Discovery

2021

DISCOVERY HEALTH

POPIA FREQUENTLY ASKED QUESTIONS FOR HEALTHCARE PROFESSIONALS

Discovery

Healthcare professional Protection of Personal Information Act (POPIA) frequently asked questions

Disclaimer

We have drafted these answers in response to questions asked by participants during the POPIA webinars which were held during June. Whilst we have made every effort to ensure the accuracy of the responses, Discovery Health cannot be held liable for any issues which may arise in relation to their use.

Appointment and registration of an information officer

1 | **Do practices need to register with the POPIA regulator e.g. appoint an information officer?**

Yes, information officers are, by virtue of their positions, appointed automatically in terms of PAIA and POPIA. However, the Information Regulator has set out guidelines on the registration of Information Officers as well as the deadline by which to do so.

2 | **How do we register a practice with the regulator? Where do we locate that information?**

You can find the information officer's registration form on the Information Regulator's website at https://www.justice.gov.za/inforeg/docs/InfoRegSA-eForm-InformationOfficersRegistration-2021.pdf

You can also find the full guidance note on information officers and deputy information officers outlining obligations and liabilities at: https://justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf

3 | **Does the Information Officer need to be the most senior local staff member? Can this be delegated to anyone?**

The most senior staff member should be the information officer; however, they can delegate responsibilities. Please refer to the guidance note recently published on 1 April 2021 with regards to information officers and deputy information officers (DIOs) from the Information Regulator:
https://justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf

4 | **In practices with lots of practitioners who work under their own practice number and are responsible for their own practice - do we appoint each of them as deputy information officers?**

The practice will need to appoint an information officer on behalf of the practice. Each of the individual practitioners can delegate their responsibilities to this person. In a group practice with multiple practitioners who treat in their own names, but bill as one group practice, one person can be appointed as the information officer. Deputy information officers do not need to be appointed.

5 | **I have a website and I have heard there is a need to have a privacy policy on the website. What should this entail?**

It is recommended that a website has a privacy policy or privacy statement in the event that the practice or business associated to the website shares any personal or special personal information. The privacy policy or privacy statement available to view on the website should include how your practice collects, uses, shares and processes personal information. Discovery Health has created a guideline for medical practices to assist with the creation of your own privacy statement. This is available on request.

6 | **Where would I find a PDF copy of the POPI Act?**

Information relating to the POPIA act can be found at:
https://www.justice.gov.za/inforeg/legal/InfoRegSA-act-2013-004.pdf

7 | **I run a bureau and I would like to know if the regulator will be issuing certificates to state an organisation is compliant?**

The Act does not mention or require the issuing of any certification as to a responsible party's compliance to the Act.

Patient consent

8 | **Do existing patients need to sign a new consent form with regard to POPIA?**

While it would be ideal to get patients to re-sign their consent forms if these were not POPIA compliant, it would be acceptable for the practice to communicate their most recent privacy statements (which should include consent terms) to existing patients and provide the opportunity for existing patients to provide feedback to the practice regarding any objections they may have without re-signing.

9 | **Do you need proof of a written consent from a patient to share info between professionals?**

It is advisable to cover this issue in your privacy statement in which the data subject (patient) will consent to having their information shared with other medical professionals for the provision of health care and related services. This should then be considered as part of the contractual agreement entered into in order to fulfil the services being rendered.

10 | **How old must the data subject be to sign consent? If the client is younger than 18 years old, do the parents then consent on their behalf? Typically, we also get consent from children too.**

Data subjects must be older than 18 years old to sign their own consent. Children under 18 are legal minors who, in South African law, are not fully capable of acting independently without assistance from parents or legal guardians.

11 | **Privacy regarding children under the age of 18? Can it be shared with other doctors in the best interests of the child, even though the child may object?**

The purpose of sharing this information should be clear to the patient's parent or legal guardian (assuming the child is younger than 18 years of age) upfront. This should be considered as part of the contractual agreement entered into in order to fulfil the services rendered.

12 | **Doesn't POPI say 12 years of age, as long as the data subject understands? This obviously doesn't stand for the account.**

There is no reference to 12-year-olds in POPIA.

13 | **If the main member is not available to sign a patient information form, will an email from the main member suffice?**

It would be preferable to obtain a signature from the main member, but where this is not possible, there needs to be evidence of an attempt to obtain consent.

14 | **Regarding previously treated/seen patients, is it acceptable to send out emails to inform them that you are now POPIA compliant. Do you need written acceptance from patients?**

You can send out your privacy statement which details your practice's approach to POPIA which will inform your current / "old" patients how you treat their personal information.

15 | **In a university where research may be done retrospectively, how do we get consent for that?**

Should there be any PI or SPI contained within the data set, it is highly recommended that any personal information be de-identified to such an extent that any attributes in the data cannot be used to identify the data subject. De-identified data would then not be subject to the conditions of the Act. Where this cannot be done, you would need to obtain the data subjects' consent and give them an opportunity for them to opt-out of such research. If this is not possible, the responsible party needs to ensure that security measures are in place to prevent any personal information falling into the hands of an unauthorised party.

16 | **Does the consent form need to be in more than one language? Or is English OK?**

There is no bespoke legislation stipulating that the consent form needs to be in multiple languages.

Access and sharing of data

17 | **How does the act apply to locum tenens, especially over a weekend where one would hand over in-patients?**
The patient should grant consent to the practice more broadly to avoid difficulties with data sharing when locums are in attendance. The terms included in the main practitioner's contract with the locum should cover POPIA related matters. This should then be considered as part of the contractual agreement entered into in order to fulfil the services being rendered.

18 | **I offer a mobile therapy service. I don't have rooms or colleagues. All patient information is kept at my house. What do I need to implement to ensure security of information when there is no risk of other patients or colleagues accessing the info?**

The information should be secured in the event of other unauthorised third parties accessing the information (e.g. theft). The Act does not prescribe specific measures but proposes that the responsible party must put into place reasonable and appropriate security measures to protect the personal information in its possession or under its control. For example, the information should be kept in a locked cabinet.

19 | **If a patient's information or file needs to be handed over to another healthcare professional (e.g. if they move from one therapist to another), how does one ensure compliance with POPIA in terms of this?**

The privacy statement should include a clause or clauses which enable information to be shared by practitioners within a practice, as well as between healthcare professionals with an understanding that it will be used for the purpose for which the information was originally obtained. This should then be considered as part of the contractual agreement entered into between yourself and the patient.

20 | **If you sell a practice how does this affect the patient information? In other words, do you need their consent to sell their information to a new practitioner or not?**

The privacy statement should include a clause or clauses which enable information to be shared by practitioners with other practitioners (including in the event of a sale) with an understanding that it will be used for the purpose for which the information was originally obtained.

21 | **Does POPI still apply after death and if so, how?**

POPIA only applies to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.

22 | **If the healthcare professional or bureau want to do a query with the medical scheme on an account via email, do you need to attach the signed patient consent, otherwise you won't be helped?**

Proof of patient consent is not required. The sender's email address will be first be verified against the email address on record before a response is provided. If the email details do not match, the response will be shared, but to the email address on record.

23 | **If a practice requires blood results prior to administering treatment to patients from labs, can this be done without written consent from the patient, as the bloods are required in order to render services?**

If the collection of blood samples relates to the eventual rendering of the services, the purpose/specification should be made clear to the patient upfront. This should then be considered as part of the contractual agreement entered into in order to fulfil the services to be rendered and that providing the blood results is a requirement.
When a patient goes to a pathology lab, they fill out a form and sign this. If the pathology lab's terms and conditions include a privacy statement where the patient consents to sharing information with other parties (e.g. referring doctors), then there should be no issue with information being shared between different practice types.

24 | **If a secondary treating doctor requires results for a patient, can a practice release these results, even though the secondary treating doctor is not the initial referring doctor, without written consent? Please comment on referrals for e.g. x-ray or specialist?**

The practice may include conditions within their privacy statement to make patients aware of the sharing of their personal information with an authorised party in order to render appropriate treatment. Practices should make the patient aware that they will be sharing their personal information and special personal information with a third party to provide the required care. If the patient refuses this sharing, they need to be made aware of the implications.

For any kind of medically-related referral (e.g. psychologist to psychiatrist), the referring practitioner should ensure that the necessary consent has been obtained by the data subject (patient) to share information with another practitioner when the referral is related.

25 | **Please comment on sharing information, x-rays, pathology pictures etc. as well as using apps such as Whatsapp and/or the use of Whatsapp where healthcare practitioners share information regarding patients. This is a quick way to update each other post a consult, e.g. a psychiatrist has seen a client and wants to give feedback to a psychologist. As a psychologist, there is usually a fair amount of communication from/with patients on email and even Whatsapp - if this information is being shared directly with the 'data subject' and not third parties, I presume we still need to implement the same level of security on such correspondence to prevent breaches?**

WhatsApp is not considered a secure means of transmitting information between parties. Thus, an alternate solution should be sought in-order to share such information.

26 | **When a patient is admitted to hospital for emergency care, various individual private practitioners may be involved in treatment. It may not be practical to obtain consent prior to such treatment. Is there a reasonable period available to obtain such consent, following initial treatment?**

The health practitioner will be exempted under section 32 of the Act when it comes to the proper treatment and care of the patient in these circumstances.

27 | **Does this affect sharing of ICD-10 codes between healthcare professionals and Discovery and also information in PMB applications?**

The POPI Act refers to any special personal information, which would include diagnosis codes (ICD-10 codes). This type of information can continue to be shared by healthcare professionals and Discovery but due care must be taken to ensure it is protected when shared.

28 | **Does a bookkeeper also need to sign a privacy statement?**

A bookkeeper should only have access to any information that relates directly to their function. A practice/practitioner will need to ensure that there is a contractual arrangement between yourselves and your bookkeeper, that includes a clause/s related to the privacy of information and how this is shared.

29 | **Regarding de-identifying data, who, besides the practice, must be informed?**

If a formal request is made by a data subject to delete or de-identify their data, they should be given feedback once this is completed. When data is de-identified for general purposes or after an agreed period of retention, the affected data subjects do not need to be informed.

30 | **Would 'informal' communication with patients on email (e.g. therapy patients sending emails about something that happened) also need to be subject to a level of password protection or encryption as one needs to with third parties etc?**

Where an email being sent contains any 'special personal information' it must be encrypted. If a patient sends you/your practice any information, it would be up to the individual if they wish to encrypt it or not.

31 | **Regarding the mental health profession, how would I go about sharing information to a school after seeing a child?**

It should be clear to the patient parent/legal guardian (assuming the school child is younger than 18 years of age) the purpose of sharing this information upfront. This should then be considered as part of the contractual agreement entered into in order to fulfil the services rendered.

32 | **We had a meeting with some senior hospital staff and management, with regards to changes they should expect in the next few weeks, with security changes, the agreement and ETC. The biggest "pain" they had, is the removal of generic logins and ICU and PEADS for example. The stated that they have several physicians attending to several patients in**

the same, mostly in a secure room. Having to log off and on, would be an annoyance and they didn't see leaving the screen open as big risk. What would your response be to this?
The information officer of the responsible party would be responsible for the access to information. The doctors would need to consider who has access to this information (e.g. if all the patients are being cared for by the same doctor and set of nurses, as long as no other patients or visitors could see this information, then they would not need to log off for every patient).

Storing and retention of data

33 | **Is storing reports on the cloud considered secure and how does one then access/put contracts in place with these providers? I would personally rather keep it on my computer; apparently "the cloud" is in the UK?**

Information being stored in the cloud is as secure as the providers of these services make them. Since it is in their interests to ensure their services are secure, they do endeavour to provide high levels of security. The terms and conditions of their contracts should be carefully considered and understood before entering into contracts with these providers. While many of the providers do store data overseas (e.g. Ireland), some are opening up data centres in South Africa to overcome the issue of data transfers outside the borders of South Africa.

34 | **Online/ Video consultations: what the best practice between recording the consultation and not recording? If doing online consultations on Zoom would this be acceptable? And how does this pertain to security of online consultations?**

In order to record a consultation, the practitioner must obtain consent from the patient – irrespective of the online video conferencing solution used. The purpose of recording must also be understood and explained. The recording of the consultation should also be secured by storing the recording securely on the solution platform or by downloading the recording and storing it securely on a file server with security controls in place.

35 | **If one keeps patient files/notes on a laptop to which no one else has access and which is password protected, would one also need to password protect/encrypt all folders/files themselves?**

For files on a laptop which no-one else has access to and which is password protected, files and folders do not need additional encryption or protection. However, when files are shared which include personal information or special personal information, these files should be encrypted or protected.

36 | **Would storing reports, patient info, etc. on a digital platform like OneNote etc. be sufficient (it is password protected)?**

Yes – a digital platform which is password protected would be sufficient to store information of a PI or SPI nature.

37 | **Does the retention of patient data also apply to children?**

Yes, but it will be subject to your retention policy. The HSPCA recommends that children's information be kept at least up to the age of 21. For more information visit:
https://www.hpcsa.co.za/Uploads/Professional_Practice/Conduct%20%26%20Ethics/Booklet%209%20Keeping%20of%20Patient%20Records%20September%20%202016.pdf

38 | **Data retention: Does this only apply to inactive patients? If patients are ongoing, must one destroy information that is 6 years old?**

Yes – only for dormant or inactive patients. For ongoing patients, information older than 6 years (or the period you wish to retain records for) can be retained for the duration that the patient is active. Any records containing Personal information (PI) must not be retained any longer than is necessary for achieving the purpose for which the information was collected. Unless there is a retention period required by law or that the record is required for other lawful purposes. The HPCSA provides specific guidance on the retention of health records for health practitioners. Other industry codes or Acts would need to be taken into account regarding the prescribed period for retention of records when it comes to other aspects of practice management, including but not limited to the Tax Administration Act, Labour Relations Act, etc.

39 | **Do we have to keep children's records until the age of 21 or just for 6 years?**
The HPCSA advises up until the child reaches 21 years of age.

40 | **Please could you clarify if you should shred patient files and information about a patient that is no longer at your practice, even if the recommended 6 years hasn't lapsed?**

Any records containing Personal information (PI) must not be retained any longer than is necessary for achieving the purpose for which the information was collected. Unless there is a retention period required by law or that the record is required for other lawful purposes. The HPCSA provides specific guidance on the retention of health records for health practitioners. Other industry codes or Acts would need to be taken into account regarding the prescribed period for retention of records when it comes to other aspects of practice management, including but not limited to the Tax Administration Act, Labour Relations Act, etc.

Loss of data

41 | **What happens if the office is broken into, or your car is stolen, with patients' files in it?**

In the event of a security or information breach, where personal information has been compromised, the Information Regulator as well as any parties whose personal information has been accessed or acquired by an unauthorised party must be notified. The Act provides specific detail on what the notification should contain (See Section 22 – Notification of security compromises). Where applicable, the South African Police service should also be notified.

42 | **A follow on from the question about an office break in - if there is a break in and things are disturbed such that no files are stolen but you have no way of knowing what information about patients might have been 'accessed' / seen - would this still need to be reported to information regulator, police, and patients?**

It is recommended that a prudent approach be taken and therefore is there is any concern that information may have been accessed (but not removed), this should be logged as a data breach and the necessary processes followed to report the incident.

43 | **Does reporting data breach to regulator also apply to stolen cell phones? How do you secure your clients telephone numbers on your cell phone? If it is stolen?**

In the event of a security or information breach where personal information has been compromised, the Information Regulator as well as any parties whose personal information has been accessed or acquired by an unauthorised party, should be notified. You should ensure that you have the necessary security measures in place on your device e.g. secure passwords; up to date antivirus software etc. In addition, the necessary technologies should be in place on a mobile device to ensure that if the item is stolen that all/any information can be wiped clean and thus removing all access to the perpetrator.

44 | **How about when computer maintenance is being done?**

Where any maintenance is taking place, where the person/s doing the maintenance may obtain or have access to any personal information, measures need to be in place to ensure that none of the personal information is compromised in anyway and that the person/s doing such maintenance has entered into an agreement which includes POPIA related clauses.

Debt collection processes

45 | **How does the act apply to debt collectors?**

The Act applies to any private and public body. However, the Act should also be read in conjunction with other Acts, such as the National Credit Act, Consumer Protection Act etc.

46 | **What happens in terms of handing over bad debt?**
The POPIA Act must be read in conjunction with other Acts e.g. National Credit Act.

47 | **What about using next of kin details for debt collection?**

The privacy statement is a key document to protect the practitioner regarding collection of outstanding debt. It should be drafted to include the right to share next of kin data with operators / or authorised third parties in order to recover monies owing to a practice.

48 | **Does a debt collector qualify as a 'third party'? Do I need to ensure they comply to the act?**

A practice should enter into an "operator" relationship with a debt collector in order to protect PI / SPI they may share with them in order to collect outstanding monies.

Destroying patient information

49 | **What are the pre-requisites before shredding dormant patient file?**
Any records containing Personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected. Unless there is a retention period required by law or that the record is required for other lawful purposes. The HPCSA provides specific guidance on the retention of health records for health practitioners. Other industry codes or Acts would need to be taken into account regarding the prescribed period for retention of records when it comes to other aspects of practice management, including but not limited to the Tax Administration Act, Labour Relations Act, etc.

50 | **Is the practice required by law to shred patient info if not being used after 6 years? - if still maintained in a secure environment.**

Records containing personal information may be retained for periods in excess of a specific period for historical, statistical, or research purposes. Provided there are appropriate safeguards against records being used for any other purposes. This does create additional risk, in that the responsible party still needs to comply with the Act whilst the records are under their control. The HPCSA provides specific guidance on the retention of health records for health practitioners.

51 | **If a member asks you to delete information, do we do this? Can a patient's request to delete (de-identify) records override the legal requirement to retain medical records (e.g. for 6 years)?**

The HPCSA provides specific guidance on the retention of health records for health practitioners. The practice must ensure that they follow this guidance and any other applicable legislation.
Other industry codes or Acts would need to be taken into account regarding the prescribed period for retention of records when it comes to other aspects of practice management, including but not limited to the Tax Administration Act, Labour Relations Act, etc.

52 | **How does a practitioner delete/destroy patient paper files legally after HPCSA's proposed storage period?**

They would shred the paper files which have been identified as exceeding the HPCSA's retention period (provided the practice has agreed to this retention period).

Other

53 | **What will be the best way of sending patients claims through to the medical aids? Does anything in particular need to be taken into account with sending accounts to Discovery?**
A practice should ensure that any communication sent to a medical aid administrator (e.g. Discovery Health) is sent securely. This can be done using PMA and B2B software where the provider has entered into a contract with the software provider on an operator basis.

A patient can use existing functionality on the Discovery app, which allows the patient to submit a claim securely via the Submit a claim functionality under the Medical aid tab.

54 | **Would claims or invoices then need to be encrypted in email form? Or are emails generally considered to be secure enough?**

A data subject is not required to formally secure a claim or invoice sent to Discovery. However, the data subject can elect to secure the email with security features in their email. If they elect to encrypt a PDF image with a password, they will need to find a way to provide the password to the recipient of the claim or invoice.

55 | **If HCP sends an encrypted statement (with ICD-10) to a patient, how will the patient be able to send the statement to Discovery to claim?**

A patient can use existing functionality on the Discovery website and App, which allows the patient to submit a claim/s securely via the "submit a claim" functionality.

56 | **What about patient reminder emails? For example: This is a reminder that you are due for a dental check-up etc.**

If the email includes any personal information which could identify the data subject, then it should be secured. Alternatively, a message containing minimal details in the reminder, but is sufficient to convey the required details of the reminder can be sent to the patient. E.g. "Dear Andrew, this is a reminder of your dental check-up, on 1 May, at 14:30" instead of "Dear Mr Andrew Smith, this is a reminder of your dental check-up, on 1 May, at 14:30 at Smile Dental Clinic, 15 Long Drive".

57 | **Who can assist in helping me set up security on PC, email and cloud systems? What is best cloud for health practice to use?**

Any reputable technology company providing such services can assist. There are numerous cloud service providers which have a global presence which could be used.

58 | **Is Google mail, calendars regarded as secure enough? Is Gmail POPI compliant?**

Google which provides the Gmail platform and related services, endeavours to secure this platform based on the number of users globally and their need to protect their clients' information and their own reputation and business. It should be noted that Gmail is a generally accessible mail service and if staff in a practice receive information to such accounts to their own Gmail accounts, the risk exists that if the staff member leaves the practice, they will still have access to the Gmail account and patient information contained therein. Therefore, it is not recommended to use Gmail accounts for practice administration, but rather ensure that any email accounts provided to staff, are also managed by the practice and are deemed to be used for communications and the functioning of the practice.

Interacting with Discovery

We need to verify the identity of any personnel within the practice (e.g. practitioner, practice manager, receptionist etc) or working on behalf of a practice (e.g. Bureau) to ensure that we comply with POPIA when sharing information or gathering information.

Telephonic interactions

59 | What is the verification process when you contact the call centre?

You will need to confirm the following details:

- Full name
- Surname
- Identification number

Website login

60 | What do I do if I do not have a website login?

You need to register on our website in order to create a Discovery digital ID. To do so, please follow the steps below:

Go to www.discovery.co.za

- Click on Register
- Enter a form of identification to create a one-time pin (OTP)
- Select the communication channel (SMS or email)
- Enter the OTP you receive
- Create a username and strong password
- Read and accept the terms and conditions

If you are an existing Discovery client and have login details in your personal capacity, you will have access to different landing pages on our website. Login using your existing details, and then change the default "You and your family" in the top navigation bar to "Healthcare Professionals**".**

- Help with login details
    - For help with login details, please follow the steps in our "Trouble logging in?" section on http://www.discovery.co.za/portal/individual/login-help.

61 | How do I find the information sent to my secure inbox?

To access your secure inbox, follow the steps below:

- Log into www.discovery.co.za
- Select Healthcare professionals from the top navigation drop down
- Click on the Communication tab at the top of the page
- Select Personalised practice communications
- Select if you are acting on behalf of yourself (as a practitioner) or your practice.

62 | How to search for documents in your secure inbox

Your secure inbox includes the ability to search for documentation by following the steps below:

- Use the search tab to enter your patient's name or search for a document heading.
- All documentation in your secure inbox is ordered chronologically.
- You can define the date range for your search using the filter
- Select "Clear all filters" to remove the search filters

Privacy statement

63 | Is it possible that you upload the template Privacy Statement you have developed onto the Health Professionals site for us to download? Where can we get the Privacy Statement Guidelines on your website?

The privacy statement template is available upon request.

Find out all you need to know about POPIA and how to prepare

We have put together a series of POPIA podcasts and a downloadable 10-point checklist to help you and your staff prepare.