The Protection of Personal Information (POPI) Act FAQs

10	1. Who is the responsible party in respect of the information occupational therapy students collect from patients with profound intellectual disability and other serious disabilities who attend NGOs or NPOs? Students collect information about identifiable data subjects but might anonymize the information by using initials only. Because of the nature of occupational therapy, it will be possible in most instances to identify the patient based on the combination of other information, so de-identifying information is not possible. We are dealing with two issues: (1) the legal ground to process in my view would be for training purposes primarily, and secondly providing OT services in keeping with the students' level of education and training (as per the OT annexure to the HPCSA Regulations) this information and (2) the safekeeping of the information This is my worry. Whose job is it to keep the info safe, if we are processing it for educational purposes, but other people might want to process it for medical/custodial purposes? Does the work with these patients form part of the (practical) course work of the student to qualify for the degree? YES, Or is the student acting in his/her own capacity? NO. What consents do the competent person sign with the institution in which the patients are treated in respect of the course work of students and the use of their personal information and special personal information for this purpose? To date there has been no consents that I know of (nor the knowledge of my one colleague who coordinates the specific block I am worried about). Some of the placements are residential facilities, but I do not know whether the facility lets the curator (used in its broadest and most encompassing way, not necessarily limited to formally appointed persons) know that students will be working with the patients. When I was responsible for this fieldwork about 6 years ago, we got "high level" permission for the students to be there, but it was never specific for a specific person; and we organized that a senior official of the institution allocate patients to the students – it was never a question of arrive and then just grab patients. By "high level" I mean a senior person who was deemed authorized, gave permission for the students to come to the placement for fieldwork and either delegated the duty or allocated patients to the students themselves.

	As the students are not practitioners and are not running a business, I think it is safe to say that the University would be the responsible party for the personal information it gathers by means of the student work for academic purposes. The processing of the information would relate to ordinary personal information, special personal information (medical information), and if they work with minors, information about children.
	• We need to determine firstly whether the processing is for a legitimate propose – the answer is straight forward – yes, it is necessary for the training of students and the treatment of the patients.
	• Then we need to determine the legal ground for processing – section 32 allows a special exception for the processing of information about health and sex life by "medical professionals, healthcare institutions or facilities or social services (NGO?), if such processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned". The purpose, I would assume would be not only practical experience for the student, but in essence to treat the patient. The remaining issue is then whether the students are regarded as medical practitioners or whether the OT who supervises them plays that role. As the students are not registered yet, they would not be, but the supervisor would take responsibility and would, in my opinion, fulfil that role.
	• If my argument is correct, there is no need for consent to process the medical information, as the processing thereof is covered by section 32.
	• The problem is however not the processing as far as treatment is concerned, but for academic purposes.
	• We could look at the exception in respect of statistical or research purposes – if you can fit the academic work into that category, we do not need consent either, if there are safeguards in place.
	• Research purposes may be a tricky horse to ride. The DoH Guidelines pertain to 'research that involves living human participants' and require prospective and independent ethics review. While the DoH Guidelines apply to 'health research', this is broadly defined as all research which contributes to the knowledge of:
	  ○ biological, clinical, psychological, or social welfare matters including processes as regards humans.
	  ○ the causes and effects of, and responses to disease.
	  ○ effects of the environment on humans.
	  ○ methods to improve healthcare service delivery.
	  ○ new pharmaceuticals, medicines, interventions, and devices; and
	  ○ new technologies to improve health and health care.
	• I am not sure that educational purposes would fall within this definition.
	• Deidentifying where the identity cannot be linked to the data subject and the information cannot reasonably be reidentified, takes the information out the ambit of application of POPIA. Whilst your current method may not be effective, there are other ways, e.g. not using initials, but serial numbers which are kept separately, etc.

- If none of the above are workable, we would have to rely on consent which must be given by the competent person. The definition states that it would be any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child. I interpret that is a guardian by parentship of court appointment. POPIA does not deal with adults without legal capacity. In my opinion, it would be safe to deal with such persons in the same manner as children.
- I cannot see that the consent of the institution would be sufficient in the absence of a consent from the competent person mandating them to share the information with the University.
- The remaining option is to apply for exemption with the Regulator on the basis that it is in the public interest and offers a clear benefit to the data subject.

2. Who must consent to students processing these patients' information? Is it sufficient to get consent from the head of the organization, or must we get permission for processing from a guardian/curator/other legally competent/responsible person (e.g., parent)?

   Did the competent person give specific consent to the institution for processing information for academic proposes?

   I do not know the answer to that. I would assume NO, because the NGOs/NPOs are not part of the GDOH training platform and I do not know whether the University has MOUs in place with these facilities – since we are probably the only department placing students there, it is unlikely for MOUs to be in place. Which is in my view of course a whole other can of worms.

   The University only must process the information on legal grounds pertaining to its own processing and purpose, i.e., medical treatment and research purposes. The NGO remains a responsible party and needs to ensure that its sharing of the information with the University is lawful. It is advisable that proper MOUs are entered into between the University and the institutions to meliorate risk and these would probably contain mutual undertakings and indemnities.

3. Must we get expressed consent from a legally competent/responsible person to disclose this medical information to the NGO/NPO? I assume it is par-for-the-course for us to have to get expressed consent to disclose to the academic supervisor, who will be a registered occupational therapist.

   Did the competent person give specific consent to the institution for processing information for academic proposes? Same answer as above. Probably not.

The institution in any event needs this information to care for the patients and there would be an implied contractual right to obtain the information. Whether you require consent to share the information with the institution would depend on the relationship – if are you a private medical practitioner who treats patients independent of the institution, you would need consent to share the information with the institution, - where you treat the patients under auspices of the institution, no further consent is necessary (as in a hospital).

4. When we as an academic department do a risk analysis, is it sufficient to say for a risk that students will keep information on their computers which may be vulnerable to breaches, that we have instructed students a) not to keep patients' information on their computers, and b) told them to only submit patient reports for marking using initials, c) only submit reports for marking to an university-controlled, hopefully encrypted cloud-based platform? I am of the opinion that it will be virtually impossible for us to ensure that students do not breach patients' rights in terms of POPIA, so we will ALWAYS be in a position of likely breaching POPIA, and the statutory vicarious liability makes me a little worried.

   The answers to this would depend on who the responsible party would be as per question 1. Hence my question 1.

1. This brings us to the safekeeping of the information. The University as responsible party would be responsible to secure the information. Uploading to an encrypted platform is probably safest. As far as the student is concerned, this becomes a conundrum. The student retains the notes, names, information etc. on his/her laptop. Leaking thereof, hacking or even loss of the laptop, would be regarded as a data compromise. The University would be liable for damages or may be fined by the Regulator. The University needs to take reasonably practicable steps to avoid such events. I suggest you consider options such as:
   - Students sign an indemnity in favour of the University in respect of damages or fines in cases of a data compromise.
   - Implement rules that such information can only be saved on a secure University server with password protection and may not be stored on personal devices, alternatively devise a proper deidentifying or anonymising features to protect information.
   - Teach a class in POPIA awareness with the focus on this specific dilemma.

   A further issue is how long may the information be retained, for what purpose, on what legal ground and when and how must it be destroyed.

   The above are my opinion. There are no decided court cases or any such guidance. So, the interpretation of the Act may still change and we would have to rethink the solutions. I suggest you approach the legal department of the University and have this resolved properly.

9.	**QUESTION:** I wanted to ask you what the "POPI" obligations of a school and its teachers are. I often have teachers sending me pics or videos of kids I see without me asking for it. I am covered from my side but them? **ANSWER:** Schools are very much subject to POPIA and are at a very high risk if one considers the personal information they process. That means that when they send information to you, they must also comply with POPIA. If you would feel more comfortable about it, I suggest you have a discussion with the Head about the issue and ask them to ensure that they have consent before sending you such information on an unsolicited basis.
8.	**QUESTION:** Are we allowed to send the name of a child in the body of an email e.g. in response to a referral or must be always use abbreviations? If you send a questionnaire via email for a teacher to fill in, can you add the name of the child (no DOB) and send in word, or must your password protect it since it has the child's name on it? **ANSWER:** It is part of the medical process to get the information from the teacher. It is therefore in the best interest of the child to get the form filled out by the teacher. If you have the consent of the parent to approach the teacher, you are covered. Standard safety precautions ought to be: • Send the email to an address that only that teacher would have access to, i.e. not a general school email address. • Inform the teacher that the information should be protected and kept confidential to protect the school and the child; and • Only give enough information to allow the teacher to identify the child. •

7. **QUESTION:** I was audited by a medical aid last year.
The process was harrowing to say the least and unfortunately, I was not optimally assisted or supported by my peer review.
I was also advised to provide the MA with entire files of my patients.

The MA measured my time spent with a patient based on the amount and extent of the content of information recorded in my progress notes.
I am therefore quite concerned about what POPI guidelines caution us on, what is recorded and how this information is stored and who has access to the information.
What takes precedence POPI or the MA?

I was personally pained by my patient's information shared with me under our confidentiality agreement, which was then reviewed by an auditor, who to my knowledge was not a health care worker. I was also concerned that the information I recorded in my extensive note taking could have been construed by the MA as non-compliance and therefore placing my patients at risk of non-medical aid support because of this information reviewed by an auditor.

ANSWER:

1. **Medical Scheme Audits**
   Section 59(3) of the Medical Schemes Act provides medical schemes with the right to deduct any amount from any benefit payable to a member or supplier of health service where:
   - The amount was paid bona fide whilst the member or a health service provider was not entitled to the payment; or
   - Any loss has been sustained by the medical scheme through theft, fraud, negligence, or any misconduct.

   Some medical schemes see this as a manner to circumvent the duty to effect payments of all genuine claims within 30 days of receipt of the account. The fact is that Regulation 6 requires that where a medical scheme is of the opinion that an account, statement, or claim is erroneous or unacceptable for payment, to inform both the member and the relevant Service Provider within 30 days after receipt of such account and provide an opportunity for amendment and resubmission (within 60 days after it was returned). This does not allow them to suspend payment. If they choose not to use this procedure, they still bear the onus that the practitioner was not entitled to payment. In the absence thereof, they contravene the duty to pay within 30 days.

   The above presupposes that the medical scheme, who bears the onus, must set out and be able to prove that the medical partitioner was not entitled to the payment or that it suffered loss through theft, fraud, negligence, or any misconduct.

When a medical scheme wants to do an audit, it needs to inform the practitioner in writing on which grounds they want to do the audit and clarify any legitimate queries the practitioner may have. During an audit the scheme is entitled to access to any treatment record held or by a managed by the practitioner and other information pertaining to the diagnosis, treatment, and health status of the beneficiary, but such information may not be disclosed to any other person without the express consent of the beneficiary.

Payments to a practitioner cannot be suspended merely because an investigation is underway, or the outcome of an investigation is pending. The payment can only be suspended when the scheme is able to prove that one of the above events took place and they are able to prove what the quantum of the payment or loss is.

I do not want to go into the bullying tactics and intimidation used, but attach the guideline issued by the HPCSA in this regard.

2. **Patient Privacy Rights**
You are not entitled to share the medical information of the patient with the medical aid without the voluntary, express, specific, and informed consent of the patient of the patient (or a court order, etc). This has always been the position. See the Ethical Guidelines on Patient Records

> No health care practitioner shall make information available to any third party without the written authorisation of the patient or a court order or where nondisclosure of the information would represent a serious threat to public health (National Health Act (Act 61 of 2003)).

POPIA reconfirms this existing obligation.

My advice would be that should you ever be put in this position again, to:

- Ask for exact grounds supported by facts on which there is a reasonable suspicion that the scheme has paid money to you/the patient that neither were entitled to or that theft, fraud, negligence, or any misconduct took place.
- Ask for extension of the period in which you must respond on the basis that you want to seek legal advice.
- Contact your lawyer, OTASA and the HPCSA for assistance.
- Never make any concessions or sign an Admission of Debt just to make the matter go away. This is about more than money; you also may be admitting to misconduct which could cost you your registration with the HPCSA.

6.	**QUESTION:** I would like to have more information on how the POPI Act affects me as I am in the UK and do not practise anymore. I do have files from past patients in storage. **ANSWER:** POPI is only applicable to the processing of personal information within the borders of South Africa, or to personal information processed by companies domiciled in South Africa, although they are outside the borders of South Africa. If Carli operates in the UK, she will not be subject to POPI, but would be subject to the GDPR. The GDPR is applicable to activities taking place within the EU (and UK) and to activities taking place anywhere in the world in respect of citizens of the EU (and UK).
5.	**QUESTION:** Please can you confirm if we do have to fill this attachment (Application form for authorisation to process personal information of children) in as part of the POPI Act. If so, also not sure if we only must be complete by December)? Also, not sure if there's any standard answers (unsure of certain questions)? I have my own paediatric practice at a school (work on my own); I don't share information overseas etc. I have complied with the rest of the other POPI Act documents, consent forms etc. **ANSWER:** If information about children needs to be sent cross border, one may get consent from parents, ensure that there is adequate protection in the country of destination, in exercising a contractual right or obligation, etc. Only if there is no other option, this form is used to apply for specific pre-authorisation from the Regulator to send information cross border. It is a last resort. If no information is sent cross border, no such application would be necessary.

4.	**QUESTION:** Is it possible to ask the compilers of the document whether it will be possible for them to compile a one-page POPI consent form for us? At present it is 3 and a quarter pages long. There is no way that my patients will read a three-page document before signing. I would like to reduce the length but require some guidance regarding what must absolutely remain and what bits I may remove and just explain verbally. If I can ask each new patient to sign one document, it will be much easier to be compliant. **ANSWER:** The current from is very complete. It could be possible to reduce the length of the form, but that would mean redrafting it entirely. I would have to quote on that. It would help if the member can tell us want parts are not relevant. (pieter@griesselconsulting.co.za)
3.	**QUESTION:** I currently offer services to health facilities, and they provide me with the patient details i.e. medical aid details, personal details, authorisation numbers etc. Please confirm if I need to have anything in place to ensure I am POPIA compliant? **ANSWER:** Ashley would not stand in an operator relationship with the health facilities, as Ashley would process the information for her own purposes, i.e. to treat the patient. She would therefore be a Responsible Party in her own right. She only needs to have her own POPI compliance in place, have consent where necessary, sign contracts as necessary and protect the information. The health facilities individually have a similar duty, and one would hope that that have consent to refer and share the personal and specifically special personal information with Ashley. She is entitled to ask whether consent is in place, but there is no duty on her to police the health facilities. If she feels exposed, one could attempt to ask indemnities from them, but due to the unequal bargaining power it is unlikely that they would sign such indemnities. She could perhaps ask the facilities to see their Privacy/Data Protection Policies.

2.	**QUESTION:** I would really appreciate a basic guideline for compliancy. **ANSWER:** We have an e-book available on this topic - Practical Compliance – Steps and checklists for a comprehensive POPIA compliance framework @ R450 ex VAT. Contact info@griesselconsulting.co.za for more information.
1.	**QUESTION:** Does anyone make use of overseas assessment tools for example the Cambridge Brain Sciences (CBS) assessment or online rehab tools such as Brain HQ or Cognifit? Just wondering how to state that our practice is therefore using Transborder Flow of data subject information in our policies and PAIA manual? **ANSWER:** We must first determine whether there is any flow of identifiable personal information, i.e. can we identify the data subject by looking at the data. • If no, the information is not covered by POPI. • If yes, we would need comply with one of the following: o The foreign country must have laws that provide adequate protection like POPIA. o Or, if not, there are binding corporate rules that provide adequate protection. o Or, if not, there must be an agreement between the sender and the receiver that provides adequate protection. o Alternatively, the data subject/parent can give consent. o I some case one could argue that the transfer is necessary for the responsible party to perform in terms of a contract. Obviously, consent would be by far the easiest. You would therefore have to have the patient (or the parent) sign consent to allow you to share specified information with Cambridge Brain Sciences, Brain HQ or Cognifit, indicating what the information is that would be shared and what it would be used for. Patients/parents may however be informed about data protection and may want to know whether the information would be adequately protected. Should these institutions be based in the UK or EU, they would have a data protection undertaking in place about protecting the information. These countries fall under the GDPR and would have adequate protection in place. If not, one might want to obtain a copy of their data protection policy to present to patients/parents.