Green Cross Health
Telehealth Services –
Privacy Impact Assessment Report

June 2020

Privacy Impact Assessment Report – Contents

1. Purpose

Green Cross Health (GXH) is currently in the process of introducing a new **Telehealth Policy and Procedure** for its medical centres.

Telehealth has become an important modality for assisting health practitioners to provide safe, quality health care, improve health equity and increase service efficiency. Virtual consults supplement rather than replace in person care and is in context to the patient ability and capability for virtual and their life circumstances.

Telehealth is defined by the National Health IT Board as "the use of information and communication technologies to deliver healthcare when patients and care providers are not in the same physical location".

The term telehealth in our context refers to the use of any information and communication technologies we use to engage with and care for our patients.

Currently GXH's medical centres are increasingly using telehealth for varying situations from triaging patients for Covid-19, providing video and phone consultations and helping patients manage long term conditions. Virtual consultation have started occurring as a common mode of service delivery since mid-March 2020 as a direct result of the COVID-19 pandemic and related Government Alert Level 4 lockdown.

Accordingly, this Privacy Impact Assessment (PIA) will review any related privacy implications, and proposed risk mitigation, as part of the roll out of this new service mode, with a particular focus on virtual consultations between health practitioners and patients.

2. Scope of the PIA

2.1Scope

This PIA focuses on GXH's medical centres only, with regards to the delivery of telehealth between health practitioners and patients.

2.2The process

This PIA was developed by the National Clinical Services Manager, with assistance from a health legal privacy specialist. The GXH Privacy Policy, related Medical Centre Privacy Policy, and new Telehealth Policy and Procedure documents were reviewed and are referenced as part of this PIA process.

3. Personal information

Generally, the personal information involved in telehealth services is the same personal and health information as currently collected, stored, used and shared within the medical centres as part of the overall delivery of in-person health services to patients.

The introduction of telehealth services means that patient personal information will now be collected and transferred between the health practitioner and patient via a different mode (ie virtual consultations – via video or phone).

This mode of delivery means that personal information may be recorded in a different way (eg where the health practitioner and/or patient records the consult), and also means that the information is being transferred in a different way via technology which may sometimes create technical challenges in respect of that personal information.

Importantly, the environment in which the virtual consultations are occurring is different to in-person consultations, with both parties (health practitioner and patient) being in different locations. This means that there are news risks arising in respect of how privacy is managed in this context.

4. Privacy assessment

The following table sets out the information privacy principles in the Privacy Act, and the relevant framework that GXH must consider, alongside the proposed new practice. This assists in identifying where they may be privacy implications arising.

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment
1	Principle 1 - Purpose of the collection of personal information Only collect personal information if you really need it	Generally, the purpose for collecting patient personal information for the delivery of telehealth services (ie virtual consultations) is the same as for in-person consultations (ie to ensure appropriate health services and treatment can be provided). Differences are: • A difference to in-person consults is that where the person is unknown to the HP, their identity must first be confirmed and verified. In the centre, this would usually be done at reception by administrative staff. • Additional personal information will be collected about the individual's technology set up and location. • In a telephone consult additional questions may be asked due to the unavailability of facial and body language queues.	Needs consideration due to new additional purposes for collecting personal info	1

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment
2	Principle 2 – Source of personal information Get it directly from the people concerned wherever possible	Generally, the source of personal information is the patient directly (similar to in-person consults). In circumstances where the patient is unknown to the provider, information may be collected from a shared care record (eg Your Health Summary, HealthOne). Access will require patient consent.	Needs consideration due to possible additional means for collecting personal info	2
3	Principle 3 – Collection of information from subject Tell them what information you are collecting, what you're going to do with it, whether it's voluntary, and the consequences if they don't provide it.	Health practitioners will follow a new template checklist and form which sets out the proposed process for virtual consultations, including the gathering and use of personal information for the purpose of health service delivery and treatment. Virtual consultations will generally not be recorded – but they may be in exceptional circumstances (when the parties agree). The health practitioner should ensure at the beginning that the patient is not intending to record a virtual consultation. Where a patient (or family member or other support person) indicates that they wish to do so, the health practitioner can determine in the circumstances whether this is acceptable or not.	Needs consideration (new form outlining process)	3
4	Principle 4 – Manner of collection of personal information Be fair and not overly intrusive in how you collect the information	The manner of collecting personal information prior to and during a virtual consultation is typically via speaking with the person directly (similar to in-person consults).	Complies (no change to current practice for in-person consults)	N/A

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment
5	Principle 5 – Storage and security of personal information Take care of it once you've got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse.	Type of technology used is key – eg encryption, and whether or not the technology stores information as it is transferred. GXH intends to recommend safe technology to be used by the medical centres (eg Doxy Me). Location is key here. It depends on where the patient is, and also where the health practitioner is based. Both parties need to ensure that privacy is protected in that location. Where the HP is based outside of the medical centre (eg at home), it will depend on how they gather and use the patient's personal information as part of the telehealth service. Recordings – what happens if the patient or a family member or other support person records the consult? Policy will be implemented setting out GXH expectations. Training will be provided for staff.	Needs consideration and further planning	4 5 6
6	Principle 6 – Access to personal information People can see their personal information if they want to	No change to current in-person practice Virtual health service will enable open notes which would be an enhancement.	Complies (no change)	
7	Principle 7 – Correction of personal information They can correct it if it's wrong, or have a statement of correction attached	No change to current in-person practice	Complies (no change)	

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment
8	Principle 8 – Accuracy etc. of personal information to be checked before use Make sure personal information is correct, relevant and up to date before you use it	Is there a possible issue here in terms of when the HP may not hear the patient's response or understand correctly what they have told them (eg due to quality of technology mode/set up)?	Needs consideration	7
9	Principle 9 – Not to keep personal information for longer than necessary Get rid of it once you're done with it	No change to current in-person practice	Complies (no change)	N/A
10	Principle 10 – Limits on use of personal information Use it for the purpose you collected it for, unless one of the exceptions applies	No change to current in-person practice	Complies (no change)	N/A
11	Principle 11 – Limits on disclosure of personal information Only disclose it if you've got a good reason, unless one of the exceptions applies	Issue arising where the HP wants to discuss a matter with a patient but there are other people in attendance. For in-person consults, those other people would be asked to leave the room and wait in the waiting room. What will happen for virtual consults?	Needs consideration	8
12	Principle 12 – Unique identifiers Only assign unique identifiers where permitted	No change to current in-person practice	Complies (no change)	N/A

5. Risk assessment

This section further describes the privacy risks identified through the PIA process and the related risk assessment.

Ref	Privacy Risk	Risk Assessment (Low / Medium / High – based on chance of occurring and severity of impact)
R1	Purpose of Collection – new info being collected (identity verification; and technology/location details)	High (identity verification) Low (technology/ location details)
R2	Source of personal information- consent to access shared care records when available	Low
R3	Collection of Info process – ensuring person appropriately informed at beginning	Medium/ High
R4	Storage and Security – ensuring type of technology used for virtual consults is secure and encrypted	High
R5	Storage and Security – ensuring location of patient and HP respectively protects the parties' privacy	High
R6	Storage and Security – recordings (ensuring patient or family members or others in support do not record consults without HP knowledge/consent)	Medium/ High
R7	Accuracy – quality of technology may affect accuracy of personal information collected and relied on	Medium
R8	Disclosure – other people in attendance during virtual consults – how to protect patient confidentiality and ensure one-to-one discussions where considered necessary	Medium

6. Recommendations to minimise impact on privacy

Ref	Recommendation
R1	Purpose of Collection – new info being collected (identity verification; and technology/location details): Identity verification by reception using 3 patient identifier verification if patient is enrolled and known to the centre and/or confirmation of ID (driver's licence, passport or birth certificate) for casual patients prior to booking. Health practitioner identify verification using 3 patient identifiers, prompt build into Telehealth Advanced Form as a required field.
R2	Source of personal information- consent to access shared care records when available Where there is access to a shared care record (eg HealthOne, Your Health Summary) that may benefit continuity of care, the provider will ask for patient consent to access and this will be documented on the Telehealth Advanced Form
R3	Collection of Info process – ensuring person appropriately informed at beginning: Informed Consent expectations outlined in Telehealth Policy and Procedure and obtaining Informed Consent is a required field of the Telehealth Advanced Form. Video recording by all parties (healthcare provider, patient, support people) will be prohibited.
R4	Storage and Security – ensuring type of technology used for virtual consults is secure and encrypted: The Telehealth Policy and Procedure identifies specific acceptable platforms for telehealth consults, which have been reviewed by Green Cross Health Head of IT. HP should avoid using personal devices, instead use devices "earmarked" for telehealth with adequate safety netting/firewalls/ malware (as per policy recommendations). The provider will log in remotely into the PMS, via the practice network which is already set up to protect information. Secure portal use for emails and other correspondence as suggested by the Telehealth Policy.
R5	Storage and Security – ensuring location of patient and HP respectively protects the parties' privacy: Privacy legislation and considerations outlined in the Telehealth Policy as well as the guide for telehealth consults. The Privacy Policy wile be updated to include working from home and should include a self-assessment checklist.
R6	Storage and Security – recordings (ensuring patient or family members or others in support do not record consults without HP knowledge/consent): Patient information given prior to the consult explaining recording not permitted without explicit consent. The Telehealth Advanced Form also provides acknowledgement of the agreement not to

	record. The contingency plan within the Telehealth Policy and patient information outlines the consequences of unauthorized records.
R7	Accuracy – quality of technology may affect accuracy of personal information collected and relied on: The Contingency Plan within the Telehealth Policy provides guidance on what to do should the quality of the technology be poor and therefore unreliable.
R8	Disclosure – other people in attendance during virtual consults – how to protect patient confidentiality and ensure one-to-one discussions where considered necessary: Disclosure is addressed in the Telehealth Policy, the Telehealth Advanced Form, and the guidance for telehealth consults.

7. Action plan

This section sets out what actions are being taken (whether short or long term) and how they will be monitored in respect of the identified risks.

Ref	Agreed action	Who is responsible	Completion Date
R1	Update policy and advanced form to include identity verification		7/7/20
R2	Update advanced form to include shared record access consent		7/7/20
R3	Update policy to include prohibiting video recording.		13/7/20
R4	Update policy to include acceptable IT platforms and use of secure messaging		7/7/20
R5	Create a Working from Home Policy to include a self-assessment checklist	Miriam/ Kelly	TBA
R6	Update policy and patient information to include contingency planning		7/7/20
R7	Update policy to include contingency planning		7/7/20
R8	Update policy and advanced form to protect patient privacy		7/7/20