POPI ACT COMPLIANCE CHECKLIST AND TEMPLATE PACK FOR DENTISTS

SADA
THE SOUTH AFRICAN DENTAL ASSOCIATION

The South African Dental Association **(SADA)** NPC

POPI CHECKLIST – AT A GLANCE

Step 1: **AUDIT**	Do an audit of all of the existing information being processed by your business: What information is being collected? ☐ How is information being collected? ☐ For what purpose is this information being collected? ☐ Where is this information stored? ☐ Review agreements you have with others, especially looking at what the third party's responsibilities are regarding the information you share with them ☐	**Step 2:** **CLEAN UP**	Remove any information that is no longer required by the business, including information relating to: Customers who are no longer using your services ☐ Customers who have not consented to being on your database ☐ Employees who have left the Business ☐	
Step 3: **WRITE UP PROCEDURES**	Put in place "best practice" procedures for how you want to move forward: What are our reasons for collecting information? ☐ How do we intend to safeguard that information? ☐ How will we respond to our customers if things go wrong? ☐ For how long will we hang on to information? ☐ How will we destroy information that we no longer require? ☐	**Step 4:** **COMMUNICATE**	**Communicate your processes to your users. Draft the relevant documents that your customers will need for knowing what's happening to their information. All these documents should be in clear, plain language and accessible to the end users. Some of the documents you might want to look at include:** Consent forms ☐ Privacy policies ☐ Cookies notices ☐	

Step 5: **T R A I N YOUR PEOPLE**	Train everyone in your practice. Even the most robust compliance plan will fail if the people on the ground are not equipped to implement it. Training and education can never be a once-off exercise, and the practice should have some idea of how often and in what way constant training needs to take place. The best way to ensure compliance with your obligations would be to train your people to: Recognise when they are dealing with personal information ☐ Understand what their own responsibilities are within your practice ☐ Know who to contact if they have questions or concerns ☐			

Important things you should know about POPI				

Who does POPI apply to?	• The Act applies to anyone who is processing personal information including dentists.
	• "Processing" includes collecting, recording, storing, or using information.
	• "Information" includes names, addresses, biometric information and anything else that identifies a person.
	• POPI does not apply to any processing of personal information that is used only for personal purposes i.e. not as part of a business or in a public space (like social media).
	• In a nutshell, POPI will apply to dentists who need to put processes in place to ensure that they are compliant.
		How do you get POPI compliant?	• Compliance is much more than just having a privacy policy in place (but, this is certainly better than nothing).
			• The first step is to understand what your responsibilities are in terms of POPI.
			• More importantly, you need to understand:
			  ○ what personal information you are collecting for your business
			  ○ how it is being used
			  ○ for what purpose you are using the information you are collecting.
			• This is not a once-off exercise. You need to constantly monitor your business and make sure that everyone within the business knows what they can or can't do,	

			and what the implications are of not complying.	
What happens if I don't comply?	• First of all, you could be breaking the law and face criminal liability or a hefty fine. • For less serious offences, the maximum penalty would be a fine, imprisonment for up to 12 months, or a combination of the two. For more serious offences the maximum penalties are a R10-million fine, or imprisonment for a period of up to 10 years, or a combination of both. • The Information Regulator could also order you to take specific steps within a specified period including ordering you to immediately stop processing personal information. • You could also be ordered to pay a monetary amount to the person whose personal information has been abused. • Over and above all this, there is also reputational damage to your business, as customers may not be very likely to want to engage with any business that is abusing their personal information.	**What is a privacy policy?**	A privacy policy is a roadmap for your customers to see: • What type of information you are collecting about them; • For what purposes you are collecting this information; • How their information will be used and protected; and • What they can do about changing or deleting their information. A privacy policy is just one step in ensuring that you are compliant with POPI. You could certainly have a privacy policy in place and still not meet all your obligations under POPI, which is why it is important to conduct a full audit of your business to see where your gaps are.	

How do I conduct an audit on my business?	• An audit is the first step in performing a "Gap Analysis" on your business.
	• As a starting point, you would need to sit down and look at things from your customer's experience.
	• Once you have established what information you are collecting, you would then need to look at how you are collecting this information.
	• You might be collecting information:
	  ○ automatically without asking your customers for their consent (the most usual example of this is when you collect information on your customer's browsing behaviours); or
	  ○ directly from your customers with their consent (like asking them to fill out their details in an order form or sign up to a mailing list).
		What are my obligations in terms of POPI?	• The Act requires that all personal information needs to be processed lawfully and in a reasonable manner.
			• This means that you are not required to have iron-clad fool proof processes in place, but that you must be able to defend your actions if called upon to do so.
			• In a nutshell, you need to position your business to be able to say "We did everything that could have been reasonably expected in the circumstances to comply with our obligations". It will not be good enough to say that you weren't aware of your obligations or that it wasn't your fault that personal information was abused.	

	• Once you have a grasp on what information you are collecting, you need to work out:
	  ○ what your customers know about where their information is being stored, sent, and used for.
	• You are now in a position to compare what you are currently doing against what your obligations are in terms of POPI, and to then address your "Gaps" by making the necessary changes to your business activities to bring it in line with POPI.
			• So, what does it mean to process information "lawfully and reasonably"?
			• First and foremost - you can only collect information for a:
			  ○ Specific
			  ○ Explicitly defined
			  ○ Lawful purpose
			• And you must communicate all of these to the person whose information you are collecting.
			• For example, you cannot collect email addresses from your customers for the purpose of issuing their invoices, and then use those email addresses to market your new business products to them, or worse, sell that information to a third party for that other business to contact your customers.
			• The important thing to remember is that, as long as people know and understand what they are signing up for, you can continue your business with much less stress. Put differently, if you tell your customers that you would like to send them information about upcoming products or partner services, and they provide their consent for you to do this, you're pretty much covered.
			• That said, you must give people the opportunity to "opt-in" to these communications and sharing of their information.	

CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

STEP 1 – APPOINTMENT OF INFORMATION OFFICER	All practices will have to appoint an Information Officer and deputy information officers, if required or applicable but not necessary Register your Information Officer and deputy information officer with the Information Regulator on their electronic portal https://www.justice.gov.za/inforeg/docs.html Complete Online form (regulator presently working through technical glitches) The Information Officer's Registration Form is available on their website for completion and submission by e-mail (under Documents tab, under "Forms") https://www.justice.gov.za/inforeg/docs/InfoRegSA-eForm-InformationOfficersRegistration-2021.pdf	The Information Officer are to ensure that they comply with the prescribed responsibilities, ensuring that: • They develop a framework to ensure compliance, implementation and monitoring. • a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information; • a PAIA manual is put in place or updated, as prescribed in sections 14 and 51 of POPIA; • internal measures are developed together with adequate systems to process requests for information or access thereto; and • internal awareness sessions are conducted regarding the provisions of POPIA, regulations made in terms of POPIA, codes of conduct, or information obtained from the Regulator	Who is the Information Officer in a dental practice? The head of the business or practice is its Information Officer. In a dental practice this will be: • solo practitioner owner • incorporated practices –sole director or a director designated by the practice with second director as deputy information officer • partnership – the designated partner with fellow partner being the deputy information officer • association practice – all practitioners operating in their own names will have to register themselves as information officers. A practice may also appoint a Deputy Information Officer to assist the Information Officer who may be the employee or practice manager. If you also operate a separate legal entity that owns and leases equipment to the practice, that separate entity must also appoint an Information Officer. The Information Officer must be trained on POPI Act and show this record to the Regulator when required.	
STEP 2 ASSESS THE CURRENT RECORDS OF PERSONAL INFORMATION IN YOUR PRACTICE	Assess and compile a list of the personal information you currently process in your practice	**Possible Sources of personal information in a dental practice** • Patient Information Sheet for new patients • Appointment diaries (electronic and paper) • Appointment diaries on website • Patient file – front cover, clinical notes, technician accounts, x-rays with patient identification, reports, pre-authorisation, reports, motivations, consent forms, health questionnaire, e-mail complaints or request for information from patient etc.		

		• Referral to dental technician (workslips) • Referrals to specialists and reports from them • E-mail correspondences from and to patients and other providers • Medical scheme information, submission of claims, motivation and pre-authorisations, prescriptions etc • Details of dental suppliers, IT service providers, switching companies, other contractors whom you pay on a recurring basis. • Employees files • Financial information of debtors (other than patients) and creditors • Information on websites, social media platforms where cookies are used or online appointment, • Personal information on cellphones • Whatsapp and other apps • Computer records on hard drives and servers including cloud storage of patient files or lists • Correspondences with regulators such as HPCSA, SADTC, SAHPRA, CMS etc		
STEP 3 –AUDIT CURRENT PROCESS USED TO PROCESS PERSONAL INFORMATION (COLLECT/RECORD/ STORE AND DISSEMINATE DATA)	Evaluate the current processing activities that are being undertaken by the business involving personal information and/or special personal information. Create a detailed list/schedule of these processing activities setting out: • where the information is being processed; • what type of information is being processed; and • by whom the information is being processed. Evaluate all service agreements relating to data processing and update your contracts accordingly	Practitioners will have to assess if too much information is held and if level of detail is far more than required for providing services to patients. For example, in case of implant suppliers, patients may be identified only by their name or reference number for the purposes of return, identifying component, repair, replacement or refund. For example, in the case of technicians, only the patient's name and a reference number need to be used on the workslip for the technician. If technician is claiming directly from patient or scheme, the technician will obtain personal information or obtain consent from patient to furnish personal information.		
STEP 4 – REVIEW 8 CONDITIONS OF PROCESSING	**1 ACCOUNTABILITY** **Who is responsible?** **s 8**	**Appointment of Information Officer discussed in Step 1 above** The first condition places the blame squarely on the shoulders of the data processor and no one else. Doing so		

PERSONAL INFORMATION ITO POPI ACT		makes it easier to investigate, cite, and punish violations of the law. Consequence of non-compliance to the POPIA could result in fines of up to R10 million and/or up to 10 years in jail time for some offences.		
	2 **PROCESSING LIMITATION** **What info can you collect and do you have permission?** **ss 9 - 12**	Have you identified the specific method or tool you will use to collect the identified personal information? For example: automated forms, email, whatsapp, social media, website, manual forms etc Personal information must be collected directly from the data subject (patient), unless: a) the information is in a public record or made public by the patient; b) where patient is a child, that child has consented or parent or guardian has consented to collection of information from another source; c) information collected from another sources will not prejudice a legitimate interest of the data subject; d) where collection from another source is necessary— i. for maintenance of law ii. to comply with an obligation imposed by law iii. for any court proceedings or tribunal which has commenced iv. in the interests of national security or v. to maintain the legitimate interests of the patient or of a third party to whom the information is supplied; e) compliance would prejudice a lawful purpose of the collection; or	**National Health Act** **s15. Access to health records** (1) A health worker or any health care provider that has access to the health records of a user may disclose such personal information to any other person, health care provider or health establishment as is necessary for any legitimate purpose within the ordinary course and scope of his or her duties where such access or disclosure is in the interests of the user. As long as you are processing personal information in the context of your ordinary day to day practice or the treatment and management of patients, you are not barred by the prohibition that applies as a general rule **What justifies processing?** Consent ito POPIA -means an **voluntary, specific and informed expression of will** in terms of which permission is given for the processing of personal information **Consent is only one justification.** It is recommended that dentists obtain consent in their daily practice. • It is easy to prove in the event of a dispute • All parties know where they stand	**MULTI DISCIPLINARY TEAMS** It is permissible in the ordinary course of a dental practice to deal with personal information. What about information that is shared or moved around and at the same time be compliant with POPIA. If you are discussing with the patient the sharing of personal information that you hold with your colleagues (for specialists referrals or second opinions), technicians, medical schemes, debt collectors, services providers, dental suppliers etc, if the patient has agreed to them involved in their care or for you to collect your fees, then there is no problem. Get consent in writing from them If the patient is unable to consent, but he/she requires treatment from a colleague, and you need to discuss their case, this would be also fine as it is for a legitimate interest and necessary for the proper treatment and care of the patient. When it comes to sharing information with a medical scheme, you should have informed consent of the patient (or the person authorised to consent) for all information shared with the scheme. While there might be exceptions, it is best to ensure

f) compliance is not reasonably practicable in a particular case.

Is personal information collected by your practice directly from:

- □ Patient/s
- □ patient's parent or guardian
- □ creditors
- □ suppliers
- □ contractors
- □ dental technician
- □ employees
- □ medical schemes/managed care companies
- □ any other source or party the practice is dealing with

Assess do you have permission to collect the personal information

- It is part of normal everyday practice

You can collect data from a third party if it is already in the public record or Data Subject consents to it.

USE THE TEMPLATE SADA CONSENT FORM SUPPLIED

What justifies processing?

- Processing is necessary for the performance of your contract with the patient;
- Processing complies with an obligation imposed by law on you as practitioner;
- Processing protects a legitimate interest of the patient;
- Processing is necessary for the proper performance of a public law duty by a public body; or
- Processing is necessary for pursuing the legitimate interests of the practitioner or of a third party to whom the information is supplied.

appropriate and proper consent.

ICD-10 Coding

- Previously the HPCSA "strongly recommended" getting a patient's written consent before disclosing information to a medical scheme.
- Such written consent can be a "once-off" applying to patient contact concerning the same or a similar clinical condition, but subject to verbal reminders and confirmation (which should be documented in the patient's records).
- When the patient presents with a new condition, it
- will be necessary to obtain new written consent although the HPCSA booklet makes no such recommendation.

WhatsApp Groups

- There is uncertainty on how the Information Regulator intends dealing with WhatsApp in the future.
- WhatsApp messages are end-to-end encrypted, which is good, but the data is stored outside of South Africa which may not necessarily accord with POPIA.
- If you have a general WhatsApp group with your colleagues or dental group, most of whom will not be involved in patient's care:
  - Sharing a patient's personal information with people who do not need to see it is problematic
  - It may be that the Regulator will look kindly upon this practice (Legitimate interest/necessary for treatment), but we do not know yet

				○ Anonymise patient names as far as possible ○ Obtain consent on admission and treatment discussion stage.
	3 PURPOSE SPECIFICATION **Is the info relevant, up to date and serving the correct purpose?** **s 13 & 14**	Have you identified all the personal information that you currently require for your practice? The information must be collected only for a "specific, explicitly defined and lawful purpose" related to one of your normal activities. In case of dentists, it is to provide dental services, continuation of care, medical history submission of claims to schemes, sub-contract a technician or dental supplier etc. Is the patient (DS) aware of this purpose? One can also cite the National Health Act and the HPCSA ethical guidelines on record keeping, retention of records etc	**Retention of Records** POPI requires that you cannot hold onto records forever. Once you no longer need them for the processing purpose, you no longer have a right to keep them unless: • Retention is required by law (for example the Health Professions ethical rules on retention of records provide that you must retain them for at least 6 years after they become dormant or in case of children at least 3 years after they turn 18 years. Other legislations require a much longer retention period. Once you no longer have a right to hold onto the personal information or file, you must "destroy or delete...or de-identify" the record as soon as practical. The process should render the data irretrievable. Any destruction should be such that it cannot be reconstructed.	
	4 FURTHER PROCESSING LIMITATION **Has the info purpose or processing changed?** **s 15**	POPIA requires you to consider the relationship between further processing and the original purpose, the nature of the information, potential consequences of further processing, how you collected the data, and any contractual rights. When processing further information, you must consider the initial purpose of collecting the information was.	Unfortunately, POPI does not provide a defined list of what will constitute “compatibility”. It rather answers the question in the negative. In practical terms, this means that you cannot collect personal information for a specifically defined purpose, and then use it for a purpose that is not linked to the original purpose at all. By way of example: As dentists, you collect information about your patients. If you	

		You may process further information if it's necessary for the health of the patient or another individual. Below is where the practitioner can argue that the further processing will not be incompatible with the original purpose for processing: Consent If the patient consents to the further processing, the practitioner can further process it. Public record Its allowed if it is contained in the public record or patient makes it public (for example Facebook). Maintenance of the law If the further processing is necessary to maintain, comply with the law, or for court proceedings, or national security, it will be allowed. Health or safety threat If the further processing is necessary to prevent or mitigate a threat to public health or safety or the life/health of the data subject or another individual, further processing is allowed. Historical Statistical and Research purposes Further processing is allowed for these purposes, provided that the information is not in identifiable form. Regulator Exemption If the Regulator exempts it.	collect information for purposes of a specific dental treatment, you could possibly argue that if the patient returns after a period of time with another dental complaint, the information collected the first time, could be used under the "further processing" provisions of POPI – because the two reasons for processing are closely linked (both being for purposes of providing dental services to the patient – although the two consultations have got nothing to do with one another.)	
	5 INFORMATION QUALITY **How is the info kept up to date and relevant?** **s 16**	**Do you have a process in place if your patients/ suppliers/employees etc. would like to change or access their personal information?** You have a responsibility to maintain their records and take reasonable, practical steps to ensure that the information is complete, accurate, not		

		misleading and remains updated where necessary Accuracy is more assured if you obtain information directly from the DS. It is always advisable to validate the personal information as it is being captured. If it is not possible for the data subject to input their own information, or if the information is captured from one format to another (i.e. from a paper form to an IT system, then the information should be sent to the data subject for validation. When advising Data Subjects of the information you hold and for what purpose you hold it, they must be given details of how to update their information or withdraw consent. This procedure should be covered in the POPIA policies and procedures manual. It is advisable to develop procedures for automatically checking the accuracy of information on a regular basis, but sending a validation request to the data subjects.		
	6 OPENNESS **Are you able to adequately share personal info with the owner of that info?** **s 17 to 18**	Is the DS whose information aware you are collecting such personal information and for what purpose the information will be used? Do you let DSs know when you collect information? They should know: • Where you collect information • Where you don't collect information • The source of your information • Your practice's name and address	**TRANSBORDER INFORMATION** A practitioner may not transfer personal information outside of the country unless the recipient is in country with equivalent protection rules, or the patient has consented to it, transfer is necessary for the performance or conclusion of the contract or for the benefit of the patient and its not practical to obtain consent.	

		• Why you collect the data (your purpose) • Whether the collection is voluntary or mandatory • What happens if the data subject doesn't provide their data • Laws that allow data collection • If and when you intend to send the data to a third country Proof of consent to be retained to safeguard you against any complaint made by DS.	This will apply where the practitioner is reporting claim or complaint to a foreign indemnity provider. If cloud computing used, where servers hosted on the Internet to store, manage or process data, as opposed to a local network, the practitioner remains solely liable for establishing and maintaining the confidentiality and security measures in respect of the processing or retaining of personal information. If Cloud Computing Services is not domiciled in South Africa, the Responsible Party must further take reasonably practical steps to ensure that the service provider complies with the laws relating to the protection of personal information of the territory in which the service provider is domiciled.	
7	**SECURITY SAFEGUARDS** **Are you keeping all the data safe and secure?** **s 19 to 22**	POPI expects from you as far as security measures: Integrity and confidentiality of personal information by taking technical and organisational measures (Personnel and how you deal with them as security measures/risks) against loss, damage, unauthorised destruction, unlawful access or processing of personal information. How do you store personal information and is it safe against unauthorised use? POPI only requires to you take "reasonable steps". Thus, you do not need to put alarms or lasers but do not leave cabinets or offices unlocked. **Paper Files and Information**	NB – Health related PI is a special category under POPI for a reason –You can expect the Regulator to take breaches regarding this category of data very seriously. Your reception desk might be one of the most vulnerable locations in your entire practice. Why? Every patient you treat walks up to the reception desk and discusses their visit with the receptionist for at least a minute or two. What do they see when their eyes wander around that reception desk? What do they hear? What can they grab? Take a photo of? Possible violations on reception desks	

		Are they in locked steel cabinets or locked filing room? Does receptionist have the key with a spare key in the safe? Do all staff have access to files or only designated staff members? Describe the protocols to be followed when requesting access or files. All designated and authorised health care professional staff only has access via receptionist and only for those patients being seen. Requests for copies of files are handled by the practice Information Officer The public should have no access at all such as contractors carrying out repairs or landlord's personnel for example. No patient files are left out, files that require billing are handed to finance immediately and when done, handed to reception to re-file. Files taken by doctor to write reports are left in his/ her office for completion and then handed back for filing. Electronic Records The HPCSA rules on records require records must be password protected. All electronic records must be backed up on a daily, weekly or scheduled basis which back-ups are stored offsite. All changes to records must be initialled and signed by the dentist. **Data Breaches** No matter how well prepared you are, data breaches can happen. Notification must happen as soon as reasonably possible by informing the Information Regulator and the data	The most often POPIA violations one can glean at reception desks are things like: • Seeing the receptionists' open computer with the day's schedule, complete with full patient names • Computer and Wi-Fi passwords written on sticky notes, stuck to a computer monitor (in plain view to the public!) • Patient records on clipboards by the keyboard and easily viewable • Keys (probably to a back office) within arm's reach • Bulletin boards with new patient names and notes about patients • Unopened files which still identify name and address of patients • Patient messages for the dentist written on a pad of paper next to the phone on the reception desk, and in full view. • Recently received faxes left in plain view on the desk. • Recently printed prescriptions left sitting on the desk in plain view. • Unshredded patient records thrown in a trashcan shared by receptionists and waiting room patients. • Patient files placed in clear file holders, clearly viewable to anyone walking by.	

		subject unless identity of data subject cannot be established. Outside of this you may only delay notification of the data subject if a public crime prevention organisation or the Regulator determines that notification will impede a criminal investigation by the public body concerned. POPIA acknowledges that you may first need to secure your system again **Notification to Patients** a) sent by mail to the data subject's last known physical or postal address; b) Sent by email to the data subject's last known email address; c) Placed in a prominent position on the website of the responsible party; d) Published in the news media; or e) As may be directed by the Regulator. It may be necessary to do more than one –e.g. SMS and e-mail. You will have to provide the patient with enough information to enable the patient take protective measures against the possible compromise including: a) a description of the possible consequences of the security compromise; b) a description of the measures that the responsible party intends to take or has taken to address the security compromise; c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and		

		d) if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information. You need to get ready to train your staff and your response plan should form part of your staff training exercise		
	8 DATA SUBJECT PARTICIPATION **Can clients freely see, correct or remove the data you are holding?**	A patient is entitled to ask the practitioner free of charge if it hold personal information of the patient. This is where PAIA comes into effect. Under the Act, everyone is entitled to a copy of any information that pertains to them, regardless of the context. A patient may also request a record or a description of personal information held including any third parties who had or have access to such information. The request if submitted by another person such as an attorney, it must be submitted with a consent. In the case of a dental practice, the record isn't solely the patient's information – the doctor has made notes & those records contain their intellectual property. If the patient requests a copy of their information, there is a process to follow. The patient will need to complete a requester form stating why they want the information. May have access to this request within a reasonable time, on payment of a prescribed fee, in a reasonable format the is generally understandable.	The Regulator has reminded everyone that there is no such thing as a POPIA manual. At the present moment, you do not need to submit your PAIA manual to anyone. The regulator will publish a PAIA manual template on their website as soon as possible. It is currently in the final approval process. It will be user-friendly and people will be able to populate it. In the past private entities like dental practices were exempted from having to compile and submit a PAIA manual. Some practitioners also spent money to get their PAIA manual ready although prior to exemption being granted, SADA provided members with a template. Many organizations (especially SMEs) are currently exempt up until 1 July 2021 from having to have a PAIA Manual. The regulator has asked the Minister to extend the current exemption until 31 December 2021. There is no PAIA manual deadline	Set up a mechanism (included in your PAIA manual and privacy policy) whereby data subjects can: • inquire whether you hold their personal information; • request the identity of all third parties with access to their information; and • request a record or description of their personal information. Establish an accessible process to allow a data subject to: • make corrections to information; • withdraw consent for the processing of information; and • object to the collection of information Inform patients of their right to submit a complaint to the Information Regulator.

		If a fee is requested, the patient must be given an estimate and may request a deposit or part of the fee to be paid. It may also refuse to provide disclose any information requested on grounds of refusal as contained in Chapter 4 of Part 2 and Part 3 of the Promotion of Access to Information Act. The patient may request correction, deletion of personal information or which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully. A data subject may, in the prescribed manner, is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully. They may also request you to destroy or delete a record of personal information that no longer need to retain.		
DIRECT MARKETING	Processing of personal information of a patient (data subject) for direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail is not allowed unless the patient has given consent, is a patient of the practice. The practitioner may request the consent in the prescribed form once from the patient. The practitioner may only process the personal information of a patient who is a customer, obtained details in the context of providing products/services and for direct marketing of similar products or services. The patient must be given a reasonable opportunity to object, free of charge to such use of his, her or its electronic details.	Practitioners who send recall messages for check-ups at regular intervals must obtain patients consent before doing so.	If you engage in direct marketing (via electronic means) Determine if patients have given their consent for the processing of their information (for the purpose of direct marketing); or are they already a customer of your practice. Ensure that the customer information has been obtained: • in the context of the provision of dental services or products; and • for the purpose of direct marketing of your own products or services. Give the patient a reasonable opportunity to freely and informally object to the use of their electronic details at the time of obtaining their	

			details and every time communication is sent to them. Check that all direct marketing communications contain details of the sender and an address or contact details to which the patient can object to receiving such information in future.	
SPECIAL PERSONAL INFORMATION	What is 'special personal information'? Special personal information is information concerning an individual's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information, the criminal behaviour of a person subject to the extent that such information relates to the alleged commission by the employee of any offence or any proceedings in respect of any offence allegedly committed by an employee or about the disposal of such proceedings	Are there exceptions to the processing of special personal information? Yes. • The first exception being consent of the patient. • Religious and philosophical beliefs – by religious organisations • race or ethnic origin if its for a purpose or to advance interests of those disadvantaged by unfair discrimination • health or sex life processing by health professionals is permitted Personal information of children should only be processed subject to consent.		
STAFF AND COMPLIANCE	s19 of POPIA talks of organisational measures –that includes your Staff and their role in your practice As the Responsible Party, you will be in as much trouble if a staff member discloses information to someone who shouldn't have it	**Staff Training** You will have to conduct training with your staff on: • What constitutes confidential personal information for patients; • What security measures you have adopted in your practice; • What their role is in implementing those security measures; • To whom they can and cannot disclose personal information e.g. Medical schemes for processing claims, sub-contracting dental technician, referral to other specialists or dentists who are also treating the patient, implant supply company are acceptable;	**Sample Staff Undertaking** I, _____, the undersigned employee undertake to: a) Maintain as strictly confidential any information of any person where I have gained knowledge of such information in the course of my employment with Dr _____; **b)** Only process as much of a person's information when it is necessary for the performance of my duties as an employee of Dr _____(for example, sending relevant patient information to a medical aid scheme, technician, debt collector,	

		• What to do when they suspect a data breach. Keep proof of staff training –Schedule of attendees with their signature. The Information Regulator may request this Have your staff sign undertakings re: personal information of patients along with their employment agreements.	trader); and comply with the policies of Dr _____as they relate to data protection and confidentiality.	
OPERATORS	**Operators** • **Operator**–means a person who processes personal information for you in terms of a contract or mandate, without coming under your direct authority • Basically, any third-party service providers eg: your outsourced claims administrator, IT provider, accountant, cloud storage solutions etc. • You, as the dentist, however remain the Responsible Party in respect of the personal information that the operator may process on your behalf. **In terms of POPIA an operator must:** a) Only process such information **with your knowledge and authorisation** b) treat personal information which comes to their knowledge as **confidential** and must not disclose it, unless required by law or in the course of the proper performance of their duties. **c)** They have their obligations, but **risk still lies with you** as the Responsible Party! **Risk Management** You will have to review all your contracts with operators when processing and storing personal information.	**Sample Operator Clauses** The Operator undertakes to ensure compliance with the Protection of Personal Information Act No 4 of 2013 (hereinafter referred to as "POPIA"), (the Operator): a) undertakes to comply with the provision of POPIA, as well as any amendments thereto and Regulations published in respect thereof; b) undertakes to treat as confidential any personal information (as defined in POPIA) that comes into (the Operator's) possession in consequence of its rights and obligations in terms of this agreement; c) undertakes to maintain reasonable security measures as required by section 19 of POPIA in relation to any personal information that comes into (the Operator's) possession in consequence of its rights and obligations in terms of this agreement; d) shall notify Dr_____ as soon as reasonably possible where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any		

	Must have a written agreement with your operators – You have to get them to agree to: 1. Undertake to comply with POPIA; 2. Undertake to treat personal information as confidential; 3. Undertake to maintain reasonable security measures of their own; 4. Undertake to notify you as soon as reasonable of the suspicion of a data breach; 5. Indemnify you against claims, fines and penalties flowing from data breach arising from their fault; 6. Undertake not process the personal information without your knowledge and authorisation.	person not authorised to have access thereto; e) undertakes not to process personal information that has come into (the Operator's) possession in consequence of its rights and obligations in terms of this agreement without Dr_____'s prior knowledge and authorisation; and f) f) indemnifies Dr _____ against claims, fines and/or penalties for which Dr _____ may be or may become liable as a result of (the Operator's) non-compliance with POPIA, including but not limited to the failure to implement adequate security measures as contemplated by section 19 of POPIA.		

TEMPLATES

POPI CONSENT FORM

INSERT ON PRACTICE LETTERHEAD

INFORMED CONSENT
PROVIDED BY
PATIENT /PARENT /GUARDIAN
IN TERMS OF
THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 (POPIA)
FOR
PERSONAL INFORMATION TO BE COLLECTED AND PROCESSED
BY
Dr _____
("the responsible party", "practice" and also "the company")

CONSENT FOR THE PROCESSING AND USE OF PERSONAL INFORMATION

I, the undersigned an adult person (18 years or older) / **the parent or legal guardian of a child younger than 12 years of age / a child 12 years or older (***delete what is not applicable*) hereby consent to the processing of my personal information or that of my child as contemplated in the Protection of Personal Information Act No 4 of 2013, by the practice, the practice staff and third party with whom the practice has a contractual relationship for the following purposes:

a] for the purposes of identifying and / or verifying the Patient's or dependent's details;

b] treating and managing me and/or my child in terms of a dentist-and-patient relationship;

c] for further processing or the administration of the contractual relationship between myself and the practice;

d] for legal or contractual purposes;

e] communicating with other persons inasmuch as it relates to my treatment and management;

f] communicating with third parties who have undertaken to indemnify me for the costs of my treatment and management or part thereof including medical schemes and their administrators where relevant;

g] for the purposes of recovering unpaid monies and / or any other amount due to the practice;

h] for the purpose of debt collection;

i] for the purposes of identify other products and services which might be of interest to the Patients;

j] for the purposes of informing Patients about the practice's products and services.

k] processing is necessary for pursuing the legitimate interest of the practice or the third party to whom the information is supplied.

l] Other (specify reasons)_____

Withholding Consent. I understand that it the policy of the practice to require all patients complete and sign the consent. If I exercise my right to withhold my consent to the practice collecting and processing Personal Information, I understand and agree that in this case, the practice reserves the right not to provide dental services (except emergencies) and for which I take full responsibility and indemnify the Practice.

Withdrawal I understand that I can withdraw this consent at any time and I undertake to inform the practice of my withdrawal. In this case, I understand that this may affect my rights and contractual

relationship that I have with the practice and for which I take full liability and hereby indemnify the practice.

My consent is provided of my own free will without any undue influence from any person whatsoever.

I confirm that I have permission of my dependant(s) to give their consent, where such consent has been provided and I indemnify the practice against this.

The Practice Information Officer details are: _____

_____ Print Name _____

Patient Signature

Date _____ Cell No _____

E-mail address _____

Witness signature:_____ Witness initials and surname:_____

Date:_____

DOCUMENT RETENTION, DATA PROTECTION AND DESTRUCTION PERIODS

The POPI Act, requires practitioner that process personal information, to only keep information "no longer than is necessary… to achieve its purpose", subject to exceptions as required or authorised by law, required by a contract or subject to consent of patients.

Retention of Records

Owing to various legislative requirements, documents must be retained for a certain number of years, depending on the legislation. This guide refers to the legislation and identifies the timeframe in which certain documents have to be kept by dental practitioners.

There is no legal requirement (i.e. legislation or case law) that stipulates the period of time that practitioners need to keep their clinical records. However, the ethical rules of HPCSA provide for retention periods for dental records. These ethical rules if not observed, could render the practitioner liable for unprofessional or unethical conduct.

Health Professions Act 56 of 1974, Ethical Rules & Booklets	**Dental Records**	**6 years after they become dormant i.e from date when you last saw patient** **Children patients – when the child reaches 21 years**	**This would include study models, x-rays and clinical notes, certificate, reports etc**
	Prescriptions	5 years as per Meds Act or they become dormant	
	Medical devices	Medical devices: not stipulated	
	Mentally incompetent patients	For duration of person's lifetime	
National Health Act 61 of 2003 & Regulations	Stipulates that record must be created and maintained but does not provide for retention period.	Follow the HPCSA ethical rules above	
	COVID-19 and other notifiable conditions	Not prescribed but maybe be required to be shared with NICD	
Medical Schemes Act 121 of 1998	Claims to medical schemes, pre-authorisation and motivations	Claims must be made within 4 months ito regulations Schemes sometimes claw back and investigate for periods or around 3 years after the claim was lodged. Complaints may also be lodged long after payment is made and thus keep records for longer if practical	
Medicines and Related Substances Act 101 of 1965, Medical Device Regulations	Prescriptions / DIspensing	Medicines: 5 years or 5 years after last entry in a prescription book for dispensing dentists). No provision for device prescriptions or orders.	
	Implantable devices	Order records must be kept for 5 years after expected life of device	
Occupational Health & Safety Act 130 of 1993	Employee (claimant) records. (earnings, time worked, overtime, etc.)	4 years after last entry, except where regs under OHSA on specific conditions	
	Employee records relating to re-opened claims	Not prescribed,	
	Medical reports	4 years after last entry, except where regs under OHSA on	

		specific conditions / sectors require differently (see below)	
		Not prescribed, but 4 years after last	
		Not stipulated, but would have to be retained until patient claim is finalized and provider accounts settled.	
Compensation for Occupational Injuries and Diseases Act, No 130 of 1993	A register or other record of the earnings and other prescribed particulars of all the employees	4 years	
Consumer Protection Act 68 of 2008	Fixed-term consumer agreements	Not stipulated in CPA. As per dental records periods	
National Credit Act 34 of 2005	Incidental credit agreements	3 years after document created	
	Agreement / contract / applications (signed Ts&Cs / billing notices / agreements to r(e)pay)	3 years after termination	
Income Tax Act 58 of 1962	All payroll, payroll calculations (deductions, benefits, etc.), returns, and all related info	5 years from date of submission to SARS	
Value Added Tax Act 89 of 1991	Records of goods / services supplied, invoices, credit notes, charts & codes of account, bank statements, etc., all customs documents,	5 years from date of submission of return	
Basic Conditions of Employment Act 75 of 1997	Written particulars of employment , incl all contracts and documents pertaining to the contract.	3 years after termination of employment.	
	Certificate of service	On employee file, 3 years after employment	
	Current employees occupation, time worked, remuneration, job, etc,	3 years after last entry on record	
Skills Development Act No 97 of 1998	Skills levies, including tax incentives	As per tax requirements (5 years after filing or submission)	
Unemployment Insurance Fund Act 63 of 2002	Name, id nr, address of employment & monthly remuneration	5 years after submission to SARS	
Short-term Insurance Act 53 of 1998	Policies, documents on claims, etc.	Not specifically governed but retain for at least 3 to 4 years after expiry of policy or 3 years after claim is finalized.	
Companies Act, No 71 of 2008	Incorporated practice	General rule for company records	7 years or longer
		Notice of Incorporation (Registration certificate)	Indefinite
		Memorandum of Incorporation and alterations or amendments	Indefinite
		Rules	Indefinite
		Register of company auditors	Indefinite
		Copies of annual financial statements, accounting records record of directors and past directors, after the director has retired from the company	7 years

Protection of Personal Information Act, 4 of 2013	Section 14 of the Protection of Personal Information Act states that personal information must not be retained for any longer than is necessary to achieve the purpose for its collection	If there is no legal requirement to keep the information, it should be deleted. The Act therefore places an obligation on the person collecting the data to delete or remove it at a certain time.	Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless retention required by law, required for lawful purpose related to the practice, required by contract or patient has consented to retention.

INFORMATION REGULATOR DOCUMENTS AVAILABLE ONDREGULATOR'S WEBSITE

INFORMATION OFFICER'S REGISTRATION FORM
https://www.justice.gov.za/inforeg/docs/InfoRegSA-eForm-InformationOfficersRegistration-2021.pdf

GUIDANCE NOTE ON INFORMATION OFFICERS AND DEPUTY INFORMATION OFFICERS - 1 APRIL 2021
https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf

GUIDANCE NOTE ON THE PROCESSING OF PERSONAL INFORMATION IN THE MANAGEMENT AND CONTAINMENT OF COVID-19 PANDEMIC IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 (POPIA)
https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf

GUIDANCE NOTE ON APPLICATION FOR PRIOR AUTHORISATION
https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PriorAuthorisation-20210311.pdf