HealthIM Privacy Framework

Version 3.02

30 June 2020

HealthIM™

108 Ahrens Street West, Unit 3
Kitchener, Ontario, Canada
N2H 4C3

www.HealthIM.com

TABLE OF CONTENTS

1. OVERVIEW

HealthIM is committed to protecting the private data of its clients and the communities they serve. This document may serve as a reference for those exploring the suitability of adopting HealthIM from the perspective of a privacy impact assessment. Enclosed you will find a thorough examination of the policies, procedures, and safeguards that HealthIM employs to protect data and the privacy rights of its users and their clients.

1.1 EXECUTIVE SUMMARY

HealthIM's network architecture and encryption practices were designed to safeguard the rights of persons in crisis and to meet relevant municipal, provincial/state and federal standards. The platform is designed to improve the safety and outcomes of interactions with persons in crisis by supporting crisis responders. To achieve this, the system connects police, healthcare and community mental health agencies with prompt access to relevant information to supplement their experience and professional judgement.

Information is collected from persons in crisis, their friends and family, bystanders and based on the observations of the responder. Considerations are made to limit the collection of information to only that which is strictly necessary for responders and care providers to deliver effective, appropriate care to the person in crisis.

Information is used by and disclosed to police, healthcare, and community mental health agencies in order to improve the safety and delivery of care to persons in crisis. HealthIM is designed to minimize the potential for misuse of information and to limit the use, disclosure and retention of information to only what is required.

HealthIM has been designed for use in acute crisis situations where obtaining informed consent from persons in crisis may not be possible at the time of collection. A common finding of privacy impact assessments conducted on HealthIM concludes that personal information can be collected, used, disclosed and retained without consent, to eliminate or significantly reduce the risk of serious harm in emergency situations. In these situations, the acute needs of the person in crisis and the significant benefits to their interests provided by collection and disclosure of their information have been found to constitute grounds for implied consent. When the person in crisis is being referred to a non-acute partner agency (e.g., a community outreach organization), informed consent is required. HealthIM may be used by the user to track whether consent to disclose information was given. Safeguards to ensure consent is provided prior to disclosure of information are embedded in the HealthIM system.

Encryption, safeguards and network architecture are employed to protect data at rest and in transit in compliance with applicable legislation and industry standards. Information is collected in a standardized format based on an evidence based clinical risk screening instrument.

Policies and procedures to ensure that privacy and data security practices are respected at all times are overseen by a designated privacy officer, in fulfillment of obligations under applicable legislation and a commitment to accountability and responsible governance.

1.2 GUIDING PRINCIPLES

The HealthIM Privacy Framework was developed to comply with Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA) and comparable legislation. Compliance with the European Union's General Data Protection Regulation (GDPR) was also assessed in order to ensure HealthIM meets stringent privacy and data protection standards domestically as well as internationally. An audit of privacy and security practices and policies identified the following five principles to guide the approach to responsible data processing:

Responsible Collection of Data – A commitment to only collect data that is necessary to protect the safety and interests of persons in crisis and to improve the delivery of appropriate, effective care by professionals responding to mental health crises.

Responsible Use, Disclosure & Retention – A commitment to providing a system through which data is used and disclosed only for the legitimate purpose(s) for which it was collected, and that it is retained for no longer than necessary to fulfill those purposes.

Data Security – A commitment to meeting or exceeding industry standards for data security through advanced cryptography, secure network infrastructure and privacy by design.

Accountability & Governance – A commitment to ensuring compliance with all applicable privacy legislation and industry best practices, using the present framework as a guide and having designated accountable individuals to assume this responsibility.

Complete Transparency – A commitment to provide clients, prospective clients and other interested parties with a complete and detailed account of how HealthIM processes and protects data, as well as policies and procedures as they relate to the privacy rights of the client and the individual.

1.3 DEFINITIONS

This Privacy Framework employs the following definitions, as stated in PIPEDA:

Breach of Security Safeguards means the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards or from a failure to establish those safeguards**.**

Personal Information means information about an identifiable individual.

For the purposes of this document and as defined in GDPR:

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person [i.e. not a corporation].

Recipient (Receiver) means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Controller means a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of processing of personal data.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

For the purposes of this document and as defined by HealthIM:

The Client means the agency, group of agencies and/or organizations with whom HealthIM has secured a license agreement for the provision of software as a service (or who are pursuing a license agreement with HealthIM).

HealthIM Clients means other clients who are using an operational (or “live”) version of HealthIM software under license

Partner Agencies means agencies or organizations that the client and HealthIM have agreed may use HealthIM software under the same license agreement

Sensitive Information refers to:

1. the names, aliases, address, location of the incident and the phone number of the person in crisis,
2. de-escalation advice, triggers and contextual notes about the interaction, or
3. any of the aforementioned information alone or in combination

Person(s) in Crisis (PIC[s]) refers to an individual who peace officers or mental health professionals have reasonable grounds to believe to be experiencing a mental health crisis, by their own admission, as indicated by their observed behaviour, or as reported by a friend, family member, or other credible witness.

Referral means the disclosure of information recorded in HealthIM by an authorized user to a partner agency who is not involved in the acute response to the Person in Crisis, but who may provide support and care following the crisis response (e.g. community mental health agencies, outreach teams, social or case workers). This disclosure always requires informed consent be obtained from the Person in Crisis.

Authorized Users means professionals employed by a HealthIM client or partner agency who (1) have a mandate to provide care to Persons in Crisis and/or to respond to suspected or actual Mental Health Crises, (2) have been granted access to HealthIM by their agency and (3) have been trained how to use HealthIM for its intended purpose.

2. DATA COLLECTION

2.1 PURPOSE

Data is collected using HealthIM for the purpose of:

- Improving the safety and security of a person in crisis (PIC)
- Improving the safety and security of peace officers, crisis workers and health practitioners providing care to a person in crisis (PIC)
- Improving the quality of care delivered to a person in crisis (PIC)
- Supporting the development of evidence-based policies and procedures

These goals are treated as being mutually dependent; that is to say that no one goal is pursued without regard for the other goals. At no point does the use of any information improve the safety and security of professionals responding to mental health crises without also improving the safety and security of the PIC and improving the quality of care delivered and vice versa.

2.2 CONSENT TO SCREEN

Privacy Impact Assessments (PIAs) conducted by HealthIM clients and internal audits by HealthIM have determined that the system is intended to be used in emergency situations which require that the responder determine the most appropriate course of action for a PIC based on their unique needs and risk of harm.

In order to accurately and effectively determine the most appropriate response for the PIC, responders must collect personal information about the PIC. When possible this information shall be collected directly from the person to whom it relates, however for the purposes of law enforcement this information may be collected from friends, family, care givers, witnesses, or other existing police records where it exists and is deemed to be accurate by the responder collecting the information.

When possible the informed consent of the PIC should be sought by responders in order to collect that information, however in compelling circumstances affecting the health and safety of the individual, it may not be practical to seek informed consent. Applicable privacy legislation has been found to allow for collection of personal information without the knowledge or consent of the PIC if the collection is clearly in the interests of the individual and consent cannot be obtained in a timely manner. Through the lens of harm reduction, the collection of this information for the purpose of providing emergency mental health care is commonly found to be of great enough benefit to the PIC that the benefits resulting from collection of his/her personal information outweigh the potential for harm resulting from collection without informed consent.

While this is a common finding amongst all jurisdictions in which HealthIM currently operates, it is strongly recommended that any agency considering adopting HealthIM conduct a thorough PIA in order to ensure that the system's design is appropriate for use in the jurisdiction(s) in which it is intended to be used.

2.3 LIMITATION

HealthIM has been designed to collect only information which serves the purposes outlined in Section 2.1 in order to improve the safety, security and quality of care delivered to a PIC.

Fundamental to this principle is the use of separate versions of the BMHS as developed by interRAI; the BMHS-Police and the BMHS-General. The core versions must remain unchanged according to HealthIM's agreement with interRAI and agencies must use the version that is appropriate for their mandate. Other agency specific information may be collected along with the information contained in the screener as is appropriate (e.g., the PIC's Health Card Number may be collected by Canadian health care facilities when appropriate but shall not be collected by law enforcement agencies), but this additional information is also limited to what is necessary for the responder to fulfill their obligation to the PIC, as determined through a PIA.

The personal information that is collected is essential so that authorized parties may access associated records which pertain to the appropriate care of the PIC (warrants for examination by a psychiatrist, case history, medical history, etc.). Incident location, which is also considered sensitive information, provides vital context to others who may be involved in the care of the PIC (identifying areas the PIC frequents for outreach workers, areas that can trigger or exacerbate the PIC's anti-social behaviours and should be avoided as a condition of probation, etc.).

It is necessary for responders to record their observations about the PIC's behaviours and mental state at the time of the interaction through the digitized BMHS in order to determine the PIC's acute risk of harm to themselves, others, and their risk of failing to care for themselves. The notes section is designed to capture any information which informs the delivery of care to the PIC that was not captured in the afore-mentioned fields. The screener has been proven to be an effective and valid tool to support responders in their efforts to determine the most appropriate response to a PIC and communicate with the PIC's health care providers.

Sections relating to de-escalation tactics and triggers are included in HealthIM for the express purpose of informing any responder(s) who subsequently interact with the PIC of any strategies that may be employed to improve the safety, quality and outcomes of the interaction. The information that is intended to be recorded here satisfies the findings of numerous coroners' inquests which suggest that de-escalation tactics and known triggers should be made more readily available to responders in order to prevent escalation that may result in a critical incident.

Clerical information such as the dates and times at which particular events occurred are recorded to inform the care of the PIC (to track how long they have been held in custody, how long they have been waiting at hospital, which agencies they have been referred to for outreach, etc.). This ensures the accountability of those involved in providing appropriate care to the PIC (who was involved in the interaction, who obtained informed consent for a referral, etc.), and to evaluate the effectiveness of HealthIM as a tool for improving the quality of care delivered to PICs.

Case or incident numbers may only be entered in a valid format (as specified by the client) in order to reduce the chance of the record being associated with the wrong individual. Free text entry fields are also limited in favour of structured responses.

2.4 DATA COLLECTED

Personal Identifiers

When responding to a PIC, authorized HealthIM users record information which is directly related to the goals outlined above. Specifically, the system collects the PIC's names, reported gender, date of birth, aliases, most recent address, phone number, and the location of the incident. These categories meet the criteria for sensitive information and are processed accordingly. Note that some of this information is agency specific and as such not all of this information is collected by any one agency.

BMHS

To complete a HealthIM record, responders record their observations about the PIC's behaviour using a digitized version of the BMHS. The BMHS is a clinically validated tool which "is designed to document (1) indicators of disordered thought and (2) indicators of risk of harm to self or others" (interRAI User's Manual version 9.3). The screener is designed to capture and standardize responders' observations about PICs in clinical language and to provide structure to the assessment of the PIC's needs in order to better inform decisions relating to their care. This tool replaces the recording of unstructured, subjective information about the responder's interaction with a PIC (notes in police general occurrence reports, case notes for social workers, etc.). After the sensitive information is separated and encrypted, the completed BMHS is considered pseudonymized data which cannot be attributed to any individual or household

Contextual Notes

Following completion of the digitized BMHS, responders are able to record narrative or contextual notes about the encounter that may be relevant to others involved in providing care or support to the PIC. While HealthIM does not make recommendations about how users should use this section, these uses may include using the field to record the name and phone number of the PIC's case worker, or to explain the nature or content of observed hallucinations, delusions, or persistent ideations. Additional sections are provided to record any de-escalation tactics that had a positive impact on the responder's interaction with the PIC and to record any triggers which had a negative impact on the interaction. Because these fields may contain personally identifying data the contents of these fields are treated as sensitive information.

Responder Details

HealthIM collects personal information about the responder; specifically, their name and an identification number that may vary depending on configuration (badge number, HRMIS number, employee identification number, etc.).

Other data points collected in the course of a HealthIM record include:

- Organizational unit of the responder (shift, department, team, etc.)
- Date and time the interaction began
- Incident (case, occurrence, etc.) number
- Disposition / call outcome (not taken to hospital, voluntary transport, involuntary apprehension, apprehension under an existing order)
- Destination(s) (if PIC is transported to another site)
    - Date and time of arrival at the destination(s)
    - Date and time of departure from the destination(s)
    - Outcome of the interaction (admitted to care facility, not admitted, transferred to other agency, unknown)
- Referral(s) made or offered (if applicable)
    - The date and time at which the PIC either consented to having their information transmitted to another agency or declined the offer
- Date and time the BMHS was completed and when the responder ended the call

Again, note that some of this information is agency specific and as such only information that is relevant to the responding agency would be collected. Similar to the completed BMHS questionnaire, when this information is encrypted and stored separately from sensitive information these fields have been deemed to be pseudonymized data.

3. DATA USE, DISCLOSURE & RETENTION

3.1 PURPOSE

HealthIM facilitates the use of information collected by HealthIM Clients and their authorized employees to improve the delivery of appropriate, effective care to PICs. The use, disclosure and retention of information collected by HealthIM Clients is essential in order to achieve the stated purpose of collection.

3.2 USAGE

The use of information collected in a HealthIM record may vary depending on the interaction, however, in all cases the information is pseudonymized then transmitted from the authorized user's device to HealthIM's servers. This transmission of data is necessary in order to route the information to the appropriate partner agency or agencies, should any be selected. The transmission of data to the HealthIM servers is also necessary to facilitate search queries, analytics and to maintain audit logs. It is important to note that sensitive data exists on HealthIM servers exclusively in its encrypted form and by design cannot be decrypted until it is transmitted from the server to an authorized receiving device.

Information from HealthIM servers may be used by pre-set recipient agencies (as determined by HealthIM Clients during the implementation process) on a case-by-case basis. Case-by-case authorization to use information retained in HealthIM's servers is given by the employees of HealthIM Clients to their recipient agencies using the HealthIM software interface (e.g., a police officer may select a hospital site to receive information about an incoming patient). Any use by recipient agencies shall be consistent with the purpose of collection as identified by the HealthIM Client that is disclosing the information. Hospitals who receive a HealthIM record, for example, may use the personal information to help verify the PIC's identity in order to access their medical history. Records are tailored to emphasize the information which is most salient to care providers at the selected destination.

Recipient agencies are identified by the HealthIM Client during implementation and may include (but are not limited to) hospitals, detention centres, mental health crisis centres, mobile crisis response teams, community outreach or community mental health and addictions agencies. In order to use the information contained in a HealthIM record the agency must also have a mandate to provide care and protect the legitimate interest of PICs. The agency must also be approved as a partner agency by a HealthIM client and must agree to participate as a HealthIM receiving site. It is recommended that PIAs be conducted by recipient agencies as well as the HealthIM Client in order to determine whether the system's design is consistent with locally applicable legislation and agency policy and to determine whether it is necessary to obtain informed consent from a PIC in order for the receiving agency to use the information contained in a HealthIM record.

The contents of the BMHS, as a subcomponent of the HealthIM record, informs care planning at recipient agencies by providing a clinically valid measure of the PIC's risk profile and by providing indicators of the PIC's disordered thoughts as observed when the record was filled out. This information may be compared to the person's state as observed by employees at the recipient agency. Use of structured observations ensures that information communicated by responders to recipient agencies is complete and accurate.

Records include a history chart that displays dates and observed risk scores from prior HealthIM records, as well as highlighting whether the PIC was suspected of being intoxicated during those interactions. This brief history can be invaluable in establishing a "baseline" with which to compare the PIC's current risk profile and especially in determining the extent to which the risk profile can reasonably be expected to change for that PIC when they are intoxicated as opposed to sober (and vice versa).

Notes, de-escalation tactics, and known triggers are recorded by the employees of HealthIM Clients through their use of HealthIM to support the interaction between the PIC and front-line service providers at the recipient agency and to support communication between employees of the HealthIM Client and the recipient agency. This use is consistent for recipients at both transport destinations (e.g., a hospital emergency department) and referral destinations (e.g., a community mental health support service).

Clerical information contained in HealthIM records received at authorized sites are also used to inform decisions related to the care of the PIC. For example, the amount of time that a PIC has been held involuntarily may influence triage decisions in a hospital Emergency Department. This information may also be used to evaluate the effectiveness of transfer of care protocols within a community partnership (monitoring hospital wait times, community mental health agency referrals, involuntary apprehension rates, individual and organizational performance monitoring, etc.).

BMHS risk scores, known triggers and de-escalation advice are used to construct the aforementioned history chart on HealthIM records that can be accessed by other HealthIM clients within the same Province, State, Territory or regional equivalent if a BMHS record is completed for the same PIC. A number of coroners' inquests have found that a lack of access to de-escalation tactics, known triggers and associated information about vulnerable parties has been a common contributing factor leading to critical incidents. This functionality helps address the issue by incorporating as much directly applicable information as possible into the system's pre-response briefing.

Information collected through HealthIM is retained on Tier III Canadian servers in fulfillment of the contractual obligations between HealthIM and HealthIM Clients per the HealthIM License Agreement. Information retained on the HealthIM servers is used by HealthIM solely for the purpose of fulfilling its obligations to HealthIM Clients except where:

HealthIM is required to disclose pseudonymized data in an aggregate form to interRAI as per the HealthIM License agreement;

HealthIM may use pseudonymized data in aggregate form to improve its own products and services; and

HealthIM may use pseudonymized data in aggregate form to provide analysis to HealthIM Clients.

Disclosure of pseudonymized aggregate data to interRAI is required under the terms of HealthIM's license agreement to use the BMHS. This disclosure facilitates interRAI's use of aggregate BMHS data to continually improve the BMHS instrument. Aggregate data is used by HealthIM to evaluate, monitor and improve the delivery of service to its clients as well as to evaluate, monitor and improve the function of the software itself. In both cases this aggregate data is pseudonymized and cannot be reidentified by HealthIM or interRAI.

3.3 DISCLOSURE

Informed consent shall be obtained from the PIC prior to disclosure of information contained within HealthIM to partner agencies. Disclosure without consent shall only be made to partner agencies that provide acute care (e.g., a hospital emergency department) for law enforcement purposes and in situations that require disclosure without consent to eliminate or reduce significant risk of serious bodily harm.

Use of HealthIM's systems to disclose information relating to a PIC is commonly found to be substantially similar to existing procedures (typically an emergency responder disclosing information verbally to employees of the health care provider) with some additional benefits:

1. Access to HealthIM records is restricted to authorized users at the recipient partner agency that will be receiving the PIC (as determined by authorized users of the HealthIM Client). This access is granted temporarily and is determined at the time of collection by an authorized employee of the client. This secure process guarantees that only the partner agencies selected by the HealthIM client (from a pre-set list of partner agencies) may receive this information (a common flaw in communications by fax, which may sometimes be sent to the wrong destination).
2. Use of electronic communications eliminates the need for a lengthy verbal debrief which (in a public emergency department) may be overheard by third parties not involved in the PICs circle of care.
3. Use of electronic communications allows for comprehensive auditing of disclosure which would otherwise not be possible with verbal or paper communication of the information.

While digital communication cannot and should not fully replace the depth of verbal communication between employees of the HealthIM Client and the partner agencies, the transmission of a standardized summary of the PIC's behaviour (which has been screened to only include information relevant to the recipient partner agency) may be used to support transfer of care, the appropriate planning of care, and the safety of the PIC and his/her caregivers.

DISCLOSURE TO ACUTE CARE PROVIDERS

Information that is transmitted to partner agencies that are acute care providers (e.g., a hospital emergency department) is disclosed to authorized users within the patient's circle of care as identified to HealthIM during the implementation process. This typically includes (but is not limited to) emergency department triage staff, emergency department physicians, the emergency department charge nurse, the emergency department patient care coordinator, the ward clerk, mental health unit nurses and mental health unit psychiatrists.

Peace Officers and/or Crisis Workers will seek to receive the informed consent of the individual prior to disclosing the information to the above authorized users at the partner agency whenever possible. Peace Officers and/or Crisis Worker may disclose information without consent to authorized users within the patient's circle of care to reduce or eliminate a significant risk of harm to the patient or others and/or to provide those authorized users with the peace officers and/or crisis workers reasonable grounds to conduct an involuntary apprehension. This process is commonly found to be substantially similar to existing transfer of care protocols when conducting a PIA.

The disclosure of information to partner agencies that provide acute care is tracked within the HealthIM audit log, which includes the details of:

- The HealthIM Client's authorized user who is disclosing the information; and
- The authorized user(s) receiving the information at the partner agency

Separate audit logs are maintained for each partner agency and may be accessed at any time by designated staff members at each partner agency through HealthIM's web services (analytics.healthim.com).

DISCLOSURE TO NON-ACUTE SERVICES

Information transmitted to partner agencies that provide non-acute mental health support services (e.g., counselling services) shall be disclosed to authorized users only with the informed consent of the PIC to whom the information pertains. Consent is obtained directly from the PIC by an authorized user employed by the HealthIM Client. The consent is captured using a digital interface in HealthIM that allows the user to indicate whether a referral was "offered" or "not offered". Consent is captured separately for each partner agency. If the user selects "offered", a dialogue guiding that user through the process of collecting informed consent will be presented.

Authorized users shall brief the PIC using the contents of the dialogue pictured above. Upon selection of either "Consent Declined" or "Consent Received" HealthIM generates an entry in the audit log containing:

- a time stamp;
- a digital signature of the user who attempted to obtain consent; and
- the outcome (consent declined, or consent received)

If the PIC provides the authorized user with informed consent to disclose the information contained within HealthIM (including the information collected by the authorized user during the present interaction) a secure transmission is sent to the partner agency to whom the consent pertains.

3.4 DELETION OF RECORDS

Information stored on HealthIM servers shall be deleted upon request, or automatically after a period of time defined by the HealthIM Client. It is important to note, however, that the deletion of data impairs the system's ability to provide certain functions, such as the display of known triggers and de-escalation tactics from previous interactions. With this in mind, the client's policy and/or PIA may suggest retaining this information for a relatively longer period of time in order to ensure the full benefit of such functions are realized.

Local devices used to create, transmit and/or receive HealthIM records also retain the information contained in those records for a period of time before being automatically deleted from local storage. The time period prior to automatic deletion is determined during the implementation process and may be configured separately for each partner agency and the HealthIM Client.

Local retention of data is necessary to ensure continued operation of the system in the event that a network connection is not available. If connectivity is interrupted, local storage will allow authorized users to continue to make changes to their records (Wait times, leave call, etc.). Once a connection is established the system will automatically sync any new information to ensure records are accurate and complete.

3.5 LIMITATION

3.5.1. USE

Only authorized users expressly identified by the HealthIM Client and the Partner Agencies may access personally identifiable information contained within HealthIM. The specific policy regarding use of the information contained within HealthIM is to be defined by the HealthIM Client and its Partner Agencies. Though policy may vary between communities, they are substantially similar and typically include that:

> only users who require access to personally identifiable information as a function of providing services to PICs shall be designated as authorized users;
>
> authorized users shall only access personally identifiable information when required to provide service(s) consistent with the purpose of collection; and
>
> authorized users shall only access personally identifiable information pertaining to the PIC(s) to whom they are providing services;

Authorized users employed by the HealthIM Client may access any personally identifiable information collected by the HealthIM Client. Authorized users employed by a Partner Agency may only access information that has been expressly disclosed to their Partner Agency. Although HealthIM maintains a detailed audit log of each authorized user's use of the system (including accessing records) it is up to the HealthIM Client and the Partner Agencies to ensure their employees adhere to local privacy legislation.

HEALTHIM AND ITS EMPLOYEES DO NOT HAVE ANY ABILITY TO ACCESS PERSONALLY IDENTIFIABLE INFORMATION COLLECTED THROUGH USE OF THE HEALTHIM SYSTEM BY THE HEALTHIM CLIENT AND/OR PARTNER AGENCIES. Information stored on HealthIM servers is encrypted using asymmetric cryptography which HealthIM and its employees do not have the means to decrypt. Only authorized users identified by the HealthIM Client and the Partner Agencies have the means to decrypt personally identifiable information.

For the purpose of providing technical and/or training support to the HealthIM Client and/or Partner Agencies, authorized staff at HealthIM may access personally identifiable information of authorized users employed by the HealthIM Client who have interacted with the HealthIM system. This information includes:

the rank of the authorized user (police only);

the first and last name of the authorized user;

the badge number or employee ID of the authorized user;

the Platoon, Watch, or Shift of the authorized user (police only); and

the District, Division, or Detachment of the authorized user (police only);

3.5.2. DISCLOSURE

The HealthIM system restricts disclosure of information to any third parties except partner agencies identified by the HealthIM Client during the implementation process. Partner agencies have no ability to use the HealthIM system to disclose information to other third parties. Disclosure of personal information is strictly one-way from the HealthIM Client to the partner agencies.

HealthIM has implemented substantial security policies to ensure that only authorized users employed by a partner agency may be the recipient of information disclosed by the HealthIM Client. However, authorized users who have access to information collected through HealthIM may choose to disclose this information (at their discretion) by traditional means (verbally, digital and/or written communications). HealthIM claims no ability to prevent unauthorized disclosure of information by employees of the HealthIM Client and/or the partner agencies to any other individual or organization (either intentionally or accidentally) when using traditional means of communication.

At no point will HealthIM disclose personally identifiable information pertaining to an authorized user of the HealthIM Client or partner agency except where the authorized user has provided their express consent to HealthIM.

4. DATA SECURITY

4.1 ENCRYPTION & SAFEGUARDS

Respect for the privacy and security rights of PICs is both a fundamental goal and an embedded component of the HealthIM system. Privacy by design principles were employed in the development of the software to provide privacy by default to all data subjects (PICs).

To ensure the contents of the record is secure, HealthIM employs a combination of industry standard algorithms to protect the data at rest and in transit. Once the BMHS record is completed, the sensitive data is separated from the rest of the record prior to submission. This sensitive data package is then encrypted with AES-256 (Advanced Encryption Standard) using a randomly generated key. AES is specified in the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 197. This process allows for the encryption of an unbounded volume of data, but it is symmetric, meaning the same key encrypts and decrypts the data. One of the features of the HealthIM system is that the encrypted message can only be opened by the desired destinations. To achieve this, HealthIM employs asymmetric cryptography as well. HealthIM encrypts the AES encryption key data using RSA-4096 (Rivest-Shamir-Adleman) keypairs that are owned by each organization participating in the system. Since RSA encryption is asymmetric, HealthIM servers can retain the “public” key used to encrypt the data while only the organization intended to receive the information possesses the “private” key used to decrypt the data. These combined methods ensure the pseudonymization of data prior to being transmitted or stored, so that only the intended, authorized recipient is able to re-identify the data.

The private key necessary for decryption and re-identification of (RSA encrypted) sensitive data is generated by authorized HealthIM receiving sites during their installation of the software. Local generation of the private key ensures that neither HealthIM, nor any other entity apart from the receiving site has access to this key at any point. HealthIM recommends that a copy of this key file be kept separately as a backup to help prevent data loss.

Once encrypted, the record is then sent from the transmitting device to HealthIM servers and, if desired, from the servers to an authorized receiving device. All communications between HealthIM servers and HealthIM applications are completed over connections protected by TLS (Transport Layer Security). TLS is a group of cryptographic protocols used in online communications that allows two devices to agree on a one-time secure symmetric key that can be used to encrypt all messages between them for a given session. HealthIM maintains the necessary certificates used to facilitate TLS-protected traffic (TLS 1.2). This is the same industry standard protocol used by most secure websites to protect sensitive information and adds another layer of security to encrypted data while in transit.

Some functions of HealthIM, such as the safety briefing provided to responders interacting with a PIC who has previously been the subject of a HealthIM record, rely on the ability to link the PIC's past records with their identity using the Person Lookup function. In order to establish that these records are associated with the same individual, HealthIM employs a Secure Hashing Algorithm (SHA-256) as specified in NIST FIPS 180-4 to protect the identity of the individual. A series of hashed values are associated with the record based on the individuals name and birthdate information as part of the separation and encryption process. In addition to this, to increase security and prevent "rainbow table" style attacks on these hashes, each organization is assigned a unique salt string that is incorporated within the hash generation process. As such, the hash can only be generated by entering the same name and birthdate in the Person Lookup function by the service that created the record. This one-way search functionality, which is similar to what is used to protect passwords in online databases, enables the system to compare the outputs of a search (the hashes) to identify matches without having access to the initial inputs (the personal information).

In instances in which multiple clients are operating within a common jurisdiction, an encrypted copy of the PIC's record is sent from the agency who created it to other agencies in that same jurisdiction. Each of those agencies would then decrypt and re-hash the record using their unique hash key to create a copy of the identifiers that are accessible using only their authorized devices. This approach ensures that the information responders need in order to provide the most effective and appropriate response and care to the PIC is available to them when they need it, while allowing agencies who communicate with one another to seamlessly and securely collaborate. These records can also be traced back to the original created record in the case that the agency who generated the record wishes to delete it, thus respecting data ownership.

HealthIM software includes safeguards to help prevent source code tampering in addition to standard file system permissions. Checksums can be used to confirm validity of installations and source code downloads and all software is signed with standard code signing certificates that are renewed regularly.

The HealthIM server infrastructure is constantly monitored, and servers are equipped with automated alert systems to detect suspicious or unauthorized activity. Software and Security patches are tested and applied on a regular basis and penetration testing of the HealthIM system is conducted regularly as well.

These security protocols and safeguards are in compliance with FIPS 140-2 regulations, as well as Canada's Communication Security Establishment (CSE) standards for PROTECTED A and PROTECTED B information. Furthermore, these protocols and safeguards are sufficient to remain compliant beyond the increases suggested by the CSE for the year 2030.

4.2 ACCESS CONTROL

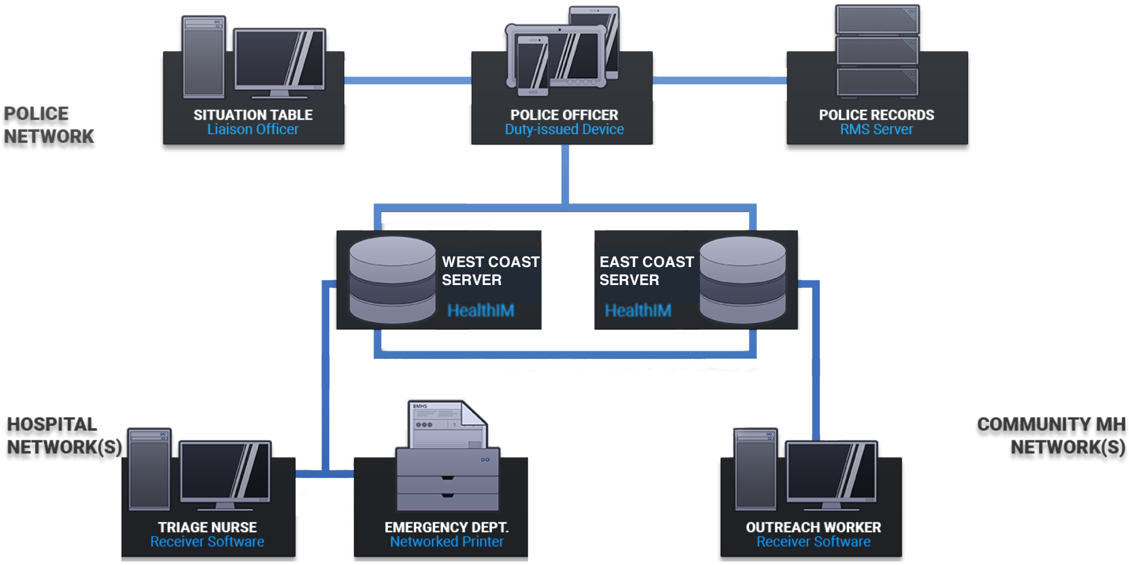
Data security is further enhanced by user access controls. HealthIM supports user authentication if necessary. However, if there are existing authentication mechanisms on the devices on which HealthIM is installed (like an existing Active Directory service) then clients typically do not need to log into the HealthIM software separately. This has been preferred to the requirement of having a separate log-in to the HealthIM software since users do not need to memorize a new password and administrators can continue to use existing user groups (along with their access and lock out requirements) without modification.

If HealthIM is to be installed on an open-access device, individual logins must be established on the servers to ensure that access to the software is limited to authorized and authenticated parties. Typically, clients do not require different user profiles to restrict access to the software since the base functions are fairly interdependent.

Access to the HealthIM Analytics site, which can be accessed through the client's preferred web browser, requires its own password and log-in. This access can be restricted, at the request of the client, to limit permissions. Default passwords are provided during the implementation of the system and are a minimum of 12 characters in length. Passwords can include alphanumeric, white space and special characters. The system permits users to change their passwords, but the aforementioned characteristics for length and character type remain requirements in order to ensure the strength of the password. Passwords are not displayed in logs and are stored in hashed form for verification. Default login delays and lockouts are in place to prevent password guessing and/or brute force attacks.

Access to any sensitive information is further controlled by the distribution of private keys. Since all sensitive information is encrypted using the process described in Section 4.1, only devices provisioned with the organization's private key are able to decrypt and view this information. During the implementation process, organization keys are distributed only to the set of devices identified by the organization.

4.3 DATA FLOW



Data is generated as responders complete risk assessments for a person in crisis. Upon completion of the report, a copy is stored locally to facilitate access in the near future and to allow responders to collect wait time information (if appropriate). Only one report is active on a responder's device at one time and is removed once the call is ended. The record is summarized as a PDF and written to a client-specified location to document the interaction via the standard file system or SFTP. If desired, a fielded XML document can also be written for use in records systems or other analytics systems. Agencies generating BMHS records typically pursue an automatic or semi-automatic process to connect these PDF or XML summaries with existing records (e.g. sync to RMS or EMR).

On submission, the de-identified BMHS responses plus the encrypted sensitive data bundle are sent to the servers. If the person in crisis is to be referred or transferred to a partner agency, an encrypted package will be made for that agency based on their public key registered with the server. The rest of the BMHS responses will be transmitted to that agency as well. A separate encrypted package is created using The Client's keys. This facilitates historical data searches for the service generating the report.

In a minority of encounters, if it is unsafe to complete the full BMHS assessment on scene, an "acute crisis alert" is transmitted to healthcare, notifying them of an incoming high-risk patient. Responders will complete the remainder of the BMHS assessment upon arrival at hospital, or when it is safe to do so, in order to ensure the full suite of Mental Health observations are updated. This update is then reflected in the receiving software.

4.4 SERVER INFRASTRUCTURE

HealthIM operates on two data centres in each country, which are located on opposite sides of the client's country of residence. The servers receive, transmit, and store identical copies of clients' data. This redundancy protects data and functionality even in the unlikely event of major catastrophes such as natural disasters.

In case of a failure at one site, the client application will operate normally using the other set of servers to maintain uptime with no loss of data. Both sites are individually capable of handling workload requirements from all HealthIM clients within their country of origin. When the off-line server recovers from the fault, all data obtained while the server was off-line will be synchronized from the operational server to ensure data redundancy is complete.

To comply with applicable privacy legislation and data sovereignty principles HealthIM has ensured that the servers meet the requirements for data residency within the Client's country. The servers are owned by companies headquartered within the same country as the data centre. Servers have also been vetted to ensure that they are compliant with all relevant legislation as it pertains to storing sensitive or protected information (e.g. PIPEDA, HIPAA).

The servers reside in data centres designed and constructed to Tier III standards as defined by the Uptime Institute. These locations have redundant and dual-powered servers, storage, network links and other IT components so that scheduled maintenance can be performed without interrupting service. The design and construction of these facilities allows for 99.982% uptime, meaning less than 2.6 hours of downtime per year and protection against utility outages for a minimum of 72 hours.

In more concrete terms this means multiple fibre optic lines from multiple telecommunications providers, power from two separate sub-stations, Uninterruptible Power Supply (UPS) batteries, three separate 1MW diesel generators and multiple HVAC and CRAC climate control systems. This infrastructure works together to ensure that even in the event of one system's failure, redundancy exists to accommodate the entire load of the data centre and maintain operation until that system is back online.

Data centres also have strong physical security measures including 24/7 security staff and VESDA smoke detectors coupled with double-interlock dry pipe fire suppression systems (to protect against fire while mitigating risk of flooding). Access points employ biometric authentication and have anti-tailgating systems. The server racks themselves have protections against unauthorized access. In addition to these physical mechanisms, all server drives support full disk encryption. Centres are also audited annually for certain physical compliances with respect to flood, fire, and earthquake protections.

5. ACCOUNTABILITY & GOVERNANCE

5.1 COMPLIANCE & IMPACT ASSESSMENTS

HealthIM strongly recommends that all agencies considering implementation with HealthIM conduct a PIA or local equivalent to ensure compliance with local privacy legislation. Threat Risk Assessments (TRAs) may also be completed at the discretion of the HealthIM Client. This document is designed to support and inform the completion of a PIA and/or TRA, and includes common findings from 29 other Canadian communities currently using HealthIM. Any outstanding questions may be directed to HealthIM's privacy officer.

PIAs conducted by current HealthIM clients have found the system to be acceptable and appropriate for use in Ontario, Manitoba, Saskatchewan, and British Columbia. HealthIM has also been the subject of a Federal ATIP PIA in addition to self-assessments conducted using the GDPR and PIPEDA self-assessment tools. While these assessments have consistently confirmed HealthIM's compliance with privacy and security best-practices, we acknowledge that each client and jurisdiction is unique. HealthIM welcomes further examination of the system and will actively assist in efforts to conduct a PIA or TRA.

5.2 COMMITMENT TO PRIVACY & SECURITY

HealthIM will support all reasonable requests from clients and prospective clients regarding validation and assessment of the privacy and security standards of the system. Previous implementations have included third party penetration testing, privacy impact assessments, threat risk assessments, and a federal algorithmic risk assessment. The reference materials included in this document are designed to support a PIA and/or other assessments. Any other requests or inquiries may be directed to the privacy officer whose contact information is listed below.

5.3 DATA PROTECTION & PRIVACY OFFICER

HealthIM has appointed a Privacy Officer to ensure that the organization is, and continues to be, compliant with privacy legislation as it applies. The Privacy Officer will address complaints, questions and inquiries from clients and the public and will ensure HealthIM staff act in accordance with internal privacy and security policies and standards.

Privacy Officer & CEO – Daniel Pearson-Hirdes
E-mail – danielph@healthim.com

5.4 INDIVIDUAL/CLIENT DATA ACCESS

All data created through use of HealthIM will remain the property of the agency who generated the data. The HealthIM Client may access this data at any time using the secure web portal and key files provided by HealthIM. Access to this web portal is tracked and included in audit logs that are available for download by the HealthIM Client at any time. Upon request HealthIM will provide the HealthIM Client with any or all data created by the HealthIM Client and its authorized users.

Due to the strict privacy and security requirements of the system, HealthIM and its staff are unable to access any personally identifiable information collected by the HealthIM Client. Any individual wishing to access personally identifiable information stored on HealthIM servers must request access directly through the HealthIM Client who collected the data. As a result, Freedom of Information requests relating to any information stored on HealthIM servers are the sole responsibility of the HealthIM Client.

The HealthIM Client may, at any time, request that any or all data created by their agency be permanently deleted from the HealthIM servers. Individuals seeking to have their personally identifiable information deleted from the HealthIM Servers must submit their request through the HealthIM Client who collected the data. The HealthIM client would then be responsible for verifying the request and instructing HealthIM to delete the data in question from the HealthIM Servers.

In all above cases the incident or case number may be used as an identifier for records that are to be deleted or accessed. These unique numbers may be used to identify the record to HealthIM staff without disclosing personally identifiable information contained within the record. This system ensures that HealthIM is able to provide the required technical and training support to the HealthIM Client without requiring access to any personally identifiable information.

HealthIM will respond to all requests pertaining to access or deletion of data within 30 days of receiving the request. In the case of a particularly complex request HealthIM may send a notice of extension along with the reasons for extending the time limit. In this case, the individual or client may also be entitled to make a formal complaint to the Privacy Commissioner of Canada.

5.5 COMPLAINT PROCESS

Individuals may contact HealthIM's Privacy Officer regarding any issues related to processing of their personal data, the nature and function of the software and/or the practices, protocols and security measures HealthIM employs to protect their data. The Privacy Officer is committed to providing thorough and transparent answers, advice and investigation when faced with a complaint.

HealthIM does not have the ability to access personally identifiable information collected by the HealthIM client. As a result, any complaints originating from individuals (excluding authorized users employed by the HealthIM Client and/or the partner agencies) regarding freedom of information requests or access to records will be directed to the HealthIM client. 24

Should an individual or organization be dissatisfied with the results of an investigation into their complaint or with the amount of time an investigation is taking they are entitled to lodge a formal complaint with the Privacy Commissioner of Canada under PIPEDA. HealthIM will cooperate fully with any investigation or audit initiated by the Privacy Commissioner.

5.6 DATA BREACH PROCEDURE

In the unlikely event of a data breach, HealthIM will notify clients as soon as possible after the organization determines that a breach has occurred. The risk of an attacker obtaining data is minimized by HealthIM's encryption and data security protocols. The storage of data in its pseudonymized form and the use of encryption protocols ensure that in the event of a breach, that data would not be accessible in a useable format. Any breach of HealthIM safeguards and security protocols (regardless of whether an attempt was made to access data) would be a significant event and as such all clients who may have been affected would be notified.

Additionally, HealthIM will report any breach that creates a real risk of significant harm to an individual or client to the relevant authority or authorities (e.g. Canada's Privacy Commissioner under PIPEDA).

In the case of a physical breach (e.g., an unauthorized user gained access to hardware maintained by the HealthIM Client) audit logs will identify what information was accessed, the user associated with the device, the IP address, and the time of access. The encryption and decryption keys for a given device can also be revoked at any time to prevent access to sensitive information in the case that a device is stolen. HealthIM will work with the HealthIM client to determine the severity of the breach and corrective actions as needed.

6. FREQUENTLY ASKED QUESTIONS

Question: Can HealthIM see any of the information on the servers?

Answer: HealthIM cannot see any personal information about PICs.

HealthIM can see pseudonymized records, aggregate statistics, individual BMHS answers and risk scores, and responder information (name, ID number).

Question: What is cryptographic hashing?

Answer: Cryptographic Hashing is a one-way function of encoding information. It is not encryption because it cannot be decrypted. Data is encoded into a hash string or digest. If an identical set of data is fed into the system, it would be encoded as an identical digest. A search could then be done to see if the new digest matches anything in the system. This happens without any decoding of the data.

Cryptographic hashing is most often used with passwords. A user enters their password and it is encoded. The next time that password is entered the digests are compared and if they are the same, the user is allowed into the system.

HealthIM uses this process to encode personal data instead of a password. When a match is found, it allows history data to be pulled out of the system for the record.

HealthIM uses Secure Hash Algorithm (SHA – 256), which is one of the strongest available.

Question: In what format is the record kept when encrypted?

Answer: As a text string. This is the most efficient way of storing the data. At the hospital, the receiver software stitches the text string into a PDF record once again.

Question: Why types of servers do you use?

Answer: The servers are Linux (Ubuntu), running Rails (Ruby), using a PostgreSQL database

Question: What are the minimum system requirements to run the software?

Answer:
- Windows 7 or higher / Android version 6.0 or higher / iOS version 11 or higher
- Screen resolution:
    - Static Terminal: 1024 x 768 or greater
    - Mobile: 480 x 800 or greater
- 250 MB disk space for the application
- Internet access to HealthIM’s two servers in the agency’s country

Question: Is any information stored on the devices? If so, for how long?

Answer: Yes. On the Client's reporting devices, one report at a time is kept on the device. Once transmitted to HealthIM's servers, that report is deleted. In an instance where connectivity to HealthIM's servers is not possible, it would be possible for multiple reports to be kept on one device. The instant connectivity was re-established, all completed reports would be sent to HealthIM's servers and deleted from the device.

For partner agencies, reports are kept on their devices for a configurable period of time. The default for this period is one week. HealthIM can adjust this period, at the request of the partner agency, if the partner agency wishes for reports to be kept for a greater or lesser period of time.

Question: Who has access to assessments in the HealthIM system? Can a responder view a PIC's history of assessments?

Answer: HealthIM staff have access to the analytics system to see pseudonymized records for client support.

If a Responder initiates a HealthIM record on a PIC who was previously the subject of another record they will be advised of the PIC's past observed risk scores and of their known triggers and de-escalation tactics from those previous records. This information is essential to the ability of responders to provide the most effective and appropriate response and care to the PIC.

Responders can also use the analytics system to see de-identified records for their entire service if they have been granted access by their administrator.

Question: Are records accessible by other HealthIM clients?

Answer: All services using the HealthIM system within the same jurisdiction will have access to a PIC's historical information if, in the initiation of a HealthIM record, they search for a PIC who has previously been the subject of at least one other HealthIM record.

The system is designed to prevent browsing or searching for individuals without a justifiable purpose. This information only becomes available to a responder after they enter the name and DOB of a PIC with whom they are interacting. If information generated by another HealthIM can help to better inform that interaction it is provided to the responder in order to improve the delivery of effective and appropriate response and care to the PIC.

Question: How does HealthIM deal with service specific Firewalls?

Answer: All traffic is routed over port 443 (HTTPS) to the two Canadian IP addresses. Specific IP address exemptions may be required if there is not a general whitelist of port 443 traffic. HealthIM would be happy to provide the IP address of the two Canadian Servers for this if needed.

Can HealthIM function over TCP/IP protocol networked environment?

Answer: Yes

Question: If your product will operate over a remote access connection, what is the minimum bandwidth required on such a link?

Answer: App data transfer is less than 500 kB per record download

Question: Has your application performance testing included different levels of network latency?

Answer: Yes, the application is capable of operating in a variety of network latencies and can recover from connection loss.

Question: Does your software have the ability to be distributed to workstations or updated via SCCM?

Answer: Yes.

Question: In what format is your product's installer?

Answer: The product installer is in a .exe format.

Question: Does the client application require a separate database for operation?

Answer: No. A local SQLite database file is used for storing local data, the drive, the interface, and download functions.

Question: What is the initial size of the database file?

Answer: Less than 1 MB.

Question: What is the estimated annual growth size of the database file?

Answer: Data storage is temporary so storage will not grow linearly over time. Should not exceed 50MB

Question: What are your customer support and technical support hours?

Answer: Customer Support: 9 am to 5 pm Monday to Friday
Technical Support: 24/7 with 24 hour response time during emergencies

Question: What is the schedule and client requirements for software updates?

Answer: Updates to HealthIM software may be deployed on a flexible timeline. When an update is available, HealthIM will inform the HealthIM Client of the new update including a change log and supporting training material (if required). Any software updates are backwards compatible. No daily maintenance required.

7. PIA REFERENCE MATERIALS

Flow of information
Information is collected by authorized users employed by the HealthIM client for the purpose of providing appropriate, effective care to persons experiencing a mental health crisis. This information is encrypted and transmitted from the authorized user's device to the HealthIM servers (located in the client's country of jurisdiction). If an authorized user determines it is necessary to disclose information to a partner agency to provide services consistent with the purpose of collection, the information is transmitted (in its encrypted format) to a dedicated receiving device at the partner agency equipped with HealthIM receiver software. The information is then decrypted and stitched into a useable format.

Who manages/accesses/uses the system?
The HealthIM client manages access to the system and dictates which of their employees and/or which partner agencies will be granted access to HealthIM software and/or the secure web portal. Access to the secure web portal is restricted by a username and password combination. Individual user profiles with configurable permission levels are available for the secure web portal. Access to the HealthIM screener software and HealthIM receiver software is typically secured using existing authentication processes employed by the HealthIM Client and/or partner agencies (e.g, two-factor authentication, an existing username and password at a nursing station, etc.). If the existing security protocols on the HealthIM Client and/or partner agency devices is not sufficient, additional user authentication controls (a username and password) may be enabled in the software itself.

Linkages to other systems
Automated or semi-automated synchronization with records management software or electronic medical records software can be established at the client's request. This typically involves the export of a PDF or fielded XML document from HealthIM which can then be appended or imported to an existing record. This synchronization is a one-way process.

Potential future enhancements
No significant changes to the system are anticipated in the foreseeable future. Patches and updates may be deployed to fix bugs and enhance user experience, but core features are expected to remain unchanged.

Potential future uses of information
No changes to the use of information are expected in the foreseeable future, since the purpose of the system is narrow and well defined by clients' mandate from the public sector and from legislation.

Authority for the Collection, Use and Disclosure of Information

Mental health responders use HealthIM to provide more effective and appropriate care to persons experiencing a mental health crisis. Information collected with HealthIM is necessary to improve the safety, security and outcomes of mental health crisis situations for the person in crisis, emergency first responders and health care providers. Information is disclosed (in an emergency situation, to reduce or prevent the risk of serious harm) to acute care providers within the PICs circle of care, or with the informed consent of the person in crisis to mental health support services in their communities.

Decision-making and approval process

A standardized set of data is collected at the beginning of interactions between authorized users (employed by the HealthIM Client) and a person in crisis. HealthIM features three algorithms (developed and clinically validated by interRAI™) that utilize the standardized data collected to provide the user with feedback regarding the person in crisis' risk of harm. The outputs of these three algorithms are represented in three scales of 1 (low) to 10 (high), and are calculated using data from the present interaction only. Information from existing records is not used in the calculation of the algorithm scores. This information (in conjunction with the responder's professional judgement and all other information available to him/her) may be used to support decisions regarding appropriate outcomes for the interaction (e.g., referral to support services, involuntary apprehension, etc.)

Source and accuracy

Whenever possible the information collected through HealthIM is obtained from the person in crisis directly. Information sources may also include family, caregivers, friends, witnesses, existing records and the responder's own observations. The information collected follows a standardized format (the interRAI™ Brief Mental Health Screener) which (in its digitized form) includes error/logic checking to ensure data is accurate and complete. The system also features a flexible search and editing system allowing users to locate and update existing records to ensure information retained is accurate.

Notification statements

Notification of what information is being collected, how it will be used and to whom it will be disclosed should be provided verbally by authorized users whenever possible. In crisis situations involving acute risk of harm to self or others, it may not be practical for authorized users to provide notification. If it is impractical to provide notification at the time of collection, authorized users are encouraged to provide the person in crisis with notification when it is safe to do so.

Access Rights for Individuals

HealthIM clients retain access to all data generated by their organization. This data is accessible only to authorized users of the HealthIM Client (unless expressly disclosed by the HealthIM Client to an authorized user at a partner agency). Data may be accessed by authorized users via the HealthIM screener (HealthIM Client), the HealthIM receiver (partner agencies) and/or the secure web portal (HealthIM Client). Only personnel expressly authorized by the HealthIM Client may access the secure web portal. These authorized users are equipped with a username, password, and encryption key to facilitate access. HEALTHIM AND ITS EMPLOYEES DO NOT HAVE ANY ABILITY TO ACCESS PERSONALLY IDENTIFIABLE INFORMATION COLLECTED THROUGH USE OF THE HEALTHIM SYSTEM BY THE HEALTHIM CLIENT AND/OR PARTNER AGENCIES. In order to provide training / support to the HealthIM Client, authorized staff of HealthIM may access pseudonymized data within the secure web portal. Access by HealthIM staff is restricted using a username and password. HealthIM maintains an audit log summarizing all access to information retained on HealthIM Servers by all users.

Correction process

Authorized users of the HealthIM Client may access the HealthIM secure web portal to update existing records. The secure web portal includes a “record editor” feature that allows authorized users to make changes to information contained within a HealthIM record (e.g., to update a phone number that has recently changed). This feature is only accessible by authorized users of the HealthIM Client that also have access to the HealthIM Client’s private key (used to encrypt the record during creation). This ensures that only authorized users of the HealthIM Client may alter data within existing records.

Privacy & Security Measures

The HealthIM application works with existing user authentication procedures on the device if they are available. Separate user accounts can be generated if use of existing user authentication is not possible. The secure web portal can be accessed by those that have been authorized by the HealthIM client. Different user profiles (with different levels of access if desired) will be provided to track and limit access.

All collection, use, disclosure and retention of information through HealthIM is electronic, wireless and encrypted. The system employs AES-256 and RSA-4096 encryption to protect data from its generation to decryption, TLS v1.2 to provide additional security in transit and SHA-256 is used to generate hashed identifiers to link records belonging to the same individual without exposing any identifying information.

System Audit

HealthIM maintains a complete audit log including all instances where data is collected, disclosed, accessed and/or modified. The audit log is accessible to authorized users of the HealthIM Client and Partner Agencies at any time via the HealthIM secure web portal. Audit logs for each agency are maintained separately to ensure that identifiable information contained within each audit log (e.g., username, employee ID) is not disclosed authorized users of another agency.

Location of information

All records are stored in two Tier III certified data centres located in geographically redundant locations within the client's country of jurisdiction. Records may also be maintained by HealthIM clients and partner agencies, usually in PDF or XML (electronic format) although this maintenance is external to HealthIM and varies depending on client and partner procedures and policies.

Data Flow and Provincial / State Boundaries

HealthIM maintains two data centres within each country to provide geographic redundancy to all data retained on HealthIM servers. As a result, information collected by authorized users will be routed through both data centres simultaneously. Dependant on the location of the HealthIM Client, data may be required to flow across provincial (if the HealthIM Client is Canadian) or state (if the HealthIM Client is American) boundaries. Data centres are locally owned and operated within each country to ensure data does not flow across international borders. UNDER NO CIRCUMSTANCES WILL HEALTHIM INFRASTRUCTURE ROUTE INFORMATION COLLECTED BY A HEALTHIM CLIENT OUTSIDE THE COUNTRY OF ORIGIN.

Outside the province/state

Information will flow beyond province/state (or equivalent region) boundaries, since the geographic redundancy of duplicate servers is an essential part of providing secure, reliable service to HealthIM clients. Information will at no point, however, leave the federal jurisdiction of the client, and the companies operating the servers on which data is stored are owned by entities registered in that same country in order to maintain data sovereignty.

Retention & Destruction

Data is retained in an encrypted format on HealthIM servers, and temporarily on duty issued devices owned by the HealthIM Client and/or partner agencies. The HealthIM receiver features a built-in data deletion period with a default of 7 days. Upon request from the HealthIM Client, HealthIM shall delete some or all data retained on the HealthIM servers. The HealthIM Client and partner agencies are responsible for destruction of any HealthIM records that may be stored on internal record keeping systems (e.g., Records Management System, Electronic Medical Records).

CATEGORIES OF IDENTIFIABLE INFORMATION COLLECTED

COLLECTION			
CATEGORY	**TYPES**	**SOURCE**	**PURPOSE**
Contact Information	Name Address Telephone Number	Individual (Preferred) Family/Caregivers Friends/acquaintances	To verify the PIC's identity To maintain contact in order to provide support services To reinstate previous records
Individual Information	Age Gender	Individual (Preferred) Family/Caregivers Friends/acquaintances	To verify the PIC's identity For research and analysis purposes

USE		
CATEGORY	**TYPES**	**USE AND JUSTIFICATION**
Contact Information	Name Address Telephone Number	May be used to verify identity at transport destination or to contact the PIC in order to provide follow up support or care
Individual Information	Age Gender	Used to verify identity at transport destinations (in comparison with existing records) or during follow up/outreach programs Used for research and analysis to help evaluate and inform mental health crisis response policy

DISCLOSURE			
CATEGORY	**TYPES**	**TO WHOM & FOR WHAT PURPOSE**	**METHOD OF TRANSFER**
Contact Information	Name Address Telephone Number	Circle of care at acute Healthcare sites if acute care is necessary Community Mental Health Organizations to provide follow up outreach/support	Encrypted wireless transmission from HealthIM servers to dedicated receiving devices
Individual Information	Age Gender	Circle of care at acute Healthcare sites if acute care is necessary Community Mental Health Organizations to provide follow up outreach/support	Encrypted wireless transmission from HealthIM servers to dedicated receiving devices

8. REFERENCES

32nd Parliament of Canada, Bill C-43 (1983). *Privacy Act*. R.S.C. 1985, c. P-21

36th Parliament of Canada, Bill C-6 (2000). *Personal Information Protection and Electronic Documents Act (PIPEDA).* S.C. 2000, c.5

Barker, E., Chen, L., Roginsky, A., et al. (2019). *NIST Special Publication 800-56b Revision 2: Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography*. U.S. Department of Commerce, National Institute of Standards and Technology.

Communications Security Establishment of Canada (2016). *Cryptographic Algorithms for Unclassified, Protected A, And Protected B Information.*

European Parliament, & Council of the European Union (2016). *General Data Protection Regulation (GDPR).*

Hirdes, J.P., Hoffman, R, Brown, G.P. et al. (2015). *interRAI Brief Mental Health Screener (BMHS) Assessment Form and User's Manual.* Version 9.3.0, ISBN 978-1-62255-036-4

U.S. Department of Commerce, National Institute of Standards and Technology (2001). *Federal Information Processing Standards (FIPS) Publication 140-2: Security Requirements for Cryptographic Modules.*

U.S. Department of Commerce, National Institute of Standards and Technology (2001). *Federal Information Processing Standards (FIPS) Publication 197: Advanced Encryption Standard (AES).*

U.S. Department of Commerce, National Institute of Standards and Technology (2015). *Federal Information Processing Standards (FIPS) Publication 180-4: Secure Hash Standard (SHS).*