method, within 12 months prior to the certification application date.
15.	Review of Information Security Policies	The applicant's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) have been reviewed independently by a third party in the 24 months prior to the certification application date.
16.	Information Security Policy (Conformance Procedure)	The applicant has a documented procedure for internally reviewing its Information Systems for conformance to the requirements of the Information Security Policy.
17.	Threat Risk Assessment (Review/Approval)	A Threat and Risk Assessment (TRA) or equivalent Security assessment has been performed for the product and/or service, using an industry-standard method, within 12 months prior to the certification application date.
18.	Risk Management Process/Procedure	The applicant has in place a documented process for the ongoing management of the privacy and security risks associated with the product and/or service
19.	Information Processing facilities document	Services supporting Information Processing facilities (e.g. power, cooling, network) are protected against interruption. Power and telecommunication cables, specifically, are protected against accidental or malicious damage or disconnection.
20.	Asset Inventory Overview	The applicant maintains an inventory of all assets used in the provision of the service.

21.	Information Classification Policy Overview	The applicant has in place information classification policy to classify the information assets based on the confidentiality, availability, integrity requirements of the assets, and establish security control requirements appropriate to each classification of the assets.
22.	Vulnerability Assessment/Penetration Testing/Report	The applicant performs regular vulnerability assessment or penetration testing to identify and mitigate security vulnerabilities.
23.	Privacy Information Notice + Communication Procedures	The applicant provides privacy information notice to inform the individuals.
24.	Health Information Collection Policy	The product and/or service only collects limited personal health information necessary for the purposes identified.
25.	Data Retention Policy	The applicant has in place a data retention policy specifying how long the data stored in the product will be retained before being disposed.
26.	Data Retention/Disposal Process	The applicant's operational procedures include provisions to meet data retention limits and rules, including mechanisms for removal of personal health information when its retention period has expired, or on request.
27.	Data Use and Disclosure Process	Personal health information in the product and/or service shall only be used or disclosed for the purpose for which it was collected.
28.	Access Control Procedure	The applicant has in place a documented process to respond to an individual's request to access their records.
29.	PHI Correction Procedure	The applicant has in place a documented process to respond to an individual's request to correct their records.
30.	Privacy Complain/Inquiry Procedure	The applicant has in place a documented process for the management of an individual's privacy complaint and/or inquiry.
31.	Terms of Use Document	The applicant does not use Personal Health Information for Marketing or Advertising without the express consent of the patient.
32.	User Registration Process	Users (including Administrative users) are registered through a formal process which establishes the user's identity and the appropriateness of the access which they are to be granted to

		personal health information. User IDs are only used by one user, and are not reused.
33.	User Authentication System Process	The product and/or service has mechanisms in place to ensure that: user IDs are unique and cannot be re-used; user IDs can be decommissioned, or have permissions removed, and that decommissioned user IDs cannot be re-used.
34.	User Credential Management Documentation	Users (including Administrative users) hold credentials (e.g. Passwords) which allow them to prove their identity to the product and/or service. These credentials are unique, stored securely and held only by their designated user. Passwords are never transmitted in the clear.
35.	User Credential Control Process	User credentials are controlled through a formal process which includes verification of the identity of the user. The credential is held only by the user.
36.	Inactive Account Management Mechanism	The product and/or service contains mechanisms by which the access of users who have not used the product and/or service for a defined period may be identified, and if necessary revoked.
37.	Empty	
38.	User Access Privileges (Review)	The product and/or service controls access to system features by permissions which are determined by the users' roles. The product and/or service allows an administrator to create, update and report upon the permissions associated with user roles and the roles assigned to users.
39.	Security Features (Protecting access to Network and Operating System	Administrative access to Network or Operating System infrastructure is restricted to authorized personnel.
40.	Password Policy (Configuration Mechanism)	The product and/or service contains mechanisms to ensure passwords chosen by users conform to configurable password quality policies.
41.	Printed Copy PHI (Completeness/e.g. Pg. no)	The product and/or service produces a visual indication in all printed reports that multi-page hardcopy is complete.
42.	Data Validation Description (Input data)	The product and/or service includes mechanisms to validate the accuracy of received data to safeguard against data quality errors by validating all data input to ensure that it is appropriate within given prescribed rules.

43.	Availability Engineering Description	The product and/or service's availability levels are documented and supported by an infrastructure design.
44.	Business Continuity Plan	The applicant has in place a documented Business Continuity Plan (BCP) for recovery of the services in the event of disaster.
45.	Maintenance Plan (Equipment)	Equipment used for provision of the product and/or service is subject to regular maintenance.
46.	Backup and Recovery (Procedure Manual)	The applicant backs up all software and data relating to the service, encrypts backups, stores backups securely, and regularly (at least annually) rehearses restoration from backup. Restoration activities are logged.
47.	Backup and Recovery Mechanism (Procedure Manual)	The product and/or service provides the ability to back up all software and data relating to the product and/or service, including encryption of backups and logging of restoration activities.
48.	Printed Copy PHI (Confidential Label)	The product and/or service produces a confidential label in all printed reports containing PHI.
49.	Storage of PHI Policy (End User Device encryption)	The product and/or service encrypts all personal health information that is stored on end user devices, or the product and/or service ensures that no personal health information is stored on end user devices.
50.	Storage of PHI Policy (End User Device data flow)	The applicant has policies that limit the storage of PHI on movable media and personal devices, and where necessary ensure that personal health information on movable media such as laptops and removable hard drives are always encrypted, and that movable devices are always physically protected while in transit.
51.	Management of Unencrypted PHI (inventory of media)	The applicant maintains an inventory of media containing unencrypted personal health information.
52.	Protection of External Electronic Message Description	Personal Health Information transmitted outside the product and/or service using electronic messaging is protected against unauthorized access or modification.
53.	Network Security (Protection of Access on Public Networks) Description	The product and/or service contains mechanisms to protect the confidentiality and integrity of information accessed over public networks.

54.	Network Security (Secure interchange) Description	Network Interfaces between the product and/or service's network infrastructure and third parties (particularly EHR systems) which carry personal health information use strong encryption and mutual authentication.
55.	Network Security (Protection of data at rest) Description	The product and/or service has appropriate security controls to protect the data at rest from unauthorized access.
56.	System Administration Manuals (screenshot or description)	The product and/or service logs all User and system actions and can display the details of who entered, accessed or modified what data, in what role, at what time, and from what device.
57.	Audit Logs Monitoring Process	The applicant has in place a mechanism to log administrative activities, such as configuration changes, or other changes originating from a client request or routine administrative activity.
58.	Disclosure of PHI Process/Procedure	The applicant has procedures covering disclosure to third parties, which require that all such disclosures are recorded, including: the party disclosed to; the content of the disclosure; the date and time of the disclosure.
59.	Audit Logs Protection Description	Audit logs are tamper-resistant, and protected against unauthorized access, or loss of integrity or availability, to the same extent as the personal health information which they refer to.
60.	Vulnerability Management Process	The applicant has in place a process for the management of vulnerabilities.
61.	Patch Management Process Documentation	The applicant has in place a documented process for the management of the security patches.
62.	Third Party Agreement Templates	Where a third party is involved in provision of the product and/or service, the third party is governed by a legal agreement.
63.	Third Party supply relationships	The applicant has a documented procedure for managing third-party suppliers.
64.	Confidentiality Agreement Policy Document (who have access to PHI)	The applicant requires all personnel who have access to Personal Health Information to sign a confidentiality agreement.
65.	User Agreement Template	The product and/or service requires users to read and agree to a statement explaining the purposes for which information

		is being collected, and limitations that will be placed on use and disclosure.
66.	Employment Competency Evidence (Privacy/Security)	Job Descriptions for the applicant's personnel who have access to Personal Health Information identify specific responsibilities and required competencies with respect to information security and privacy.
67.	Employment Terms and Conditions	Contractual agreements with the applicant's personnel state the parties' obligations with respect to Information Security and Privacy, both during employment and after termination.
68.	Employment Privacy and Security Training Policy and Materials Overview	Training material for the applicant's personnel includes material relating to Privacy and Security requirements, and Organizational Privacy and Security Policies and Procedures.
69.	Employment Disciplinary Outline	The applicant has a formal disciplinary process dealing with personnel breaches of information security.
70.	Employment Change of Role/Termination Outline	The applicant has in place documented procedures for handling changes in the role of its personnel including termination.
71.	Physical Security Overview (Information Processing Facility)	Information Processing facilities are housed in secure areas equipped with entry controls and other Physical Security Measures designed to protect against unauthorized access, natural disaster or accident.
72.	Physical Security (Applicants Premises)	Secure areas of the applicant's premises are protected by Physical Security Measures to prevent unauthorized access.
73.	Security (Offsite Equipment)	Equipment which might leave the applicant's premises is protected by security provisions to prevent unauthorized access to personal health information.
74.	Reuse/Disposal of equipment Procedure Manual	The applicant has procedures in place to cover secure disposal or reuse of equipment, media or storage space containing personal health information.
75.	Information Security Policy Overview	The applicant's Information Security Policy (or equivalent document) requires that equipment, data or software may not be removed from the applicant's premises without authorization.
76.	Overview of Hosting Services	Overview of hosting arrangements, identifying equipment (servers, virtual or physical storage, virtual or physical network segments) hosting the product and/or service.

77.	Overview of Capacity Management	Operational procedures include monitoring of levels of usage of IT infrastructure, and planning future required capacity. Operations Documentation.
78.	Overview of Anti-malware	The product and/or service is protected against malicious software, using technical and administrative measures. Overview of anti-malware provisions (both technical and administrative).
79.	Overview of Network Protection	Networks (including virtual private networks) connecting Information Processing Facilities include protection against unauthorized access. Overview of network architecture showing network features intended to prevent unauthorized access.
80.	Description of Time Synchronization features.	The product and/or service is synchronized with an authoritative source for the current time, so that any record of the time of an event is accurate.
81.	Description of protecting Cryptographic Keys	The applicant manages Cryptographic Keys in such a way that they are protected from unauthorized disclosure. Description of Security Features protecting Cryptographic Keys.
82.	Protection for Development and Test (source code, test data etc.)	The applicant protects source code, test data, development and test system environments against unauthorized access, loss of availability or integrity. Architecture Diagrams, Policy Documents and Description of security provisions protecting source code, test data, development and test system environments.
83.	Documents/Records Management Process/Procedure Manuals	The applicant has in place procedures for management of all documents or records required for its operations.
84.	Operations Document (Overview)	The applicant has documentation covering operational procedures for the product and/or service. The operating procedures specify the instructions for the detailed execution of jobs, such as performing backups, system restart and recovery procedures, and error handling.
85.	Information Systems Development Policies	The applicant has documented policies for Information Systems Development/Acquisition and Change.
86.	Information Systems Change Management Procedure/Manual	The applicant's procedures for changes to Operating Procedures, Information Systems or IT platform components, and onboarding of new partner applications, include explicit authorization from management accountable for Information

		Security, and testing to ensure there is no adverse effect on operations or security.

10. APPENDIX B

TABLE 2: P&S Documents Requirements that FollowMyHealth Meets

ID	Requirements	Details
1.	Patient Access Mechanism	The product and/or service contains mechanisms to produce a copy of the individual's records in a format usable by the individual (i.e. human readable).
2.	Corrections Mechanism	The product and/or service contains mechanisms that can be used to record the following four elements: patient's request to correct a portion of their health record; action taken in response to the request for correction (e.g., changes that were made, if any, or the reason that changes were not made); date/time of request; date/time of action taken in response to the request.
3.	Recording & Displaying Agreement	The product contains mechanisms to record a disagreement with the individual regarding information in their records. The product can display the disagreement to users who view the individual's records.
4.	Recording Consent	The product and/or service includes mechanisms to record a patient's disclosure directives including the withholding, withdrawal or revocation of consent to access information. Where consent is given by a substitute decision maker on behalf of a patient, the product includes mechanisms to record the identity of the substitute decision maker and the substitute decision maker's relationship to the patient.
5.	User Identity Management	The product and/or service has mechanisms in place to ensure that: user IDs are unique and cannot be re-used; user IDs can be decommissioned, or have permissions removed, and that decommissioned user IDs cannot be re-used.
6.	User Credential Management Documentation	The product and/or service shall have functionality to ensure that users (including Administrative users) hold credentials (e.g. Passwords) which allow them to prove their identity to the product and/or service.

7.	Screen Time-Out & Re-authentication	The product and/or service automatically locks and requires the User to re-authenticate after a configurable period of inactivity.
8.	Account Lockout	The product and/or service denies access to a known user for a defined period, if that known user has unsuccessfully attempted to log in a fixed number of times in a defined period.
9.	Role-based Access Control	The product and/or service controls access to system features by permissions which are determined by the users' roles.
10.	Secure Log-On	The product and/or service requires a user to authenticate themselves using a secure credential, prior to granting access to any personal health information.
11.	Password Management	The product and/or service contains mechanisms to ensure passwords chosen by users conform to configurable password quality policies.
12.	End User Device Encryption	The product and/or service encrypts all personal health information that is stored on end user devices, or the product and/or service ensures that no personal health information is stored on end user devices.
13.	Audit Records	The product and/or service logs all User and system actions and can display the details of who entered, accessed or modified what data, in what role, at what time, and from what device.
14.	Audit Reports	The product and/or service is capable of reporting: comprehensive history of accesses.
15.	Sorting of Audit Reports	Audit reports are sortable on the following fields, for privacy investigation purposes: Date/Time; Patient ID; User ID; Action taken (addition, change, deletion, print, copy, transmission, consent override); Data accessed.
16.	Logging of Faults	The product and/or service creates log records when unexpected errors occur.
17.	History Retention of Patient Records	The product and/or service can display the former content of a record as it existed at any point in the past. This applies to patient data and non-patient data (e.g. practice metadata or user permissions metadata).
18.	Acceptable Use Agreements	The product and/or service includes mechanisms to make users aware of their responsibilities, by requiring users to agree to them as part of a configurable Acceptable Use Agreement.

19.	Confidentiality Message on Log-In	The product and/or service displays a confidentiality message to the user upon log-in.
20.	User Agreements	The product and/or service requires users to read and agree to a statement explaining the purposes for which information is being collected, and limitations that will be placed on use and disclosure.