Simply Privacy

ProCare

Doxy.me Independent Privacy Impact Assessment

8 May 2020

By Daimhin Warner
Director (Auckland)
Simply Privacy Ltd

Table of contents

This assessment is not legal advice, and its contents should not be taken as legal advice.

This assessment has been prepared for ProCare, which has been given licence to share the assessment with its members and other Primary Health Organisations.

In preparing this assessment, Simply Privacy has relied upon information, statements and representations provided to it by ProCare and Doxy.me. Simply Privacy provides no warranty of completeness, accuracy or reliability in relation to this information, these statements or these representations.

Executive summary

This is an independent PIA into the use of telemedicine platform Doxy.me by General Practitioners ('GPs') in New Zealand, during the COVID-19 outbreak and beyond.

GPs have good cause to turn to telemedicine solutions in order to continue delivering health services during the COVID-19 crisis, and to better deliver health services in the future. In doing so, GPs must balance patient privacy considerations against the need to effectively deliver critical health services. No telemedicine solution will be entirely free of privacy or security risks and so ProCare and its members must find a solution that offers the best medical functionality in the most privacy protective way.

Doxy.me appears to be a relatively low-risk solution. Unlike mainstream video-conferencing solutions such as Zoom, Skype or Houseparty (which have been recently criticised), Doxy.me has been designed specifically for the health industry, to meet general privacy principles, including data minimisation and security. As a global SAAS provider, Doxy.me has developed processes, policies and collateral designed to meet the requirements of multiple privacy laws and regulations, including the highly restrictive EU General Data Protection Regulation.

The real risks to GPs and their patients will arise as a result of the way GPs use the platform. In many cases, these are not new risks. They already exist to some extent in respect of in-person and phone consultations. However, Doxy.me could facilitate the collection of new health information, or existing information in new ways, and care should be taken to ensure that such collections comply with the Health Information Privacy Code and maintain patient trust and confidence.

For this reason, the majority of recommendations in this PIA are intended to assist GPs to manage their virtual interactions with patients in the same way they should all interactions. Some recommendations may provide broader guidance to the sector about improving their general privacy practices and others focus specifically on managing the privacy impacts of virtual consultations. Few relate specifically to the Doxy.me platform.

Overview of privacy risk

Health information privacy rule	Risk	Relevant recommendations
Rule 1 – Scope of collection	**Moderate**	Rec-003, Rec-004, Rec-005
Rule 2 – Source of information	None	N/A
Rule 3 – Notice of collection	**Moderate**	Rec-003, Rec-005, Rec-006, Rec-007
Rule 4 – Manner of collection	**Moderate**	Rec-003, Rec-005, Rec-006, Rec-008
Rule 5 – Security safeguards	**Moderate**	Rec-001, Rec-002, Rec-009, Rec-010, Rec-011, Rec-014

Health information privacy rule	Risk	Relevant recommendations
Rule 6 – Subject access rights	None	N/A
Rule 7 – Subject correction rights	None	N/A
Rule 8 – Accuracy	Low	Rec-012
Rule 9 – Retention of information	None	Rec-002
Rule 10 – Use of information	None	Rec-002
Rule 11 – Disclosure of information	Low	Rec-002, Rec-013, Rec-014
Rule 12 – Unique identifiers	None	N/A
Initial risk – if recommendations are not followed		**Low-Moderate**
Residual risk – if recommendations are followed		**Low**

Recommendations

Rec-001:	Use only paid versions of Doxy.me – pro or clinic – to ensure best possible privacy and medical functionality is available.
Rec-002:	Require Doxy.me to sign a Data Processing Addendum, which provides greater contractual protections in respect of the use and security of data processed by Doxy.me on the GP's behalf.
Rec-003:	Only record a virtual consultation if this is necessary for the purposes of treating the patient, and with the patient's knowledge and consent.
Rec-004:	Do not use third party software to record a consultation.
Rec-005:	Only use the Photo Capture feature if this is necessary for the purposes of treating the patient, and only with the patient's knowledge and consent.
Rec-006:	Use Doxy.me's 'Custom Terms of Service' feature to provide patients with specific privacy notice about the use of Doxy.me, and also to obtain patient consent where this is required.
Rec-007:	Update practice privacy notices to address the use of telemedicine solutions.
Rec-008:	Ensure patients have the capacity to make sound decisions about their own risk, and that they are taking steps to protect their privacy during a virtual consultation.
Rec-009:	Take steps to ensure the use of Doxy.me is as secure as possible, including setting room passcodes, keeping login credentials confidential and following Doxy.me's general security guidance for users.
Rec-010:	Be mindful of privacy and confidentiality when using Doxy.me to run consultations, particularly where it is being used in another location to the clinic.
Rec-011:	Review patient identity verification processes to ensure they effectively mitigate the risk of disclosing health information to an unauthorised third party.

Rec-012:	Consider confirming the accuracy of notes taken during a virtual consultation with the patient, particularly where these notes may be used to make significant health care decisions.
Rec-013:	Only invite other parties to join a virtual consultation if this is necessary for the purposes of treating the patient, and only with the patient's knowledge and consent.
Rec-014:	Ensure any third parties used by Doxy.me to process health information have been assessed for privacy and security risk.

About this PIA

A Privacy Impact Assessment ('PIA') is an essential part of many projects and proposals, and can be used to help agencies identify the potential risks arising from their collection, use or handling of personal information, to find out if they are meeting their legal obligations. It identifies the ways a new proposal or operating system, or changes to an existing process, may affect personal privacy, to help agencies make more informed decisions and better manage privacy risks.

Purpose and scope

This is an assessment of the use of telemedicine platform Doxy.me by General Practitioners ('GPs') in New Zealand. Having completed a high-level risk assessment of Doxy.me (which included an informal security review), ProCare made the decision that this platform was the best option and recommended it to its member practices. However, ProCare recognised that a more comprehensive privacy assessment should be completed to provide assurance to both practitioners and patients that Doxy.me did not present too great a privacy risk.

In scope	Out of scope
• Impact of use of Doxy.me by GPs on the management of health information, and compliance with the Health Information Privacy Rules (contained in the Health Information Privacy Code). • Application of Privacy Act provisions in respect of the use of service providers to process or store personal information, including a review of what health information Doxy.me collects or uses in order to deliver services. • Patient experience of using Doxy.me to interact with their GP, including potential negative perception issues, the sufficiency of transparency around patient risk, and the relevance of the practitioner/patient relationship to issues of fairness.	• Technical security risks created by the use of Doxy.me, for both GPs and their patients. While security is an important element in the privacy framework, and this PIA will identify several high-level security risks, this is not a security assessment, which will require the use of technical security experts. • The implications of using telemedicine solutions on GP compliance with medical practice standards and regulations, including the Health Practitioners Competence Assurance Act and the Code of Health and Disability Services Consumers' Rights. • The privacy impacts of Doxy.me's collection and use of information about GPs using the platform, such as contact details, billing information or web usage data. This is not sensitive information and Doxy.me's practices in this regard appear to be industry standard.

Process

This PIA has been developed remotely, and has considered the following sources of information:

- **The Doxy.me platform** – we have created a provider account for the purposes of navigating and understanding the platform and have also participated in a virtual consultation with a GP to better understand the patient experience.
- **Doxy.me collateral** – including HECVAT (assessment tool required by higher education clients in the US) completed in 2019, Terms of Service (online as at 21 April 2020), Privacy Policy (online as at 21 April 2020), and a selection of Doxy.me Help Center articles (online as at 21 April 2020).
- **Privacy Shield report** for Doxy.me (online as at 21 April 2020).
- **Informal security review** into Doxy.me conducted by Quantum Security on 26 March 2020.
- **Health industry guidance** on the use of telemedicine platforms for delivering health services in NZ.
- **Interview** with Dr Jamie Shephard (a Doxy.me pro user) on 21 April 2020.
- **Ongoing correspondence** with ProCare Chief Technology Officer Duane Makin.
- **Email engagement** with Doxy.me's Security Officer Dylan Turner, to clarify certain matters that were unclear from available collateral.

Risk-based approach

This PIA takes a risk-based approach, consistent with general principles of Privacy by Design. It does not look for outcomes that protect privacy at the total expense of other risks. Rather, it recognises that privacy is one of many risks a health agency must address. The Privacy Act itself facilitates this approach, accepting that the right to privacy must be balanced against the general desirability of a free flow of information (which is critical to the effective delivery of health services) and the right of business and government to achieve their objectives in an efficient way.

In this case, GPs must balance patient privacy considerations against the need to deliver critical health services at a time when in-person consultations are difficult, if not impossible, for most patients. No telemedicine solution will be entirely free of privacy or security risks and so ProCare and its members must find a solution that offers the best medical functionality in the most privacy protective way. This needs to be a positive-sum outcome.

Background and context

Telemedicine solutions and COVID-19

Telemedicine, or telehealth, describes the use of information and communication technologies to deliver health services when patients and healthcare providers are not in the same location.[1]

The potential benefits of such solutions to the effective delivery of health services in 'normal' times are clear. They reduce health inequity by ensuring the delivery of services to patients in remote areas, to elderly patients or those with physical or cognitive limitations, or to patients facing social or financial barriers to visiting their GP. They also improve a GP's ability to regularly interact and engage with their patients and enhance the care relationship.

For these reasons, ProCare and other Primary Health Organisations have been investigating potential telemedicine solutions for some time, and many GPs already used Doxy.me or other equivalent solutions. According to one GP, approximately 10% of consultations were run over a telemedicine platform prior to the COVID-19 outbreak. In fact, GPs have been practicing phone-based triage since the 1970s.

However, in March 2020, the government instituted a nationwide mandatory (level 4) lockdown in response to the COVID-19 outbreak. This required all NZers to self-isolate in their homes and travel only for essential services, including health services. The risk to both patients and healthcare staff of contracting COVID-19 further contributed to a reluctance to permit physical consultations.

On 28 April 2020, the level 4 lockdown will be relaxed, and NZ will move to level 3, which permits slightly greater travel and interaction. However, for the purposes of health service delivery, the risks remain the same. It is possible that the COVID-19 alert level will fluctuate between 3 and 4 for several months. In any event, there is likely to be a greater reluctance by many patients – and particularly vulnerable patients (the elderly or those with underlying health conditions) – to visit their GPs for some time.

ProCare recognised that telemedicine solutions would be critical to ensuring that health practitioners could continue to deliver health services during COVID-19 response levels 3 and 4, and beyond as the consequences of the outbreak continue. ProCare advised its members to use Doxy.me (being relatively comfortable with the risks it presented). It is estimated that 85% of GP clinics in NZ are now using Doxy.me, and approximately 75% of daily consultations are completed on the platform, with the remainder taking place either by phone or in person.[2]

[1] See Royal NZ College of General Practitioners *Position Statement: Telehealth and technology-based health services in primary care* November 2017.
[2] Based on very general estimates provided by Dr Shephard.

Doxy.me

Doxy.me is a US-based telemedicine platform, which enables encrypted peer-to-peer audio-visual consultation services for health practitioners. The platform has been designed to create a virtual GP workflow that mimics, to some extent, an in-person visit to a GP. It provides a virtual waiting room, permits patients to message their doctors, and enables file sharing where this is required.

The general process for using Doxy.me is as follows:

- GPs register with the platform and set up a virtual waiting room with a specific URL.
- When a patient makes an appointment for a virtual consultation, the GP will email or text their URL to the patient (along with a passcode in most cases).
- At the appointed time, the patient will enter the URL in their web browser and be invited to enter the virtual waiting room.
- Patients do not register to use the Doxy.me platform and are not required to provide any personal identifiers (other than entering their name in the virtual waiting room to let the GP know they are waiting).
- The GP can then initiate the virtual consultation (much like a Zoom or Skype meeting).
- While in the waiting room, and during the consultation, the patient and GP can message one another using a 'live chat' function.
- GPs can also capture still images during a consultation (for example to take a record of a specific skin condition), share their screen with the patient, and transfer files or documents to or from the patient.
- The platform loosely integrates with the GP's Patient Portal. GPs must take consultation notes in their own Practice Management System ('PMS').

Doxy.me provides varying levels of functionality and customisation depending on the account level the GP has selected. GPs and clinics can use a limited version of the platform for free, but paid versions - 'pro' and 'clinic' accounts – provide for greater functionality and customisation.[3]

The differences between the free and paid versions of the platform have both positive and negative impacts on privacy risk and medical functionality. These impacts are compared in the table below and discussed where relevant later in the PIA. To ensure that GPs can enjoy the maximum functionality of the platform and best meet privacy and security requirements, it is recommended that GPs should **not** use the free version.

Rec-001: Use only paid versions of Doxy.me – pro or clinic – to ensure best possible privacy and medical functionality is available.

[3] For more detail see https://doxy.me/pricing.

Free version	Paid versions
• No room passcode *-ve privacy impact / no medical impact* • Permits basic video-call features only *+ve privacy impact / -ve medical impact* • Does not process patient payments *+ve privacy impact / no medical impact* • Permits custom terms of service *+ve privacy impact / +ve medical impact* • Meets standard privacy and security requirements *neutral impact*	• Room passcode *+ve privacy impact / no medical impact* • Permits photo capture, group calling, screenshare and file transfer *-ve privacy impact / +ve medical impact* • Processes patient payments *-ve privacy impact / no medical impact* • Permits custom terms of service *+ve privacy impact / +ve medical impact* • Clinic version allows for custom security review addon *+ve privacy impact / no medical impact*

Doxy.me data collection

Administrative and usage data

Doxy.me must collect some personal information about GP users (such as their names, identifiers, IP addresses, payment information and information about their use of the platform collected via cookies) in order to manage user accounts and ensure that the platform is functioning optimally. It may also collect IP addresses and web usage data from patients when they use the platform from within their web browsers, but because patients do not have to register to use the platform, this information will not be connected to an identifiable individual.

Doxy.me states that it stores administrative and usage data within the Amazon Web Services ('AWS') datacenter in the US.[4]

Health information

Doxy.me states that it does not collect or retain any health information (including audio/visual information about the consultation). According to Doxy.me, servers are used to establish a connection between the GP and the patient. Video calls are encrypted peer-to-peer, meaning the audio-video data flows directly between the two individuals on the call, not through Doxy.me servers.[5] Doxy.me has also confirmed to Simply Privacy that it does not collect or store live chats generated during a consultation, or the name a patient enters when they check in to the waiting

[4] For more information see https://help.doxy.me/en/articles/3839200-where-doxy-me-servers-are-located and https://help.doxy.me/en/articles/95911-is-doxy-me-secure.
[5] https://help.doxy.me/en/articles/3839200-where-doxy-me-servers-are-located.

room. It is understood (though not confirmed) that photos and files shared are saved directly to the GP's Practice Management System, and not collected or stored by Doxy.me.

Doxy.me also provides online payment functionality, to allow patients to pay for consultations within the platform. This functionality requires Doxy.me to integrate with Stripe.com, which processes the payments and deposits them into the GP's account. This transaction information would also be health information for the purposes of the HIPC. This information would be processed by Stripe.com (and not Doxy.me) on behalf of the GP.

Doxy.me privacy compliance

The following facts, assertions and documents are relevant to Doxy.me's general privacy and security compliance:

- Doxy.me claims to be **compliant with both the US HIPAA and HITECH Act**[6] and the **EU General Data Protection Regulation** ('GDPR').[7] While Doxy.me does not provide detailed evidence to support these claims, they at least indicate that these restrictive privacy laws have been considered as part of the platform design.

- Doxy.me is an active participant in **the EU-US Privacy Shield Framework**,[8] which provides added assurance that Doxy.me has put in place policies and procedures to ensure it processes personal information in compliance with generally accepted privacy principles.

- Doxy.me states that it will sign a **Data Processing Addendum** ('DPA') for any GP users who are subject to the GDPR. This DPA is a requirement of the GDPR where a data controller (a GP) uses a data processor (Doxy.me) to store or process personal information on their behalf. It includes specific privacy and security assurances and commits Doxy.me to notifying the GP of any data breach that might impact on their data.

- Doxy.me's **Terms of Service** are relatively standard and reflect the fact that the platform does not store health information. For the most part, these Terms relate to Doxy.me's proprietary information and intellectual property. The following provisions are of interest:

    - Doxy.me clarifies that it provides services only to health providers (GPs), not to patients. Thus, Doxy.me places all liability for providing privacy notices or obtaining consent in respect of patient use of Doxy.me on the GP (clause 2).

[6] For more information see https://help.doxy.me/en/articles/95854-is-doxy-me-hipaa-compliant.
[7] For more information see https://help.doxy.me/en/articles/1621447-is-doxy-me-gdpr-compliant. GDPR is comparable to (and in many ways more restrictive than) the NZ Privacy Act.
[8] This framework was established to facilitate the lawful transfer of personal information from data controllers in the EU to data processors in the US. The GDPR permits the transfer of personal information outside the EU only where the receiving country has comparable privacy frameworks in place. The Privacy Shield Framework was developed because the US does not have a comprehensive privacy law similar to the GDPR (or NZ Privacy Act). Privacy Shield has been criticised by the European Data Protection Supervisor and may be declared invalid by the European Court of Justice.

- GP users may sign into their accounts and delete their data (clause 8).
- Clause 1 states that materials a GP posts in its virtual waiting room are theirs alone. However, clause 11 states that Doxy.me has the right to use "Provider Content" in any way it wishes. This inconsistency should be noted but would not impact on patient privacy (as health information should not be posted in this way).
- GP users have some responsibility to ensure that data is safe and secure while using Doxy.me (clause 19).

- Doxy.me's **Privacy Policy** is comprehensive but, unfortunately, also highly technical and complex. It would be difficult for a layperson to understand. The policy sets out the personal information Doxy.me collects about users, how it will be used and who it may be shared with. It relates only to administrative and usage data collected about GP users which is out of scope of this PIA. As such, it has little relevance to the management of health information by GPs using the platform. This is to be expected, because Doxy.me does not collect or store health information.

Privacy risk and compliance assessment

Relevant laws

Health agencies in NZ must comply with the Privacy Act 1993 and the more specific provisions of the Health Information Privacy Code 1994 ('HIPC'). The Health Act 1956 and Health (Retention of Health Information) Regulations 1996 are also relevant to the management of health information.

The HIPC contains 12 health information privacy rules which essentially mirror the information privacy principles contained in the Privacy Act. These rules provide health agencies with a roadmap for managing health information, from collection through to destruction. They are intended to be flexible enough to permit health agencies to collect, use and share the information they need to deliver health services; many of the rules contain exceptions that ensure privacy does not become a barrier to health or safety outcomes.

The **health information privacy rules** require a health agency to:

1. **Scope** – Collect only the health information it needs for a lawful purpose connected with its functions.
2. **Source** – Collect health information directly from the person concerned, unless an exception applies.
3. **Notice** – Tell people certain things when collecting health information directly from them.
4. **Manner** – Collect health information in ways that are lawful and, in the circumstances, fair and not unreasonably intrusive.
5. **Security** – Take reasonable steps to protect health information from harm.
6. **Subject access** – Give people access to the health information it holds about them.
7. **Correction** – Let people correct health information if it is incorrect.
8. **Accuracy** – Take reasonable steps to ensure health information is accurate and up to date before using it.
9. **Retention** – Retain health information for no longer than is required.
10. **Use** – Use health information only for the purposes for which it was collected, unless an exception applies.
11. **Disclosure** – Not disclose health information, unless an exception applies.
12. **Unique identifiers** – Take care when assigning or using unique identifiers.

In November 2020, a new Privacy Act 2020 will come into force. The new Act will introduce, among other things, mandatory privacy breach notification, increased enforcement powers for the Privacy Commissioner and new criminal offences with increased associated fines. The Act is also changing in other ways that will bring it closer to important overseas regulations, such as the GDPR. Many of the changes to the Act will be incorporated into the HIPC and other privacy codes of practice. Where relevant, new provisions in the 2020 Act are referenced below.

Finally, it is possible, though very unlikely during the current global crisis, that NZ GPs may use Doxy.me to run virtual consultations with patients who are in the EU at the time of the consultation (such as NZers who are in need of urgent medical assistance while travelling). In these cases, the collection and processing of health information would need to comply with the GDPR (though this would already be the case for phone consultations with patients in the EU).

The GDPR is essentially similar to the NZ Privacy Act. However, a key difference for the purposes of this PIA is the prohibition on processing special categories of personal data, including health information. The GDPR states that a health agency may only process health information with the explicit consent of the patient. This, and any other additional GDPR considerations, are addressed where relevant below.

Personal information impacted by Doxy.me

Doxy.me is designed to facilitate virtual consultations between a GP and their patients. This means that its use can impact **any health information** a GP might collect from a patient during the course of a consultation, including medical conditions, mental health information, personal identifiers, treatment plans, diagnoses, medications, family or employment details.

Depending on the functionality a GP chooses to use on the platform, Doxy.me might also facilitate the collection of photographs (where the Photo Capture feature is used) or files or documents that have been uploaded by a patient. Use of the live chat feature could create additional health information impacted by the platform. Doxy.me does not currently enable a GP to record a consultation, but it is developing this capability.

Doxy.me also allows users to run group consultations, and so personal or health information about people other than the patient may be impacted by use of the platform.

Governance and accountability

GPs are accountable for any privacy risks created by the use of Doxy.me. The Privacy Act states that personal information stored or processed by an agent (Doxy.me) on behalf of a principal (GP) is deemed to be held by the principal. To use GDPR terminology, GPs are data controllers – which means they decide what health information to collect via Doxy.me, and how it will be used – and Doxy.me is the data processor – which means it processes health information only on the instructions of the GP and does not collect, store or use this information for its own purposes.

This means that each GP must consider and be comfortable with the risks Doxy.me presents for both their own liability and the privacy of their patients before they use the platform. Each GP can take this PIA into account but must ultimately make their own assessment based on their own risk appetite.

For this reason, and in recognition of the fact that some GPs will use Doxy.me to interact with patients who are located in the EU, it is recommended that GPs should ask Doxy.me to sign a Data Processing Addendum ('DPA') that records the respective roles of the GP and Doxy.me, and provides additional contractual assurances to the GP in respect of data access and use, security, and privacy breach response. Doxy.me uses its own DPA. While Simply Privacy has not reviewed this document, it is likely to contain the standard content required by the GDPR. However, if GPs are concerned with the DPA, they are recommended to obtain independent legal advice before signing it.

Rec-002: Require Doxy.me to sign a Data Processing Addendum, which provides greater contractual protections in respect of the use and security of data processed by Doxy.me on the GP's behalf.

Compliance with health information privacy rules

Rule 1 – Scope

Health agencies should collect only health information that is necessary for a lawful purpose connected with their functions. There are no exceptions to this principle.

The use of Doxy.me could create **moderate risk** to a GP's compliance with rule 1.

The use of Doxy.me should not generally change the breadth or depth of health information a GP collects during a consultation. The health information collected during a virtual consultation should be the same as that collected during a phone or in-person consultation and limited to that necessary to provide the health services the patient requires.

However, Doxy.me functionality may provide GPs with the ability to collect new forms of information:

- While Doxy.me does not currently enable a GP to record a virtual consultation (unlike, for example, Zoom), Doxy.me states on its website that it is developing a screen recording feature, to be released in 2020. Further, Doxy.me notes to users that virtual consultations can currently be recorded in other ways, using applications such as Screencastify, Quicktime or Camtasia.[9]
- GPs can collect still images of virtual consultations using the Photo Capture feature. It should be noted that the platform does not make a patient aware that a practitioner is

[9] For more information see https://help.doxy.me/en/articles/95894-coming-soon-record-your-session

capturing a photo. It is important therefore that this is made clear to the patient beforehand.

- GPs can ask patients to upload files and documents, which may contain sensitive health or other information.

Rec-003:	Only record a virtual consultation if this is necessary for the purposes of treating the patient, and with the patient's knowledge and consent.

Rec-004:	Do not use third party software to record a consultation.

Rec-005:	Only use the Photo Capture feature if this is necessary for the purposes of treating the patient, and only with the patient's knowledge and consent.

Rule 2 – Source

Health agencies should collect health information directly from the individual concerned, unless an exception applies.

The use of Doxy.me will create **no risk** to a GP's compliance with rule 2.

Rule 3 – Notice

When collecting health information directly from individuals, health agencies must provide notice about what information will be collected or generated, how that information will be used and who it may be shared with.

Use of Doxy.me will create **moderate risk** to a GP's compliance with rule 3.

For many patients, the use of telemedicine solutions will be unfamiliar and unsettling. While, subject to the matters addressed above at rule 1, GPs should not generally be collecting more health information as a result of running a virtual consultation, there are a number of features provided by Doxy.me that patients should be notified about. GPs would be wise to provide patients with some assurances about the safety of their health information.

This notice, which should be provided to patients before they use Doxy.me, could be coupled with the informed consent recommended by other health agencies[10] in accordance with the requirements of the Code of Health and Disability Services Consumers' Rights. It should be noted however that this privacy notice is intended to deliver more specific information about the privacy impacts of using Doxy.me. Finally, where a GP must comply with the GDPR, this notice can also seek the consent of the patient. A suggested notice is provided at Appendix 1 of this PIA.

[10] Such as in the Homecare Medical Virtual GP Kit.

Further, all GPs should have general practice privacy notices in place currently that comply with the requirements of rule 3. Some may have developed their own notices, but many will rely on the draft notice provided by the Ministry of Health. In either case, in addition to developing a specific privacy and consent notice for use within the Doxy.me platform, GPs should update their practice privacy notices to address the use of telemedicine solutions.

Rec-006: Use Doxy.me's 'Custom Terms of Service' feature to provide patients with specific privacy notice about the use of Doxy.me, and also to obtain patient consent where this is required.

Rec-007: Update practice privacy notices to address the use of telemedicine solutions.

Rule 4 – Manner

Health agencies should collect personal information in ways that are lawful and, in the circumstances, not unfair or unreasonably intrusive. Privacy Act 2020 will introduce an additional requirement for agencies to consider the vulnerability of young people when deciding how to collect personal information.

The use of Doxy.me could create **moderate risk** to a GP's compliance with rule 4.

Collecting health information via a virtual consultation is not unlawful but it could, in some circumstances, be unfair or unreasonably intrusive. This will depend on a number of factors relating to both the GP and the patient.

- GPs should be mindful of the power imbalance that exists between patient and GP, and the fact that patients will generally trust (or feel compelled to trust) the GP's judgement on the use of Doxy.me. The impact this relationship may have on a patient's decision to use Doxy.me could, if managed badly, be deemed unfair. Being transparent about the risks, as recommended at Rec-006, will assist GPs to manage this risk.

- Virtual consultations could have a more significant impact on emotionally vulnerable patients, young patients, or those with particular cultural sensitivities. GPs should be mindful of a patient's ability to make an objective decision about their use of Doxy.me, and assist them if they feel compelled to use the platform despite unresolved concerns about it. As above, transparency will assist with this.

- Some patients may have difficulty finding a private space to use Doxy.me in their homes. GPs should take some responsibility for ensuring that patients are taking steps to protect their own privacy while using the platform and should check in with patients during a virtual consultation to ensure that they remain comfortable to continue.

- Recording a virtual consultation, or taking a photo of a consultation, without the knowledge of the patient would likely constitute an unfair collection of health information. For this reason, it is critical that GPs always inform a patient of their intention to do this and, ideally, ask for their consent.

Rec-008: Ensure patients have the capacity to make sound decisions about their own risk, and that they are taking steps to protect their privacy during a virtual consultation.

Rule 5 – Security

Health agencies should take reasonable steps to protect health information from loss, unauthorised access and disclosure, or misuse. Privacy Act 2020 will introduce an additional requirement to notify the Privacy Commissioner and affected individuals of any privacy breach that is likely to cause serious harm.

The use of Doxy.me could create **moderate risk** to a GP's compliance with rule 5, but Doxy.me appears to have put processes, safeguards and controls in place to effectively mitigate this risk.

The use of any third party cloud solution to process health information increases information security risk. However, this does not mean such solutions should not be used. Most reputable providers consider security risk to be their highest priority, particularly where their business model relies on the trust and confidence of their users. This appears to be the case for Doxy.me, which has been designed to process (though not store) health information.

Doxy.me privacy settings

Doxy.me claims the following security features, which appear reasonable in the circumstances (note, however, that this is not a security assessment):

- All video and audio communication is protected by point-to-point NIST-approved AES 128-bit encryption, by default.
- All data stored at rest is protected by full volume encryption and 256-bit AES encryption.
- Access to the Doxy.me interface is secured over TLS (https).
- Provider passwords are stored using one-way cryptographic hashing functions.
- Doxy.me staff have access to GP user data only on a need-to-know basis.

Independent assurance

While Doxy.me provides some assurance of the security safeguards and controls it has in place, it is important also to have some independent assurance that these are adequate and functioning.

- Doxy.me cites compliance with several information security standards, including FIPS 140-2, and provides a link to a report by the US National Institute of Standards and Technology[11] (this report appears to relate to the AWS encryption application that Doxy.me uses). Beyond this, we could find no other independent security assurances on

[11] https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3139.

the Doxy.me website, but Doxy.me states that it conducts annual HITECH risks assessments with third party auditors (including active penetration testing and vulnerability scans).[12]

- As noted above, Doxy.me is an active participant in the EU-US Privacy Shield Framework, although it should be noted that this cannot be taken as independent assurance that it meets the security standards required by the GDPR, as agencies generally self-certify for this framework.
- ProCare obtained an informal security assessment of Doxy.me from Quantum Security. Quantum Security stated that it was 'fairly comfortable' to recommend the use of Doxy.me by GPs on the basis that communications were encrypted, and no health information was stored by Doxy.me. However, Quantum Security qualified that its assessment was not a full penetration test, and it did not test the security functions of the platform.

In view of the fact that Doxy.me does not collect or store health information, including the content of virtual consultations, the security settings and assurances outlined above are likely sufficient.[13] However, if concerned, GPs are recommended to obtain their own independent security assessments of the platform, which could focus specifically on the security of the virtual consultation itself, rather than the limited personal information Doxy.me collects to manage the platform.

Steps GPs can take to increase security

In addition to technical security measures in place within the platform, GPs can put in place a number of organisational safeguards to ensure that their use of Doxy.me is as secure as possible. GPs could consider taking the following steps:

- Set room passcodes as default, to ensure that access to virtual waiting rooms and clinics is limited to legitimate patients only. Passcodes should be sent to patients in a separate communication to the URL invitation.
- GPs must be mindful of privacy and confidentiality when using Doxy.me to run consultations, particularly where they are using the platform from their homes. They must ensure that their screens are protected from general view, that they use headphones, and that they password protect the devices they use to access their Doxy.me account and any other GP systems or platforms. Doxy.me should never be used on a shared public Wi-Fi network.
- Take this opportunity to review their patient identity verification processes to ensure they are robust enough to mitigate the risk of fraudulent use of Doxy.me to obtain access to health information about another patient. While this is also a risk in respect of phone and in-person consultations (particularly where a patient is not well-known to GP staff), telemedicine solutions may increase the risk of unauthorised access.

[12] For more information see https://help.doxy.me/en/articles/95911-is-doxy-me-secure.
[13] **Note** – this assessment is based on the understanding that Doxy.me does not collect or store any health information relating to a virtual consultation, including audio/visual information, live chats, photos captured, or files/documents shared. Simply Privacy was unable to confirm with Doxy.me whether the latter two categories of information were not collected or stored.

- Keep login credentials confidential to prevent the unauthorised use of GP URLs or access to virtual consultations.
- Follow Doxy.me's security requirements for all users, which provide a sensible set of safeguards and reminders.

Rec-009:	Take steps to ensure the use of Doxy.me is as secure as possible, including setting room passcodes, keeping login credentials confidential and following Doxy.me's general security guidance for users.

Rec-010:	Be mindful of privacy and confidentiality when using Doxy.me to run consultations, particularly where it is being used in another location to the clinic.

Rec-011:	Review patient identity verification processes to ensure they effectively mitigate the risk of disclosing health information to an unauthorised third party.

Privacy breach notification

Privacy Act 2020 will introduce a mandatory breach notification obligation for all GPs, which will require any privacy breaches that are likely to cause serious harm to be notified to the Privacy Commissioner and affected individuals. This notification must take place as soon possible after the GP becomes aware of the breach. The Act states that an agency is deemed to know about a breach as soon as an employee or service provider knows of the breach.

Doxy.me does not collect or store health information, and so a breach that affects Doxy.me's data at rest will be unlikely to cause harm to a patient. However, if Doxy.me becomes aware of a vulnerability that could impact on, for example, the encryption of virtual consultations, this could have a significant impact for GPs and their patients. Thus, GPs must have some assurance that Doxy.me will quickly notify them of an actual or possible privacy breach.

The Doxy.me Terms of Service contain no contractual assurances around information security or privacy breach management. **For this reason, it is important that GPs require Doxy.me to sign the DPA referenced at Rec-002 above.**

Rule 6 – Subject access

Individuals have the right to request a copy of the health information a health agency holds about them.

The use of Doxy.me should create **no risk** to a GP's compliance with rule 6, though GPs should note that patients or their representatives will have the right to request copies of any photos taken by a practitioner during their consultation.

Rule 7 – Correction

Individuals have the right to ask a health agency to correct the health information it holds about them, or to attach a statement of correction to that information.

The use of Doxy.me will create **no risk** to a GP's compliance with rule 7.

Rule 8 – Accuracy

Before using or disclosing health information, health agencies should take reasonable steps to ensure that it is accurate, up-to-date, complete, relevant and not misleading.

The use of Doxy.me will create a **low risk** to a GP's compliance with rule 8.

As with phone consultations, there is a small risk that health information captured during a virtual consultation could be incorrect or inaccurate, due for example to a temporary loss of connection or mishearing by the GP. Where a GP intends to make a health care decision – such as to diagnose a condition, prescribe medication, develop a treatment plan or refer a patient to another provider – inaccuracies in the information could cause harm to a patient.

Where health information collected as part of a virtual consultation is to be used for making health care decisions, it is recommended that GPs should consider providing patients with a copy of the notes they have taken, to ensure that they are accurate, though it is accepted that there may be cases where such a step is either impracticable or inappropriate.

Rec-012: Consider confirming the accuracy of notes taken during a virtual consultation with the patient, particularly where these notes may be used to make significant health care decisions.

Rule 9 - Retention

Health agencies should retain personal information only for as long as it is required for a lawful purpose.

The use of Doxy.me will create **no risk** to a GP's compliance with rule 9, because Doxy.me does not store any health information on a GP's behalf.[14] Any health information captured via the platform or recorded about a virtual consultation will be stored by the GP in their own PMS and subject to the GP's general information retention rules (which should reflect the requirements of the Health (Retention of Health Information) Regulations).

[14] See qualification at note 13 above.

Rule 10 – Use

Health agencies should only use health information for the purposes for which it was collected, unless an exception applies to permit another use.

The use of Doxy.me will create **no risk** to a GP's compliance with rule 10, provided that Doxy.me does not collect and use health information for its own purposes.[15] However, to ensure that this remains the case, **GPs should require Doxy.me to sign the PDA referenced at Rec-002 above**.

Rule 11 - Disclosure

Health agencies should not disclose health information, unless an exception applies that permits the disclosure.

The use of Doxy.me will create a **low risk** to a GP's compliance with rule 11.

Doxy.me does not collect or share health information for its own purposes.[16] However, as with rule 10, to ensure that this remains the case, **GPs should require Doxy.me to sign the DPA referenced at Rec-002 above**.

GPs should be mindful of the fact that certain Doxy.me features may make it easier to share health information. For example, GPs can invite other parties to join a virtual consultation, including other health providers, a patient's whānau or a patient's representative. Due care should be taken to ensure that patients understand why other parties are being invited to join a consultation, and that they are comfortable with this.

GPs should also be aware that certain Doxy.me features – such as the use of the Payment feature – may require Doxy.me to share personal or health information with third party providers for processing. As noted above, a patient's payment transaction for a virtual consultation would fall within the definition of health information, and so must be managed in accordance with the HIPC. In this example Doxy.me uses the online payment platform Stripe.com.

Rec-013:	**Only invite other parties to join a virtual consultation if this is necessary for the purposes of treating the patient, and only with the patient's knowledge and consent.**

Rec-014:	**Ensure any third parties used by Doxy.me to process health information have been assessed for privacy and security risk.**

[15] See qualification at note 13 above.
[16] See qualification at note 13 above.

Rule 12 – Unique identifiers

Health agencies should take care when assigning or using unique identifiers and should not require an individual to disclose a unique identifier that was assigned by another agency. The NHI is an exception.

The use of Doxy.me will create **no risk** to a GP's compliance with rule 12.

Overall privacy risk assessment

On balance, taking a risk-based approach that recognises the health care benefits of using telemedicine solutions, and recognising the privacy and security features that have been designed into the Doxy.me platform, the initial risk of using Doxy.me is assessed as **low-moderate**.

The use of Doxy.me has a limited impact on GP compliance with most of the health information privacy rules, and for the most part the risks here are created by the way GPs used the platform, rather than the platform itself. The recommendations set out in this PIA are intended to mitigate these risks and, if GPs follow them, the residual risk of using Doxy.me is assessed as **low**.

Appendix 1: Draft privacy notice

This draft privacy notice relates to Rec-006. Use of this notice would assist GPs to comply with rule 3 of the HIPC and also the notice and consent requirements of the GDPR. Legal compliance aside, such an approach would assist patients to feel comfortable using Doxy.me to discuss and share sensitive health information.

This privacy notice, or something similar, can be uploaded to a GP's Doxy.me virtual waiting room in *Settings/Room Settings/Custom terms of service*. The patient is then directed to read and (if comfortable) agree to the notice when they check in to the waiting room.

Privacy notice about [clinic name]'s use of Doxy.me

We've decided to use Doxy.me to run our virtual consultations. We've assessed the risks of using this service, including the privacy and security risks, and we're satisfied that your health information will be safe.

Importantly, Doxy.me does not collect any health information about you. The consultation you are about to have with your doctor is peer-to-peer, which means only you and your doctor can see or hear the call. Doxy.me will not collect any audio or visual information from this call, or the live chats you have with your doctor, and the consultation is encrypted so no-one else can listen in.

During your virtual consultation, [clinic name] will collect the same sorts of health information we would collect during a normal consultation at our practice. We will record this information on your file, in our secure Practice Management System, and we will use it and protect it in accordance with our practice privacy notice.

We will not record the virtual consultation, but we might take a photo using Doxy.me if we think this is necessary for us to deliver the health services you need. If we want to take a photo, we will tell you first, explain why, and make sure you agree to it. These photos will only be held by [clinic name], not Doxy.me.

By accepting this privacy notice, you are consenting to our use of Doxy.me to run your virtual consultation and to our collection and use of your health information in accordance with our practice privacy notice.

Before your virtual consultation, make sure you are in a private space, away from family or others, where you can feel comfortable to discuss your health concerns. You could also consider using headphones to allow for a more private conversation.

If you have any further concerns about Doxy.me, or [clinic name]'s privacy practices, please discuss these with your doctor.