Collaborative Solutions for Active Living Inc. (PIP3)

Personal Information Privacy and Protection Policy (“PIP3”)

1 Preamble - Version v1.1.1 (June 2017)

This document defines the Collaborative Solutions for Active Living Inc. (“CS4”) operating policy with respect to maintaining Personal Information Privacy and Protection. CS4 owns and operates the WhoKnozMe applications software products which provide patient-centric health information Services (the “Health Information Service”). This Policy is fully implemented and integrated within all WhoKnozMe internet Portal Applications and within all WhoKnozMe databases. WhoKnozMe Application Portals contain all Users’ access to their own Personal Information as well as CS4’s access to those Users’ data elements needed to operate the Health Information Service. The Policy further outlines some of the various strategies and tactics used to protect personal information as stored within the Health Information Service data bases.

Unless otherwise indicated, or the context otherwise requires, references in this document to “Collaborative Solutions”, “CS4”, the “Company”, “we”, “us” or “our” refer to Collaborative Solutions for Active Living Inc. and its subsidiaries.

WhoKnozMe® is the technology platform name of our Health Information Service operating division.

This Policy Document is the property of Collaborative Solutions for Active Living Inc. It is provided to the Reader as a corporate information document and as our statement of our dedication and commitment to maintain the privacy and security of your personal information.

1.1 *Reference Materials*

Reference Materials used in the derivation of this policy document are contained within the attached Appendices. They include glossaries of technical terms and acronyms and external documents referenced by CS4 staff in the derivation of this document. Where possible, source website directions are provided to assist readers in accessing relevant reference materials.

1.2 *Nota Bene*

This Policy Document is still a “work-in-progress” and is not yet complete (2017-06-06). CS4 staff work on it as time and available information permits. It is long and complicated because the subject (essentially the Privacy Policy for the CS4 “patient centric” health information system) is, in and of itself, long and complicated. We are striving to create a truly modern and effective personal health information system with all the Privacy aspects designed in from the beginning along with most of the internal Data Security aspects.

Our overall data model incorporates new as well as traditional approaches for managing access to personal data.
We have made use of the extensive work (external to us) that has gone into the Health Level 7 language facility over the last twenty-odd years. The development of HL7 and particularly the latest work (“FHIR”) has moved this language from a primary messaging facility to an overall medical and health interoperability model.

The CS4 data model has been greatly evolved from an Electronic Data Interchange data model (a la ANSI ASC X12) so as to properly manage digital personal health and medical information including the inter-personal and inter-organizational relationships (i.e. providers to patients and vice versa, companies to individuals and vice versa, regulatory authorities to providers, etc.). In doing so, we have also committed to providing these services to our clients in a manner that deliberately and intelligently follows the letter and the intentions of the appropriate privacy and security legislation.

Please do not hesitate to contact us if you have difficulty or disagreement of any sort with the elements of this policy document. We welcome feedback and commentary.

1.3 *Revision History*

Revisions	By	Issue Date	Comments
Prepared	pfd, jrd	2016-01-29	Based on Patients Know Best.
Reviewed	Initial Board Review	2017-01-11	pfd, jrd, jrm-l, iah
Updates & Additions	pfd, jml	2017-06-06	Updates and developments w.r.t. Alberta Health RFP 17-1353

Table of Contents

2 Introduction

Collaborative Solutions for Active Living Inc. (“CS4”, “Collaborative Solutions”) provides WhoKnozMe, a patient-centric personal health and medical information service, along with other associated service tools collectively called the “Health Information Service".

Privacy and security in any health information system today must balance two competing social benefits:

- the need to appropriately access and share information to enhance care quality and safety as well as to provide continuity of care; and
- the need to implement reasonable safeguards to maintain the privacy of personal health information.

This Policy Document explains the provisions of CS4’s policy to maintain the privacy of your personal health and medical information and to protect it from unwarranted and/or unauthorized inspection or extraction by others. It also explains why CS4 needs access to a small number of items of your general information in order to provide the Health Information Service.

The WhoKnozMe Health Information Service provides the means by which Users can store, manage and share their own personal medical and health information in a secure and effective manner. They can also, store, manage and share the personal medical and health information of other Individuals they may care for (e.g. dependent children, incapable elders, etc.). The vast majority of this personal health information is descriptive and time sequenced in nature and solely associated with the referenced Individual. This personal information is kept internally and securely within their respective User Account information storage areas.

WhoKnozMe Users are classified in different categories depending on the licensing and subscription arrangements they have entered into with CS4. The provisions of this Policy apply without restriction or limitation to all Users without regard to their class.

2.1 *Our Commitment*

CS4 is committed to maintaining the privacy of your personal information and also to protecting it from other persons or organizations attempting to record, copy, alter, erase or otherwise interfere with your personal information. CS4 provides layered measures and procedures to limit and control access to your personal information stored in our Health Information Service while preserving reasonable access for yourself and your explicitly permitted representatives and/or Health Care Providers.

CS4 is committed to a “hands-off” approach in providing facilities for storing your personal health information. Other than for some necessary (and herein itemized) personal details associated with managing your personal account we have no access to your personal and private health information as stored by the Health Information Service.

CS4 is committed to following all applicable and pertinent Personal Information Protection Acts (PIPA legislation). Additionally CS4 is committed to following “Best Practices” for maintaining the privacy of your personal information as well as “Best Practices” for computer systems security and data security.

CS4 is committed to undertake regular reviews of this Policy. We will continually reassess our compliance with updated legislation, regulations, best practices and new information technology.

2.2 *Our Approach to Privacy and Security*

CS4 is committed to protecting the privacy of your personal information. The purpose of this Policy statement is to explain to our Users how CS4 executes this commitment by managing their privacy and the protection of their personal information when loaded into the WhoKnozMe Health Information Service. We do this by a number of means, the most important of which is the design process we followed during our initial development of the database definition and the database access techniques. Our database is organized in terms of individual virtual Safety Deposit Boxes which effectively compartmentalize all access to explicitly permitted domains and do not permit searching outside of them or through them.

Our overall processes for providing privacy and security are based around:

- A detailed design for the WhoKnozMe system database and database access routines which incorporate a priori specific stratagems and tactics to restrict and/or deny unwarranted and unauthorized intrusions into your personal information.
- Multiple levels of User-defined security controls (User_IDs, Passwords, Questions and Answers (also known as “QnAs”), etc.) for your direct access to your personal data.
- Multiple levels of User-defined personal information sharing controls including elapsed time limitations and specified termination dates.
- A series of defined software and hardware procedures used to identify and verify that the Users are who they say they are.
- The incorporation and integration of the salient processes published in various Guides and Implementation Guidelines as part of the governing Canadian PIPA legislation.
- The recording of pertinent information about all attempts to access the WhoKnozMe system.
- The building and maintaining of use-restricted Registers of Individuals, Users, Medical Practitioners, Health Care Providers and Companies.
- The timely and appropriate notification of the creation, modification and deletion of relationships between Users, other Individuals, as well as Health Care Providers and Medical Practitioners.
- The appointment of Corporate Officers to manage our Personal Information Protection processes (“The CS4 Privacy Officer”), and our overall Information System Security (“The CS4 Information Security Officer”).
- The appointment of our Registrars (“The CS4 Registrars”) who are in charge of verifying the contents and maintaining the accuracy of our Registries.

CS4 will comply, as a minimum, with all of the statutory requirements of the PIPA Legislation.

This Policy Document will be updated from time-to-time to reflect ongoing changes in legislation, in regulation and in legal understanding as well as to changes in information technology.

Should you need more information about CS4’s Personal Information Privacy and Protection Policy please contact our Privacy Officer at Privacy.Officer@whoknozme.com. Should you need more information about CS4’s Computer System Security and Data Security please contact our Information Security Officer at InformationSecurity.Officer@whoknozme.com.

CS4’s WhoKnozMe Software Products and Health Information Services conform completely to this Policy.

Nota Bene: CS4 neither has nor intends to have access to any personal and confidential information contained in your virtual Safety Deposit Boxes or in the Capsules that may be located therein. The access to your confidential information is completely controlled by you.

2.3 *Historical Basis for Protection of Personal Data*

The introduction of computer technology into the business world in the 1950s (which included hospitals and other national health services) gave rise to consideration of what fundamental rights should exist for the protection of privacy for the users and subjects behind the data in those early systems. This discussion went on for several decades on distinctly national lines in many countries including but not limited to the United States of America, the United Kingdom, France, Canada and Australia.

The first multi-national discussion on Protection of Personal Data started in Europe following the initial development phases of the European Union (“EU”). In 1980 the Organization for Economic Cooperation and Development (“OECD”) issued their Guidelines covering “The Protection of Privacy and Trans-Border Flows of Personal Data”. A short summary of basic principles behind these guidelines is included in Appendix A attached hereto.

Over time, and almost three decades later, most countries in the developed world had enacted detailed legislation covering the Protection of Personal Data. Interestingly the majority of this national legislation is based on the basic principles stated in the 1980 OECD guidelines. There are many national twists and focuses in the corpus of privacy legislation but essentially they all follow the same basic principles.

2.4 *Applicable Canadian Legislation*

The initial and primary marketplace for the Health Information Service is throughout Canada. The privacy and security of both your personal information and your personal health information is covered in Canada by extensive legislation enacted federally and provincially. CS4 has studied this legislation and has carefully crafted this Policy Document in consideration of the salient features and the specific requirements of the various applicable acts.

A characteristic of Canadian privacy and personal information protection legislation is that there are usually at least two acts per jurisdiction; one for the public sector (government and government institutions) and one for the private sector (commercial organizations). In a number of instances (notably in Ontario and in Alberta) there is yet another set of legislation relating specifically to Personal Health Information. A summary of the pertinent Canadian federal and provincial legislation is attached in Appendix D.

2.5 *Other Legislation*

As stated immediately above, the initial and primary marketplace for the Health Information Service is throughout Canada. Our incorporation of the Internet as the data communications medium permits it to be used from almost any location in the world. This means that usage in countries other than Canada would and could fall under other national legislation.

In the European Union (“EU”) personal data protection is currently regulated by the Data Protection Directive 95/46/EC and after April 2018 by the General Data Protection Regulation. In part the Data Protection Directive states “The EU data protection rules are applicable not only when the controller is established within the EU, but whenever the controller uses equipment situated within the EU in order to process data. Controllers from outside the EU, processing data in the EU, will have to follow data protection regulation. In principle, any online business trading with EU residents would process some personal data and would be using equipment in the EU to process the data (i.e. the customer's computer). As a consequence, the website operator would have to comply with the European data protection rules.” What is clear to CS4 is that when the Health Information Service is used from within the EU that the EU Data Protection Directive applies.

This above directive was written before the breakthrough of the Internet, and to date there is little jurisprudence on this subject.

In the United States of America (“USA”) there is a variety of federal and state enacted legislation that covers the privacy of personal information. In the general sense, this is referred to as Personally Identifiable Information (“PII”) and as Sensitive Personal Information (“SPI”). The Privacy Act of 1974 established a Code of Fair Information Practice that governs the collection, use and dissemination of PII about individuals that is maintained in U.S. federal systems. The primary focus of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) is to protect a patient’s Protected Health Information (“PHI”) which is equivalent to PII and SPI. The HIPAA legislation is a massive omnibus act which covers all aspects of the Health Information Services industry. It prescribes, inter alia, how the protection of personal health information must be managed as well as how the security strategies and tactics must be implemented and maintained. A review of HIPAA requirements lies beyond the scope of this document. What is clear to CS4 is that when the Health Information Service is used from within the USA then the HIPAA requirements apply.

Many other countries in the world have enacted similar legislation to those of Canada, the European Union and the United States of America. While CS4 cannot guarantee that we explicitly comply with all of this legislation, it is our intention and our practice to conform as best we can. For the moment, we conform to the overall requirements of the extant Canadian legislation.

2.6 ***Data Storage***

CS4’s data centres are located in Canada and are currently mirrored between Kamloops, British Columbia and Calgary, Alberta. Additional data centres will be added as and when necessary.

3 Characteristics of WhoKnozMe Privacy and Security

The design of the WhoKnozMe Health Information Services system is based on a fundamental CS4 requirement to maintain secure functioning of our software products at multiple operating levels.

- **Privacy is built-in by Design, not bolted-on.**
- **Security is initially built-in by Design, but later developments can be bolted-on**.

A User Account, Username and Password(s) as well as other advanced security features are critical to protecting the integrity of the WhoKnozMe database containing your confidential information. It is also important that the data model siting on and applications accessing the database collectively enables CS4 and you to secure protection of your data.

The WhoKnozMe Health Information Services are provided via an Internet portal function which accesses a proprietary Object Relational database system known as RelBuilder 2.x. This Object-Relational database system currently relies on a standard Structured Query Language ("SQL") database system known as MySQL as its primary engine. CS4 uses built-in security controls at the programming-level of the primary CS4 business objects for fundamental security. It also uses the standard SQL security functions of MySQL for initial overall database security.

The overall design controls access to individual data records based on ownership and owner-defined permissions. In other words, access to your records is under your control, and, you control who may be permitted to view, extract, modify or add to your individual data records. You may revoke these permissions as you see fit. You, as the User, may access any and all of your records but you cannot access anyone else's records unless you have their explicit permission to do so.

You may share access to some or all of your records with others, such as your spouse or partner or your various doctors or other health care givers. You may also share the records of individuals for whom you have been granted representation status (such as for a dependent child or a dependent parent.

Key components of the Health Information Service are the various relationships that the User will have with other individuals and/or organisations. Thus, an Individual (the User) will have a relationship with their own doctor (commonly a GP or General Practitioner) for regular checkups and straightforward treatments. The Individual may also have a Specialist Doctor, who their GP has made a referral to for treatment of a specific disorder, for instance to an Endocrinologist for treatment of advanced diabetic conditions. Both of these relationships would be defined for the Individual and would be known to others but not the specific details of any conditions or treatments. The information about the conditions and treatments would be stored securely within the User's vSDBox and within the GP's and the Specialist's filing systems. The Relationships are not completely private but they are also not public. The Doctors themselves are public items because of their position in society and because they must be members of a college which publishes their names and practice addresses. The relationships between a patient (WhoKnozMe User) and the doctors are thus semi-private and should not be disclosed to uninvolved third parties. Other relationships such as those of legal representation (particularly for health purposes) are also semi-private because the person who is acting as the representative for a patient has to disclose the representation agreement to various other persons, such as doctors, nurses, pharmacists, etc. in order to effect the representation.

CS4 does not own any of our Users' Personal Information. CS4 does own some information about our Users but only that information necessary for CS4 to operate the overall Health Information Service (the "Minimum User Personal Data" and "Minimum User Personal Relationship Data"). On acceptance of the Terms of Usage Users agree that CS4 may use their data defined herein as "Minimum User Personal Data" and "Minimum Personal Relationship Data" for the operation of the overall Health Information Service, without restriction. CS4 agrees not to distribute or provide said "Minimum User Personal Data" and "Minimum Personal Relationship Data" in simple or aggregate form to any Third Party unless ordered to do so by Court Order or Government Statute.

CS4 agrees not to use the "Minimum User Personal Data" and "Minimum Personal Relationship Data" in its marketing or selling efforts. CS4, however, maintains its rights and duties to communicate directly with third parties specifically referenced by Users in their own relationship definitions for notification, validation and verification purposes.

CS4 has no ability to enter any User's vSDBox and access any of their Personal Information stored there.

3.1 *Privacy Classifications of Data*

All data stored within the WhoKnozMe Health Information Service is classified as follows:

- PERSONALLY PRIVATE
- PRIVATE
- PRIVILEGED
- PUBLIC

PERSONALLY PRIVATE data is all health, medical, and other distinctly personal data about you. It includes your entire PHI ("Personal Health Information") defined earlier in this document. This is our highest level of privacy classification.

PRIVATE data is personal data about you that you have agreed to share with others. Largely this is data that defines the various relationships you are in with others and information that is associated or attached to said relationships.

PRIVILEGED data is information about you that CS4 needs to know in order to manage the Health Information Service. This includes your name, your e-mail addresses, your postal code, etc. and is further defined in the Minimum User Personal Data, Minimum User Relationship Data and Minimum Company Data.

PUBLIC data is information about you and others that exists in the public domain. An example is a list of Medical Practitioners with their names, their licensed specialties and their practice addresses that are published by their professional organization (usually called a College). Another example of PUBLIC data is your name, your telephone number, and your address as published in a telephone book or in an on-line digital directory.

3.2 *Minimum User PRIVILEGED Personal Data*

CS4 requires the following minimum personal data from each User:

- Full Name,
- Postal Addresses, (for Billings and Deliveries)
- Personal e-mail Address(es),
- Birth Date,
- Death Date,
- Contact Telephone Numbers,
- Fax Number,
- Provincial Health Number (“PHN”) or Driver’s License Number (“DLN”) or Identity Document Number (Validation), and
- Account Identification (actually generated by CS4).

This information is essential for CS4 communications directly with the User and for other CS4 administration purposes. In particular, CS4 will need to verify and be able to verify that the User is actually a person and, furthermore, test that the individual person acting as a User is actually that identified person or their permitted representative.

All of the above information is stored within the WhoKnozMe Person Registry (which contains minimum Identity and Validation information for each User) with the exception of the Birth and Death Dates. The User’s Birth and Death Dates are recoverable, as and when needed by the Registrar, via a standard business transaction.

3.3 *Minimum User PRIVILEGED Personal Relationship Data*

CS4 requires the following minimum relationship data from each relationship an Individual has with any other third parties:

1. Full Name of the Third Party,
2. Type of Relationship,
3. Position of Individual in Relationship (Object::Subject::Reference),
4. Date and Time Relationship Initiated, and
5. Date and Time Relationship Terminated as well as
6. Certification of the Relationship (if needed)

3.4 *Minimum Company PRIVILEGED Data*

CS4 requires the following Minimum Company Data:

1. Full Name,
2. Short Name,
3. Postal Address,
4. Delivery Address,
5. E-mail address(es),
6. Contact Telephone Numbers
7. Contact FAX Numbers
8. Contact Person(s)
9. Account Identification (actually generated by CS4).

CS4 requires minimum Company information for a number of reasons. First, a Company is treated in law as being notionally and legally equivalent to a "person". Second, some companies are the corporate embodiments of a person. Commonly, in the WhoKnozMe sense, a "Medical Practitioner" runs their practice as a "Professional Corporation". The individual doctor is still a person (who could also be a User of WhoKnozMe) but the Relationship that another Individual might have with the doctor would be termed "p2c" (or "person to company"). Third, a group of doctors may incorporate their professional services into a clinic. Fourth, CS4 has a Duty of Notification to a Company registered with us when other Individuals or Companies incorporate that Company into a Personal Relationship.

3.5 ***Duties of Notification***

As the provider of the WhoKnozMe personal Health Information Service CS4 has an explicit "Duty of Notification" to you with respect to the maintenance of the privacy of your personal information and another explicit "Duty of Notification" to other persons (including Companies) who are in specified relationships with you.

Each time you or a person you have authorized tries to access your personal information we record the date and time of the access request as well as the identifier for that person. Each time a change is made to your personal information we record the date and time of the access as well as the overall nature of the change and the identifier for the person making the change. Normally, CS4 does not provide a notification to you of this change. CS4 can, via a request to the Registrar, provide you with a summary list of all such permitted accesses and changes.

When you create a new relationship with a Third Party (whether a User, Medical Practitioner, Care Giver, Family Member, etc. or Company) CS4 has a Duty to Notify the Third Party on your behalf that you have created this relationship. We normally try to do this with an e-mail to the Third Party but we can send faxes and failing both an e-mail address and a fax number we will even send a regular letter to them. The Third Party can then:

1. Accept the Notification by responding positively to CS4 (in which case the Relationship will continue to be confirmed by CS4), or
2. Reject the Notification by responding (within a reasonable period of time) negatively to CS4 (in which case the Relationship will be nullified by CS4), or
3. Do nothing which will result in CS4 continuing to allow the Relationship.

When you modify an existing relationship the Third Party will be notified by CS4 of such modification.

When you terminate an existing relationship the Third Party will be notified by CS4 of such termination.

Should a Third Party attempt to access your data without your permission then we would immediately notify you of this attempt.

WhoKnozMe allows Individuals to gather, record, edit, store and share all or some of their personal health information in a secure electronic format. This promotes their ability to take an active, and when necessary, assertive role in their health management. It allows the individuals to share their information in a secure manner with family members, health representatives and health professionals. It also allows a person to store and access information in separate records for others, such as a children, parents or friends. Users can also add data to their own health records using electronic devices (e.g. blood pressure and blood glucose meters).

Collaborative Solutions for Active Living Inc. (PIP3)

CS4 is committed to protecting your privacy and personal and confidential information of which your personal health record is one type.

This Personal Information Privacy and Protection Policy (“PIP3 or Policy”) applies only to the personal information collected with WhoKnozMe software. The Policy and its protections do not extend to your other online or offline sites, products, or services for fitness, health or dietary or social media sites.

Note: A fundamental aspect of the CS4 - User Management Services is the set of tools available for password resetting, relationship notifications from Users and Practitioners as well as Message notifications all of which normally use standard e-mail as the medium.

All Users are advised to maintain a “secure” eMail service with a strong password updated frequently.

All Users are further advised to only permit “trusted” individuals to have separate access to their data.

4 Fundamental Concepts

The WhoKnozMe Health Information System is a “Patient-Centric System”. What this term means is that the Patient is always at the centre or core of the incumbent data structures and data pathways. Alternative (and more traditional) health information systems have the institution (i.e. a health authority or a hospital) or a doctor or clinic as the centre or core of the system and the patients are simply elements inside the processes.

In a Patient-Centric System we still have all the same primary elements (patients, doctors, nurses, diagnoses, treatments, test results, etc., etc.) as in a traditional health information system but the etymology, order, organization and interconnections are managed in slightly to significantly different manners. In this section we define how data is ordered, organized and stored in the WhoKnozMe system.

4.1 *Primary Data Elements*

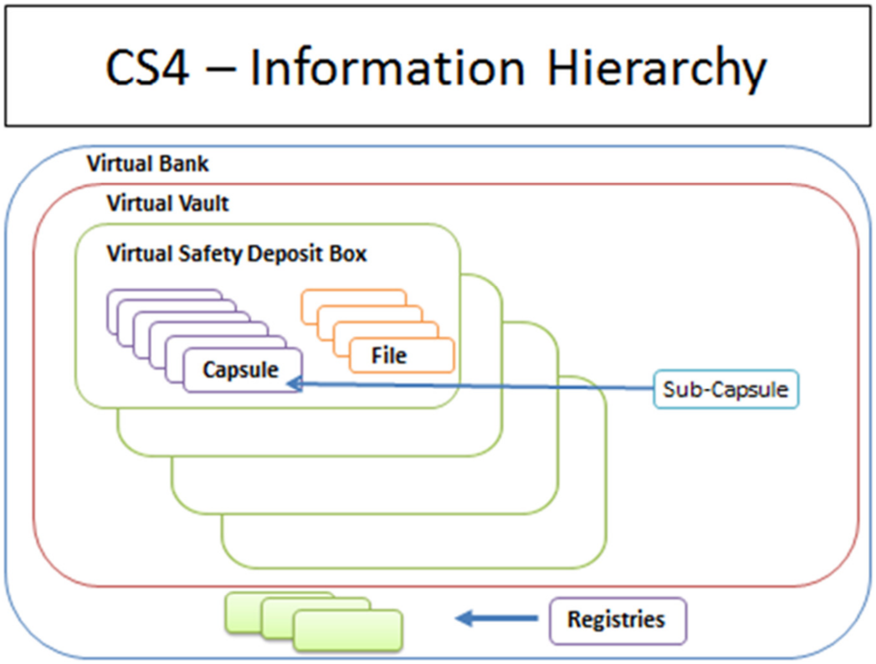
The WhoKnozMe® Health Information System organizes and maintains the following primary data elements

- Patients
  - Users
    - Personal Information
    - Personal Health Information
    - Health Representatives
    - Emergency Contacts
- Medical and Health Service Providers
  - Medical Practitioners
  - Health Service Providers
  - Care Service Providers
  - Care Teams
- Relationships
  - “Trusted” Relationships
- Registrars
  - Registries
- System Facilitators
  - Administrators
  - Customer Relations and Support Personnel
  -

All of the above primary data elements are more fully described in the following sections.

4.2 *Data Storage Model*

It is important for Privacy considerations to give the reader an outline of the WhoKnozMe information storage model. In essence, the following diagram outlines the hierarchy of our information (or data storage) model.



The all-inclusive “Virtual Bank” is an “Enterprise Level” collection of data objects which relate more to the overall data management that CS4 has to do to manage the whole system than to individual Patients. The banking analogy here is to a physical national bank. The physical security here is to control the entry of Individuals through the front door of the bank building itself. A series of Registries (containing inter alia the names of account holders) are stored at this level to facilitate the operations of the bank.

The “Virtual Vault” is the encompassing element for an application zone. In the WhoKnozMe case it is the overall bounds of the health information system. It may have millions of patients’ accounts stored within it. The banking analogy here is to the vault which would contain the working cash and banking instruments as well as customers’ safety deposit boxes. The physical security element here is the direct identification and validation of the Individual with a valid User-Account code (at the very least) before permitting entry into the vault. Only validated users can have access to the vault. A non-banking CS4 security feature is that the validated User can only “see” the Virtual Safety Deposit Boxes they own or are directly responsible for.

There are actually a number of “Virtual Vaults” for the Health Information System. The main “Virtual Vaults” of interest to those using the Health Information System are:

1. The “Patients” Virtual Vault which holds all the data owned by the Patients and their Representatives; and
2. The “Practitioners” Virtual Vault which holds all the data owned by Medical Practitioners, Health Practitioners, Health Care Providers and related individuals.

An Individual who is a Medical Doctor, for example, could be defined both as the owner of a “Practitioner’s Account” in the “Practitioners Virtual Vault” and as the owner of a “Patient’s Account” in the “Patients Virtual Vault”. The purposes, content and organization of the two accounts are distinctly different and separate.

The “Virtual Safety Deposit Boxes” (also known as “vSDBoxes”) are assigned to individual owners (or Users). The banking analogy is to individual safety deposit boxes within the bank vault. The physical security here is (1) the User has previously been identified as a valid user and (2) the User has to provide (at the very least) the correct password to enter into any Virtual Safety Deposit Box they can see. The majority of an Individual’s person information and personal health information is stored at this level.

Within each vSDBox there will be a series of virtual Capsules which have no direct banking analogy. They are used to store other essential information such as “information sharing” instructions, notifications, messages, emergency contacts, the Owner’s ePHRecord, relationships, accounts and identities and new information. Each virtual Capsule has (at the very least) another unique password which the Individual has to provide before being allowed to explore the capsule.

In addition, there may also be a series of sub-capsules within a Virtual Capsule. These sub-Capsules are used largely to contain details of personally private data that can be shared with other Users of the Health Information System.

5 Patients

In a Patient-Centric Health Information System the subject is always the **Patient**. A Patient is always a natural person and is the **Owner** of their own health information. The patient/owner may be a **User** of the system but only if they are considered to be capable. In the cases of an infant or a child below the age of majority or a dependent adult then a **Representative** will need to be appointed as the User.

In Canadian Law a person owns a copy of their own personal health information. Other persons and institutions may also own a copy of all or part of a patient’s health information. These other persons and institutions may be doctors, nurse practitioners, medical clinics, laboratories, hospitals, etc.

A patient’s ownership of their copy of their personal health information is an absolute right regardless of their age or capability. On the death of a patient the ownership of their personal health information would pass to their estate. What happens after the estate is wound-up is not as yet clear (2017).

The patient’s ownership rights extend to the maintenance of privacy of their personal health data. Should they have paper transcripts of any of their personal health data then they are themselves responsible for the maintenance of the privacy of the paper transcripts. In a household situation this could mean that the transcripts are stored in a locked filing cabinet.

5.1 *Patient’s Personal Information*

A Patient’s Personal Information includes all of the information personal to them. This includes, for example:

- their full name
- their gender
- their birth date (and thus their age)
- their citizenship(s)
- their current home address
- their Social Insurance Number (“SIN”)
- their education
- their marital status
- etc.
- and ALL of their Personal Health Information

There could easily be thousands and thousands of personal data items extant for any individual. Not all of the listed items are necessarily defined as "Private" information because, at the very least, access to the information itself will depend upon some form of identifier such as a 'full name'.

As described earlier, a substantial body of legislation exists that covers the protection of privacy and security of this personal data.

5.2 ***Patient's Personal Health Information***

A Patient's Personal Health Information comes from a wide variety of sources and, furthermore, consists of a wide variety of data types. Not all of a Patient's Personal Health Information is maintained in provincial government health information databases.

There are currently (January 2017) 19 major classifications of personal health information defined in WhoKnozMe:

1. Participant Identification
2. Demographics
3. Emergency & Care Team Contacts
4. Medical and Other Insurance Accounts
5. Present Health Concerns
6. Medicinal Products
    a. Prescriptions
    b. OTC (Over-the-Counter)
    c. Ethical (Opiates and other Restricted Analgesics)
    d. Immunizing Materials
    e. Natural Products
7. Immunization and Travel History
8. Personal Medical History
9. Family Medical History
10. Medical (Diagnostic) History
11. Injury & Poisoning & External Causes
12. Surgical and Other Procedure History
13. Other Treatments
14. Adverse Effects (Allergies, Reactions or Treatment)
15. Lab Results
16. Medical Imaging Files
17. Medical Documents
18. Patient Medical Summaries
    a. Emergency ("Emergency Medical Summary")
    b. Logbook ("Specialist Medical Summary")
    c. Intake Form ("Patient Medical Summary")
19. Health Directives

The above classifications will be augmented with successive releases of WhoKnozMe to cover conditions and treatments under Psychiatry, Dentistry, Optometry, Audiology, Chiropractic, Naturopathy, etc.

All of the above personal health information is considered to be and will be treated as Personally Private.

5.3 *Users*

Users are Individuals who operate the WhoKnozMe Health Information Service on behalf of the Patient.

There are only two types of Users, viz.:

1. An **Owner-User**, simply referred to as an **Owner**, and
2. An **Owner's Representative User** simply referred to as a **Representative**.

An Owner-User must always be a natural person because they are actually the Patient. A Representative may be either a natural person or a corporation. Most Representatives will be natural persons. All Users must be known to CS4 (i.e. they were registered at some point prior to their definition as a User in the WhoKnozMe system). (In Ontario, the Representative is also known as the "**Substitute Decision Maker**").

There are many types of Representative Users depending on the form of Representation involved. For example:

- Infants and minor children with parents will normally be represented by one or more Parent(s)
- Orphaned children would be represented by Guardian(s)
- Adopted children would be represented by their Adoptive Parent(s)
- Dependent or incapable adults would be represented by person holding a Power-of-Attorney or a Health Representation Agreement
- Deceased patients would be represented by an Executor or an Administrator
- Married patients may be represented by their Spouse

In general, Representatives would have the same administrative and executive powers as an Owner. The Owner should seriously assess the personal characteristics of any Individual they would like to appoint as their Representative to assure themselves that this person would act in their best interest.

5.4 *Representatives for Children*

As described earlier a Representative for a child (i.e. a person under the age of majority – commonly 18 or 19 in Canada) at least one of the Parents or one or more Guardians. A Child's Representative is then their Substitute Decision Maker for personal health issues. A Child's Representative(s) can also be appointed by a Court of Law if necessary.

A Child's Representative has all the powers over the medical treatment of a Child Patient, including access to their Personal Health Information. When a Child is born or a Child is initially registered with CS4 the Parent(s) or Guardian(s) will inform the Registrar of Individuals of the event and, furthermore, provide a copy of the Child's Birth Certificate. The Registrar shall validate the certificate and register the Child and the relevant Representative Relationships (i.e. Parent or Guardian). The Registrar will then ensure that the Child's account User definition status is that of Owner's Representative once the Individual(s) identified as Parent(s) or Guardian(s) is (are) known to the Health Information System. The Registrar will then assist the Child's Representative in setting the password and other security controls to the Child's User account. The Child's Representative shall ensure that they and they alone know the precise values for the security controls.

If there is more than one Child's Representative nominated then the Registrar will ascertain if the Representatives are to act jointly or severally and so note on their respective Relationships. In any event, the Representatives shall have equal but separate access to the Child Patient's Health Information. CS4 will not be involved in any other way in the administration of the Child Patient's Health Information including participating in disputes or discussions with the Child's Representatives.

Should a Child's Representative be barred from serving as a Child's Representative, often by conditions imposed by a Court such as a Divorce Order or a Separation Order, or by reason of their own incapability then the Registrar shall be presented with a copy of the Order and asked to cancel the barred Representative's Relationship and substitute that with a newly nominated Child's Representative. The Registrar will assist the newly nominated Child's Representative in resetting the account password and other security controls.

5.5 *Representatives for Underage (or Adolescent) Users*

An underage (i.e. an Individual who is younger than the age of majority (either 18 or 19 years)) may wish to become the Owner-User of their own account and limit access to some or all internal details of the medical information in their account to their Parent(s) or Guardian(s). There are various provisions in applicable laws and regulations which make this overall process a matter of discretion and careful consideration for all parties involved.

CS4 has no immediate response or solution to this particular issue. We are currently reviewing it and believe that further discussions must involve individual provincial Privacy Commissioners.

5.6 *Representatives for Incapable Users*

As described earlier a Representative is often an Individual (or a number of Individuals) who the Patient (or Owner) has specifically nominated as their Substitute Decision Maker for personal health issues in the event of their becoming permanently or temporarily incapable. Representatives can also be appointed by a Court of Law if necessary.

A Representative has all the powers over the medical treatment of a Patient, including access to their Personal Health Information that the Patient would have had if they were capable. When a Patient becomes or is declared incapable the nominated Representative will inform the Registrar of Relationships that the Patient is incapable and provide this Registrar with proper copies of the necessary certificates such as a Power-of-Attorney or a Health Representation Agreement. The Registrar shall validate the certificate(s) and register the Representative Relationship. The Registrar will then change the User definition status from Owner to Owner's Representative once the Individual nominated as the Representative is known to the Health Information System. Following this the Registrar will assist the Representative in resetting the Password in the User Account and all other security controls in the vSDBox and enclosed Capsules and Sub-Capsules. The Representative shall ensure that they and they alone know the precise values for the security controls.

If there is more than one Representative nominated then the Registrar will ascertain if the Representatives are to act jointly or severally and so note on their respective Relationships. In any event, the Representatives shall have equal but separate access to the Patient's Health Information. CS4 will not be involved in any other way in the administration of the Patient's Health Information including participating in disputes or discussions with the Representatives.

6 Medical and Health Service Providers

Medical and Health Service Providers include the following categories.

6.1 *Medical Practitioners*

Practitioners are trained and licensed medical professionals who are or have been practicing members of professional colleges for:

- Acupuncturists
- Audiologists
- Chiropractors
- Dental Hygienists
- Dental Technicians
- Dentists
- Denturists
- Dietitians
- Hearing Instrument Practitioners
- Massage Therapists
- Massage Practitioners
- Medical Practitioners
- Midwives
- Naturopaths
- Naturopathic Doctors
- Osteopaths
- Osteopathic Practitioners
- Physicians
- Surgeons
- Specialist Doctors
- Psychiatrists
- Psychologists
- Nurse Practitioners
- Opticians and Optometrists
- Periodontists
- Pharmacists
- Podiatrists
- Registered Nurses (“RNs”)
- Licensed Practical Nurses (“LPNs”)

In general, Medical Practitioners provide various levels and categories of professional medical services to Patients. They are all authorized to bill their clients for services and materials provided and most are likely to be authorized to bill insurance providers (including provincial agencies) directly for their insurance-entitled clients.

Much of the overview information available for Medical Practitioners is public information. The vast bulk of information about their work is classified as Personally Private because it is commonly medical information about their clients. The Medical Professionals must carefully and continuously safeguard this information.

Medical professionals commonly work in hierarchical association with other medical professionals. Medical Professionals are commonly and publicly identified specifically by their Patients.

6.2 *Medical Assistants and Medical Office Assistants*

Medical Assistants and Medical Office Assistants are trained and certified individuals such as:

- Emergency Medical Technicians (“EMTs”)
- Emergency Medical Assistants (“EMAs”)
- Ambulance Attendants
- Medical Office Assistants (“MOAs”)

6.3 *Personalized Care Providers and Workers*

Personalized Care Providers and Care Service Worker trained and certified individuals such as:

- Personalized Care Providers are often Registered Nurses or Nurse Practitioners
- Personalized Care Workers
    - Certified Care Assistants (“CCAs”)

6.4 *Caregiver*

A friend or family members (Spouses, Parents, Children, Life Partners, Friends, etc.) voluntarily or by statute (parent, ward or guardian) undertakes the care of another individual. The Caregiver will most often **not** be certified or licensed in any manner but may be in a validated Relationship with the “Participant (patient) to Parent”.

6.5 *Care Team(s)*

Care Team is a group of Medical Practitioners, Health Service Providers, Care Service Providers or Caregivers acting in concert to support a Patient. While a Care Team, as a whole, may be granted sharing privileges to access a Patient’s Protected Health Information this may not be a good idea particularly if the non-professional members of the Care Team are not thoroughly versed in the protection of Personal Health Information.

7 Relationships

Relationships are the mechanisms by which Individuals are linked with other Individuals ("p2p"), Individuals are linked with Companies ("p2c"), Companies are linked with Individuals ("c2p") and Companies are linked with other Companies ("c2c") in the Health Information System.

There are quite a number of operating conditions associated with the definition of Relationships:

- ❖ Relationships are Directional. They link a "subject" (Individual or Company) to an "object" (Individual or Company).
  - ➢ A "Patient" (='subject') may be linked to a "Medical Practitioner" (='object') which is the equivalent of
    - ▪ The Patient has this Doctor, or
    - ▪ The Patient presents to this Doctor
- ❖ Relationships may generate implied Inverse Relationships. For example, the Practitioner listed immediately above may be presumed to be linked to the Patient listed above as:
  - ➢ The Doctor has this Patient in their List of Patients, or
  - ➢ The Doctor treats this Patient
- ❖ Relationships are "owned" by the 'subject'. In the case of the Patient defining the Relationship this preserves the overall patient-centricity of the Health Information System.
- ❖ Relationships are Contextual. This means that the roles and purpose of the Relationship are defined attributes (as in this Patient (which is one of the roles) attends (which is the purpose) the Doctor (which is the other role)).
- ❖ Relationships are Cumulative. The Patient may attend a General Practitioner and a number of Specialist Doctors (all at the same time).
- ❖ Relationships may be consensual, referential, mandated, etc. or expired.
- ❖ Some Relationships may need to be **certified and then validated by a Registrar**. (For example, the birth of a child would require a Birth Certificate to be provided to a Registrar so that a new account could be opened. The Representative(s) for the child would be presumed, initially, to be the parent(s) listed on the certificate.)

Representation by another Person or Company requires certification and validation and is described in the immediately following sections.

7.1 *Trusted Relationships*

"Trusted Relationships" are a form of Relationship through which a User can share their personal information with other Individuals whom they trust unconditionally. They trust that the other Individuals will use the information in the Owner's best interest and, furthermore, they trust the other individuals will maintain the confidentiality and integrity of it. (This latter phrase may appear to be a non sequitur but it is fundamental to one of the tenets for only using personal health information in the best interests of the Owner.)

Trusted Relationships will involve the creation of a Virtual Capsule in the Owner's vSDBox which is visible to the Individuals whom the User wishes to share their personal information with. Trusted Relationships should be created with a great deal of care.

8 Registrars and Registries

A Registrar is an employee and an operational officer of CS4. Their role is, principally, to act as the "Gatekeeper" for specific types of information entered into the WhoKnozMe database. As the Gatekeeper they need to verify and maintain the accuracy and validity of these specific items of information. The Privacy Classifications of this key data range from Public through Privileged then to Private and ultimately to Personally Private (see Section 3.1 Privacy Classifications of Data) and the Gatekeeper is strictly charged with maintaining, preserving and protecting said items of information.

As a continuing part of their duty the Registrars will maintain three specific Registries, namely:

1. **The Registry of Individuals**. This is a list of all validated Natural Persons who exist in the Health Information System. Natural Persons who have not, as yet, been validated are also stored in the list but are not accessible by any User other than the one who created the entry. The Registrar also has access to the non-validated Individual records. All Patients as well as all Healthcare Providers, all Medical Practitioners and all Representatives (who are Natural Persons) are included in this Registry.

2. **The Registry of Companies**. This is a list of all validated Companies which exist in the Health Information System. Companies which have not, as yet, been validated are also stored but are not accessible by any User other than the one who created the entry. The Registrar also has access to the non-validated Company records. All Companies, Organizations, Societies, Corporations, etc. as well as all incorporated Healthcare Providers and all Representatives (who are Companies) are included in this Registry.

3. **The Registry of Relationships**. This is a list of all validated Relationships which exist in the Health Information System. Relationships which have not, as yet, been validated are also stored in the list but are not accessible by any User other than the one who created the entry. The Registrar also has access to the non-validated Relationship records. All classes of Relationships are included in this Registry.

9 System Facilitators

System facilitators are individuals employed or contracted by CS4 at all levels who users may meet or correspond with. All such individuals will be vitally concerned with maintaining the Privacy and Security of your Personal Information stored within our Health Information System.

Please note – ***NONE of these System Facilitators*** have any ability or authority to directly access any of your Private or Personally Private Data stored within your virtual Safety Deposit Boxes.

9.1 *Corporate Board Members*

As with all Companies the Shareholders elect a Board of Directors to provide Corporate Governance and Guidance. There are currently four (4) Directors, one of whom serves as the Chair and one of whom serves as the Corporate Secretary. All of the current Directors are Founding Members of the Corporation. Normally the Board meets formally four times per year.

9.2 *Corporate Officers*

The Company currently has two Officers, a Chief Executive Officer ("CEO") and a Chief Technical Officer ("CTO"). At the moment the CEO also serves as the Chief Architect for the Company.

The Company plans to have at least three (3) other Officers upon expansion. The positions will be Chief Operations Officer ("COO"), CS4 Privacy Officer ("CPO") and CS4 Information Security Officer ("CISO").

10 Personal Information Privacy and Protection Policy ("PIP3") Overview

This privacy policy is designed for adults capable of consenting for their own use of the "Health Information Services" for their own purposes or for their right to use the "Health Information Services" on behalf of a person in their care.

The Health Information Service is a personal health and confidential information platform that lets you gather, edit, augment, store, and share health and other information online. With the Health Information Service, you can control your own health records and confidential information. You can also share your health and confidential information with family, friends, and health care practitioners, and have access to online health information management tools.

The Policy deals with, but is not limited to the following topics:

- Collection, Ownership and Protection of Your Personal Information;
- Protection of Your Confidential Information (Vault, vSDBox, Capsules, Object Level Security);
- Joint Responsibility for vigilance by the User in their User Account management and use of the multi-level validation by CS4 of Users;
- Messaging Services as a secure communication strategy; and
- A statement establishing absolute ownership, protection and use policy pertaining to Participant Identity and confidential information about the Participant[1].

The WhoKnozMe Health Information System exists in an electronic communication world that is increasingly under attack from others whether they be individual "hackers", criminal gangs or national and international cyberwarfare forces. Their methods are devious, nefarious, complex, continuous and conspiratorial. Their motives vary from monetary gain through to diversion of resources in a national sense.

Most governments try to combat so-called "hacking" by a variety of national legal sanctions. Unfortunately because electronic communications exist on an inter-national basis these national legal sanctions have little force and effect unless the persons carrying out the "hacking" activities can be arrested in a location directly subject to the national legislation or indirectly subject due to agreed international conventions.

In any event, health information systems providers such as CS4 need to implement policies, strategies and tactics to protect the privacy of the personal data we store for our clients. This document describes our policies for maintaining and protecting the privacy of your personal health information. We allude to some of our strategies and tactics that we implement to put our privacy policy into effect. A good part of this is accomplished through our system design and coding techniques. An essential aspect of information security is actually assessing and continually re-assessing the risks (i.e. threats and vulnerabilities) we face. Once risks are identified and assessed then we need to design and implement appropriate remedial measures.

10.1 *Privacy Protection and Data Security*

Because CS4 uses an internet-based portal process to provide you with access to your own health information we need to concentrate our privacy protection and security efforts on identifying attacks over the internet as they occur and then effectively countering them. Fortunately we have good management techniques for assessing the types of attacks we might expect because of publicly available documents prepared by various U.S. government departments. The core of these documents is based on Security Risk Assessment ("SRA") techniques. Recent work by the U.S. Department of Health and Human Services ("HHS") published in September 2016 provides us with an SRA tool specifically defined for the Health Information Industry.

10.2 *CS4 Rights, Interest & Access*

Collaborative Solutions and its Users have no rights or interest in any identity, contact or confidential information collected by the Health Information Service other than each User's own Personal Identity and the Personal Identity of those Individuals in their care. CS4 may only use the Personal Identities for the purposes of operating the Health Information Services and for Users to access the full facilities of the Health Information Services.

10.3 *Access to Directories (Registrar and Users)*

As part of the Directory Services, the Registrar has co-access with the Owner of each Individual user account (Persons and Companies) for only the purposes required to maintain the accuracy of the data defining a person's name and to maintain valid contact information (Address, Phone and eMail).

Further, use of the Directory Services by a User to find and/or create a relationship with another Individual is enforced by a Business Process requiring all Users to;

1. Establish sufficient knowledge about the Person (Last and (First or Goes By) Names), a valid email address and Postal Code to check the Directory for a match, or if not present:
2. Create a new entry for the Person by completing additional Contact information,
3. Create a relationship at a minimum, a Contact, and/or Emergency Contact, Care Team Member, Genetic or Family Member, and finally,
4. To protect the privacy of the Person listed in the Directory, an eMail is always sent to the Person informing them of the creation or use by stating the role the person plays in their life, invites them to assume their identity and become a User of the Health Information Services to fulfill the duties requested in the eMail.
5. If the Individual does not know or wishes to avoid the responsibilities they can contact the Sender to either expire or remove the relationship.

10.4 *Access to and Protection of Your Confidential Information*

The WhoKnozMe Health Information Service is designed to offer only a single entry point to your private information. Like a bank safety deposit box vault, everyone must have an identity registered with the bank. While this gets you into the vault, your Username and Password are the basic locking mechanism preventing entry to the virtual Safety Deposit Box (vSDBox). Additional locking and authentication mechanisms are available through a series of additional protection tactics including; PIN, Question & Answer, one-time-passwords, trusted devices, biometrics, entry attempt logs all designed to protect your confidential information.

The Health Information Service asks you to enter a username and password to sign-in to access your confidential information.

N.B. The first time you reach the Portal, you will only be able to view public information about the Health Information Service. To use the Health Information Service you must first "Register" yourself. The registration process will ask you to create a new identity unless you are going to assume an existing identity. (An existing Identity will have been created by the Registrar or a parent, spouse, friend, family member or even a Medical Practitioner. In all such cases, you would have been notified by an e-mail stating that you are in a relationship with that other person). To create a new account, you must provide minimal personal information such as your name, date of birth, e-mail address, postal code and country/region.

We will use the e-mail address you provide when you create your account to send you an e-mail requesting that you validate your e-mail address, to include in sharing invitations you send through the Health Information System is available to add to your account.

An account allows you to manage one or more health records, such as the ones you create for yourself and your family members. You choose what information to put in your records. Examples of the types of information you can store in a record include:

- fitness-related activities such as aerobic sessions
- measurements such as blood glucose and blood pressure
- discharge summaries from hospitalizations
- lab results
- medications
- health history

You can use the Health Information Service to enter a wide range of health information into a record. You can give others permission to view, add, modify, and/or hide information in a record. Please read those for information such as where and how the Program may use, store and transfer your information; what additional information it may collect; how you can review, edit and delete the information it holds; and other choices you may have

11 Sharing Your Personal Health Information

A key value of the Health Information Service is the ability for you to share your health information with people and services who can help you meet your health-related goals. For example, you can share health information from records you control:

- to co-manage the health of a family member
- to use products and services that can improve or monitor your health
- to consult with your health care provider
- to provide fitness information to coaches and trainers

You can share information in a health record you are custodian of with another person by sending a sharing invitation e-mail through the Health Information Service. If the person accepts your sharing invitation and has or creates a Health Information Service account, you have given him or her access to that information. You can specify how long they have access (representative access does not expire but, like all sharing access, it can be revoked at any time) and whether they can modify the information in the record.

You can also choose to grant sharing access to other persons, such as your spouse, for any record of which you are the Owner or Representative.

12 How We Use Your Personal Information

We use your personal information only to provide the Health Information Service. We do not use or disclose your information except as described in this policy document.

When a user sends WhoKnozMe a help request on help@whoknozme.com the user will often tell us their name and email address. Please do not tell WhoKnozMe staff clinical information about yourself or the person you represent. WhoKnozMe staff have no ability to access any clinical information in your Health Information Service records because we have no decryption keys and so no access.

In support of these uses, WhoKnozMe may use personal information:

- to provide you with important information about the Health Information Service, including critical updates and notifications
- to send you the WhoKnozMe e-mail newsletter if you opt-in
- to determine your age and location to help determine whether you qualify for an account.

WhoKnozMe may occasionally hire other companies to provide limited services on our behalf, such as answering customer questions about products and services. We give those companies only the personal information they need to deliver the service, such as an e-mail address. WhoKnozMe requires these companies to maintain the confidentiality of the information and prohibits them from using the information for any other purpose. WhoKnozMe does not share any clinical information with these third parties because we have no clinical information to share.

WhoKnozMe may access and/or disclose your personal information if such action is necessary to:

- comply with the law or legal process served on WhoKnozMe;
- protect and defend the rights or property of WhoKnozMe (including the enforcement of our agreements); or
- act in urgent circumstances to protect the personal safety and welfare of users of WhoKnozMe services or members of the public.

Personal information collected on the Health Information Service is stored and processed in Canada.

13 How We Use Aggregate Information

CS4 may use aggregated information from the Health Information Service to improve the quality of the Health Information Service and for marketing of the Health Information Service. This aggregated information is not associated with any individual account. CS4 does not and will not use your individual account and record information from the Health Information Service for marketing

The only information we are able to aggregate is usage data, e.g. for a particular period of time how many Users are using the system, how many messages are sent, how many test results are received, etc. CS4 has no access to the actual data; i.e. who the people are, what the content of their message is, or what the test result was.

14 Account Access and Controls

When you create an account with the WhoKnozMe Health Information Service we require a small amount of information such as your name, e-mail address, postal code and service credentials. We may request other optional information, but we will clearly indicate that such information is optional. You can review and update your account information. You can modify, add, or delete any optional account information by signing into your WhoKnozMe account and editing your account profile.

You can close your account at any time by signing into your WhoKnozMe account and editing your account profile. We wait 90 days before permanently deleting your account information in order to help avoid accidental or malicious removal of your personal health information.

15 Record Access and Controls

There are a number of ePHR access levels available. The Health Information Service allows a User to access multiple personal health records provided that the appropriate conditions and permissions have been provided. This feature enables, for example, family health managers to create and manage records for their dependent family members.

The subject of an ePHR is always the Individual "Patient". In general, the Patient is the "Owner" of the ePHR however unless the Owner is a capable

When you create a record, you become pro tem the Owner of that record. As an Owner, you decide what level of access to grant other users of the Health Information Service. The Health Information Service creates a fixed list of each access by Users, which the Health Information Service keeps as a full history of the record. You can view and update records you are custodian of and can examine the history of access and changes to those records.

16 Sharing Records with Other Users through the Health Information Service

The level of access you can grant as an Owner include:

- View-only access (time-limited access)
- View-and-modify access (time-limited access)
- Representative access (no time limit)

Access becomes active only when the recipient accepts the invitation.

Representative access is the highest level of access. A Representative can:

- Read the record
- Amend the record
- Revoke the access of anyone other than another Representative to a record,

17 Deleting Elemental Items in a Personal Health Record

You cannot directly delete any elemental item in a personal health record for which you are the Owner or the Representative.

If you believe that an elemental item is incorrect, inaccurate, out of date, irrelevant, incomplete or misleading then you can do the following:

- You can HIDE the elemental item but you will have to declare the reason for hiding it (as the value(s) or text was "incorrect", "inaccurate", "out of date", "irrelevant", "incomplete" or "misleading"), or
- You can AMEND the elemental item but you will have to declare the reason for amending it (as the value(s) or text was "incorrect", "inaccurate", "out of date", "irrelevant", "incomplete" or "misleading") and then make the necessary changes to the value(s) or text. In this case the original elemental item will be marked as "REPLACED" and will be treated as though it is hidden.

HIDDEN elemental items are thus not destroyed thus preserving the historical nature of your overall personal health record. Only the Owner or the Owner's Representative can review HIDDEN or the original REPLACED data. HIDDEN or REPLACED elemental data items are not sharable.

18 Deleting Personal Health Records

You cannot directly delete any personal health record for which you are the Owner or the Representative.

You may request that the Registrar terminates your WhoKnozMe subscription. On receipt of your written instruction the Registrar will Archive your Personal Health Record and all the attendant relationships in which you are involved as the 'subject'.

When we replace our servers we will erase the old equipment completely as part of ISO 27001 (Information Security Management Systems) compliance.

19 Security of your personal information

Collaborative Solutions is committed to protecting the security of your personal information. We use a variety of security technologies and procedures to help protect your personal information from unauthorized access, use, and disclosure. For example, we store the personal information you provide on computer servers with limited access that are located in controlled facilities.

Additionally:

- The Health Information Service stores all clinical data using encryption so that only you, and the people to whom you grant sharing access, are able to read your medical record.
- The Health Information Service sends all communications, except e-mail, using encryption (that is, via HTTPS)
- You can view a history of access and actions to any Personal Health Record of which you are a Representative
- E-mail messages are not encrypted.

Each message about a record includes:

1. The person's name
2. The fact that they have new clinical data
3. The type of clinical data they have, e.g. a new test result, a new message from a doctor

4. A link to log into our secure encrypted web site to review the new data (N.B. We do not include any clinical data in e-mail messages. The user must click on the link to review it).

20 Changes to this Policy

We may occasionally update this policy document. When we do, we will also update the Version data and revision level and the date in the footer of the document. For material changes to this policy document, we will notify you either by placing a prominent notice on the home page of the WhoKnozMe site or by sending you an e-mail notification message directly. We encourage you to review this policy document periodically to stay informed about how we are helping to protect the personal information we collect. Your continued use of the Health Information Service constitutes your agreement to this policy document and any updates. Please be aware that this policy document and any choices you make on the Health Information Service do not necessarily apply to personal information you may have provided to Collaborative Solutions in the context of other, separately operated, Collaborative Solutions products or services.

We also encourage you to provide feedback and comments about the Health Information Service using the Member Services link in the Health Information Services web page.

21 Contact Information

CS4 welcomes your comments regarding this policy document. If you have questions about this policy document or believe that we have not adhered to it, please contact us by using our Member Services (Services Request) form or by telephone at +1 (250) 590-5811.

22 Appendix A: *OECD Recommendations for Protection of Personal Data*

In 1980, in an effort to create a comprehensive data protection system throughout Europe, the Organization for Economic Cooperation and Development (“OECD”) issued its “Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data”.

The seven principles governing the OECD's recommendations for protection of personal data were:

1. Notice — data subjects should be given notice when their data is being collected;
2. Purpose — data should only be used for the purpose stated and not for any other purposes;
3. Consent — data should not be disclosed without the data subject's consent;
4. Security — collected data should be kept secure from any potential abuses;
5. Disclosure — data subjects should be informed as to who is collecting their data;
6. Access — data subjects should be allowed to access their data and make corrections to any inaccurate data; and
7. Accountability — data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

The OECD Guidelines, however, were nonbinding, and data privacy laws still varied widely across Europe. The United States, meanwhile, while endorsing the OECD's recommendations, did nothing to implement them within the United States. All seven principles were incorporated into the EU Data Protection Directive of 1995.

While the OECD Guidelines do not specifically address the specific personal health information privacy and data protection issues they did and still do provide the overall basis for personal information protection legislation throughout much of the world.

23 Appendix B: Definitions

The following definitions are used within the WhoKnozMe Health Information System. They are listed here in order of appearance, more or less, to provide clarity of meaning and purpose to you while you are navigating the system.

Individual: An Individual is a natural person known to the WhoKnozMe system. A new Individual will be created as the first step during the User Registration process. Registered and Licensed Users can create other new Individuals as required for family and relationship purposes. Only known Individuals can be referenced within Relationships. Individuals are "known" by their complete names and a minimum of home address information. An Individual is a basic data object within WhoKnozMe.

User: A User is an Individual who has been registered and licensed to use WhoKnozMe. A User license defines the level of services that they contracted for during their Registration Process. Users have to provide their full names and are differentiated by address (including a valid postal code) and a valid electronic notification contact (e-mail address or FAX number). A User is a basic functional object within WhoKnozMe. Users may have to provide additional demographic data about themselves during the Registration Process. A User will have at least one User Account and, depending on their License, access to specified ranges of services. Users with "family" licenses may create and define other Individuals as "Spouses", "Children", "Dependent Parents", etc. who will be attached to them in WhoKnozMe.

User Account: A User Account is the overall personal information storage facility for a User and their family members and the means by which the defined User can invoke the personal information management facilities of WhoKnozMe. At a minimum, access to a User Account requires submission of a Username and its current Password. Users may optionally define additional User Account access controls as they deem necessary.

Username: A Username is a unique coded identifier assigned by and to the User during the Registration Process. The Username is fixed throughout the life of the User Account.

Password: A Password is a coded identifier that you use to verify yourself to WhoKnozMe. Your Password should be at least 8 characters in length with a mixture of Upper and Lower Case characters, numbers and Special characters. Your Password should be changed often and particularly if you think someone else might know it. Keep your Password as confidential as you can because it is the weakest element of our security control. Passwords are maintained in an obscured manner in the database and cannot be decoded by CS4.

Virtual Safety Deposit Box: Each User will have at least one (1) virtual Safety Deposit Box ("vSDB" or "vSDBox") in the WhoKnozMe system to hold all their own Personal Health Information, and as many other virtual Safety Deposit Boxes ("vSDBox") as needed for each other person they are personally responsible for (e.g. dependent children, incapable parents, etc.). Each vSDBox can have its own independent security provisions and may only be entered by the Owner, or by a Person authorized by the Owner, who must satisfy the specific security conditions. Various types of Capsules containing messages, account details, relationships, etc. will exist within the individual vSDBox.

Custodian: Defined only in PHIPA (Ontario 2004) and HIA (Alberta 2000) and may be referred to as a health information custodian. A Custodian is an Individual or Organization who has custody or control of personal health information as a result of or in conjunction with their performing work. A Custodian is subject to specific rules and duties when dealing with personal health information. CS4 does not use the term Custodian as we do not believe that this term applies to us.

Information Manager: Defined only in HIA (Alberta 2000) and may be referred to as a health information manager. An Information Manager is appointed or contracted for specific information management services by a Custodian and is subject to the same specific rules and duties when dealing with personal health data as a Custodian. (N.B. CS4 considers our company "Collaborative Solutions" to be somewhat equivalent to the Alberta HIA definition of an "Information Manager".)

Collaborator: Collaborators are either contributors of Key Resources including licensed technology to the CS4 Multi-Function Platform or as an industry or technical specialist or consultant.

Associate or Business Associate or Representative: An Associate is defined in the Associates Program as part of the distributed sales and client services team engaging individual users or collections of individuals, participants or providers. The Associate is a professional corporation, association, cooperative or association with at least one Provider. Associates are assigned industry vertical or geographic territories. Associates earn fees for on-boarding and/or selling a subscription service. They also earn an annuity to support the User (Individual or Provider). They earn concierge service fees by acting a Personalized Care Provider. All parties are signatories to the PIP3.

Personalized Care Provider or Provider, Practitioner: A Provider is defined as licenced or certified personalized care provider or practitioner generally as a member or licensee of a medical or allied medical College or Professional Association. The applications used by the Provider are the LifeLine – eChart and Care@LogBook. Each application relies on the Patient having a LifeLine ePHRecord + digital LogBook and Treatment Planner. The Provider may assist the Patient in the creation and maintenance of their ePHRecord. Default User-Role is "Provider". All parties are signatories to the PIP3.

Personalized Care Worker or Worker: A Worker is defined as a certified personalized care worker reporting or managed by a Provider as defined above. The applications used by the Worker are the LifeLine Care@LogBook. Default User-Role is "Provider-Delegate". All parties are signatories to the PIP3.

Innovator: An Innovator is an application developer using the CS4 Multi-Functional Platform ("MFP) and Medical Information Framework ("MIF") and Mobile App Platform ("MAP") to create extensions or new applications. The MFP has the Patient and Provider clients, registration, security and protection framework and other commercial services plus common tools and services reachable from the MFP, application programming interface ("API"). The Innovator prices the service and CS4 shares in the revenue. The maintenance and support is negotiated between the Innovator and CS4. Default User-Role is "Admin-Innovator" with only access to service objects directly related to their application". All parties are signatories to the PIP3.

Substitute Decision Maker: [jm-l]

Emancipated Minor (p.16 OCR Guide to Privacy …) [jm-l]

24 Appendix C: Acronyms

Electronic Health Record (“EHR"): EHRs are insurer and facility-centric. They focus on medical institution (hospitals, clinics etc.) or hospitalist -physician-specific information and are configured to reflect the needs hospitals or larger clinics where and the medical services insurer.

Electronic Medical Record (“EMR”): EMRs are provider-centric. They focus on clinics or physician-specific information and are configured to reflect the needs of individual physicians or groups of physicians responsible for the direct care of a patient. [N.B. EMRs are never used within WhoKnozMe nor are they available from it.]

Electronic Protected Health Information (“ePHI” or “EPHI”)

PHR is a synonym for **ePHRecord** or **ePHR** (i.e. a patient-centric health record)

Electronic Personal Health Record (“ePHR” or “EPHR”): ePHRs are patient-centric and contain information from a broad range of health providers. An ePHR generally contains subsets of sharable information including cumulative patient profiles with current prescriptions, allergies and immunization history. It will have integrated information related to in-patient and out-patient encounters with the health care system. Information within the ePHR is not always accessed with each patient encounter, but is used when additional information is required during a patient visit. Laboratory, diagnostic imaging results, and other results are also found in the ePHR but are not necessarily delivered to a specific provider for review; i.e. information is reviewed via a "pull" decision on the part of the provider at the time the information is required.

Health Insurance Portability and Accountability Act (“HIPAA”)

Virtual Safety Deposit Box (“vSDB” or “vSDBox”): vSDBoxes are virtual containers of an Individual's ePHR. They are unique to the Individual and may have their own access controls (in addition to the usual access control of a User Account).

Patient Derived Data (“PDD”) – Patient Derived information such as personal observations and Home devices for BGM, BP, weight, etc.

Allied Medical Practitioner Derived Data (“AMPDD”) – Doctor derived data from an appointment, BP, weight, etc. observations, etc.

26 Appendix D: Applicable Canadian Legislation and Guidelines

An overview document entitled **"Fact Sheet – Privacy Legislation in Canada"** has been published by the Office of the Privacy Commissioner of Canada and is available at:

https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp

The following ACTS were consulted during the initial derivation of this Policy document:

Canada:

PA **Privacy Act** [R.S.C., 1985, c. P-21]

applies to federal government and federal government institutions.

http://laws-lois.justice.gc.ca/eng/acts/P-21/FullText.html

PIPEDA **Personal Information Protection and Electronic Documents Act**

applies to federally incorporated and federally regulated companies.

http://laws-lois.justice.gc.ca/eng/acts/P-8.6/

DPA **Digital Privacy Act** [S.C. 2015, c.32]

Contains inter alia significant amendments to the Personal Information and Electronic Documents Act

http://laws-lois.justice.gc.ca/eng/AnnualStatutes/2015%5F32/page-1.html

Alberta:

FIPPA **Freedom of Information and Protection of Privacy Act** [RSA 2000, Chapter F-25]

applies to the Alberta government and Alberta government institutions.

http://www.qp.alberta.ca/documents/Acts/F-25.pdf

PIPA **Personal Information and Protection Act** [S.A. 2003, Chapter P-6.5]

applies to Alberta companies and private organizations

http://www.qp.alberta.ca/documents/Acts/P06P5.pdf

HIA **Health Information Act** [R.S.A. 2000, Chapter H-5]

http://www.qp.alberta.ca/documents/Acts/H05.pdf

British Columbia:

PIPA **Personal Information and Protection Act** [SBC 2003] CHAPTER 63

applies to British Columbia companies and private organizations

http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

FIPPA **Freedom of Information and Protection of Privacy Act** [RSBC 1996] CHAPTER 165

applies to British Columbia government and public organizations.

http://www.bclaws.ca/Recon/document/ID/freeside/96165_00

E-Health **E-Health (Personal Health Information Access and Protection of Privacy) Act** [SBC 2008] CHAPTER 38 (also referred to as PHIOPPA)

http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_08038_01

Ontario:

FIPPA **Freedom of Information and Protection of Privacy Act** [R.S.O. 1990, c.F.31]

https://www.ontario.ca/laws/statute/90f31

PHIPA **Personal Health Information Protection Act** [S.O. 2004, c.3, Sched. A]

https://www.ontario.ca/laws/statute/04p03

The following GUIDES and GUIDELINES were consulted in the initial derivation of this Policy statement

Canada:

PIPEDA Personal Information Protection and Electronic Documents Act

https://www.priv.gc.ca/information/pub/guide_org_e.asp

DPA **Digital Privacy Act** [S.C. 2015, c.32] Significant amendments to the Personal Information and Electronic Documents Act

http://laws-lois.justice.gc.ca/eng/AnnualStatutes/2015%5F32/page-1.html

Alberta:

PIPA **Personal Information and Protection Act** [S.A. 2003, Chapter P-6.5]

HIA **HEALTH INFORMATION – A PERSONAL MATTER A Practical Guide to the Health Information Act**

https://www.oipc.ab.ca/media/383665/practical_guide_to_hia_aug2010.pdf

British Columbia:

PIPA **Personal Information and Protection Act** [SBC 2003] CHAPTER 63

http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

FIPPA **Freedom of Information and Protection of Privacy Act** [RSBC 1996] CHAPTPR 165

http://www.bclaws.ca/Recon/document/ID/freeside/96165_00

Ontario:

PHIPA **A Guide to the Personal Health Information Protection Act** December 2004

https://www.ipc.on.ca/wp-content/uploads/Resources/hguide-e.pdf

FOIPIPA **A Mini-Guide to the Freedom of Information and Personal Information Protection Act**

July 2014

https://www.ipc.on.ca/wp-content/uploads/Resources/provincial%20guide-e.pdf

27 Appendix E: "Privacy by Design"

"Privacy by Design" is a concept developed by Dr. Ann Cavoukian in the 1990s when she was the Information and Privacy Commissioner for the province of Ontario, Canada. As of the initial date for the development of this Policy document she has moved on to become the Executive Director of the Privacy and Big Data Institute at Ryerson University located in Toronto, Ontario, Canada.

"Privacy by Design" has become an internationally accepted as an essential component of fundamental privacy protection. "Privacy by Design" advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather privacy assurance must ideally become an organization's default mode of operation.

"Privacy by Design" means building privacy into the design, operation and management of a given system, business process or design specification; it is based on adherence with the 7 Foundational Principles as follows:

1. **Proactive not reactive – preventative not remedial**. Anticipate, identify, and prevent invasive events before they happen; this means taking action before the fact, not afterward.
2. **Lead with privacy as the default setting.** Ensure personal data is automatically protected in all IT systems or business practices, with no added action required by any individual.
3. **Embed privacy into design.** Privacy measures should not be add-ons, but fully integrated components of the system.
4. **Retain full functionality (positive-sum, not zero-sum).** Privacy by Design employs a "win-win" approach to all legitimate system design goals; that is, both privacy and security are important, and no unnecessary trade-offs need to be made to achieve both.
5. **Ensure end-to-end security.** Data lifecycle security means all data should be securely retained as needed and destroyed when no longer needed.
6. **Maintain visibility and transparency – keep it open**. Assure stakeholders that business practices and technologies are operating according to objectives and subject to independent verification.
7. **Respect user privacy – keep it user centric**. Keep things user-centric; individual privacy interests must be supported by strong privacy defaults, appropriate notice, and user-friendly options.

In short **"Privacy by Design"** is a (programming design and development) framework based on proactively embedding privacy into the design and operation of Information Technology systems, networked infrastructure, and business practices.

Ryerson University and Deloitte LLP have teamed up to provide a "Privacy by Design" compliance assessment and certification service.

Reference materials are available from: http://www.ryerson.ca/pbdi/index.html

28 Appendix F: “Security Risk Assessment”

The U.S. Government has published a number of texts on the subject of Security Risk Assessment.

The general approach on Security Risk Assessment for all U.S. Government funded agencies and organizations comes from "The National Institute of Standards and Technology ("NIST"), U.S. Department of Commerce":

- Guide for Conducting Risk Assessments, NIST Special Publication 800-30, September 2012
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

The specific approaches on Security Risk Assessment for Health Information Systems comes in three volumes from "The Office of the National Coordinator for Health Information Technology" [published in September 2016]:

- Security Risk Assessment (SRA) Tool – Administrative Safeguards / Physical Safeguards /Technical Safeguards can all obtained via downloads from:
  https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

The actual SRA Tool for Windows or iPads can be found in the above location.

29 Appendix G: “Privacy and Security of Electronic Health Information”

From "The Office of the National Coordinator for Health Information Technology":

- Guide to Privacy and Security of Electronic Health Information

  https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf