Disclaimer: The South African Medical Technology Industry Association (SAMED) is providing this opinion as guidance in the context of current legislation, relevant Codes and policies, as well as industry practice, where available. The advice is provided on the basis of the information submitted by the requester. The advice is not a substitute for appropriate legal advice and is not binding on SAMED. SAMED, its board members, committees, employees and members, will not be responsible for any inaccuracies or omissions, or, liable for any damages or loss of whatsoever nature suffered by any person as a result of relying on or using the advice provided.

FAQ on POPIA requirements for medtech companies

No.	QUESTION	RESPONSE
1	**Does one have to put passwords to open documents?**	This would depend on the outcomes of the information and security assessment that Responsible Parties must undertake. Passwords are part of security measures that must be implemented in terms of section 19 of POPI. Implementation of passwords to open documents will depend on the type of information being transmitted, i.e. high risk/medium risk or low risk.
2	**Must one undertake educational training with staff?**	This is a requirement in terms of Regulation 4 of the POPI Regulations issued in 2018. Training must be done on a regular basis. It can be done by internally or by external trainers. Seek professional advice if you are unsure.
3	**How does SAMED, assist member companies around POPIA?**	SAMED does not undertake any POPIA activities on behalf of members. SAMED has held several sessions with informed persons to explain POPIA to members and held a session to answer member questions on POPIA. SAMED also circulates POPIA updates and requirements via the SAMED News. If members would like more detailed assistance, then they should contact a professional.
4	**What does POPIA say on authorisations on behalf of surgeons, patient implant records, patient details on invoicing and all patient data on report analyses?**	POPI prohibits the processing on health information unless you have patient consent/contract or there must be a law compelling you to process the information or exercising or protection of a right. In addition, POPI Conditions of lawful processing also provide that you limit the information you process to your business purpose.
5	**What is the deadline for registration of a company Compliance Officer?**	Deadline for registration of Information Officers has been removed due to the malfunctioning of the registration portal. The Information Regulator is working on resolving this.
6	**What does POPIA say about Operators (Persons processing personal information for and on behalf on another, with the knowledge and authorisation of the Responsible Party)?**	Members must ensure that there is a need to process personal information for and on behalf of the Responsible party, if not, they must avoid it at all costs. Otherwise, Operator contract must be established with the POPI operator clauses. No other way.
7	**What is the liability of Deputy Information Officer (DIO)?**	The DIO is not accountable to the Information Regulator, the Information Officers is. The DIO can only be disciplined in terms of company policies for any failure to perform their duties as DIO. These duties must be part of their Job Description (JD).

8	**Are we allowed to use the patient details on the invoice when sent to Hospitals? Does all our quotations and invoices have to be password protected?**	This would depend on the outcomes of the information and security assessment that Responsible Parties must undertake. Passwords are part of security measures that must be implemented in terms of section 19 of POPI. Implementation of passwords to open documents will depend on the type of information being transmitted, i.e. high risk/medium risk or low risk. POPI prohibits the processing on health information unless you have patient consent/contract or there must be a law compelling you to process the information or exercising or protection of a right. In addition, POPI Conditions of lawful processing also provide that you limit the information you process to your business purpose.
9	**Can I capture Patient Information for track and trace of medical devices and adverse events?**	Only if the law requires information identifying the patient, then such information must be provided, if not, only the device number and batch number will be required. The reporter must provide the unique identifier of the device in question. SAHPRA requires only initials, age/date of birth and gender – the full name is not required for Adverse Event reporting. POPI prohibits the processing on health information unless you have patient consent/contract or there must be a law compelling you to process the information or exercising or protection of a right. In addition, POPI Conditions of lawful processing also provide that you limit the information you process to your business purpose.
10	**Can I process patient identification information?**	Refer to Questions 1, 4 and 9 above.
11	**Marketing by email and phone**	Consent is required and opt out and unsubscribe is required without unnecessary formality to the data subject.
12	**Prior Authorisations**	Due date for application of processing requiring prior authorisation has been moved to 01 February 2022. The Responsible Party remains liable even in cases where the processing of affected information is done by an operator.
13	**Patient information for Track and Trace and AE.**	This would depend on the outcomes of the information and security assessment that Responsible Parties must undertake. POPI prohibits the processing on health information unless you have patient consent/contract or there must be a law compelling you to process the information or exercising or protection of a right. In addition, POPI Conditions of lawful processing also provide that you limit the information you process to your business purpose. Only if the law requires information identifying the patient, then such information must be provided, if not, only the device number and batch number will be required. The reporter must provide the unique identifier of the device in question. SAHPRA requires only initials, age/date of birth and gender – the full name is not required for Adverse Event reporting. Passwords are part of security measures that must be implemented in terms of section 19 of POPI. Implementation of passwords to open documents will depend on the type of information being transmitted, i.e. high risk/medium risk or low risk.
14.	**Are there compliance templates from the Information Regulator?**	No templates are provided by the Information Regulator. Seek professional assistance.

15.	**Can I still do training in hospitals?**	Medtech companies must obtain consent to access patient information in theatre or at the hospital for training on their medical device(s). Training is a Consumer Protection Act requirement.
16.	**Are there POPI Policy Templates?**	There are no official POPI Policy Templates. Seek professional assistance
17.	**Is there a need for industry to work together on POPI?**	Industry Code can be drafted and approved by the Information Regulator.
18.	**Are the definitions in the POPI Act non-exhaustive?**	Yes, definitions are not exhaustive as they refer to “including” or “not limited to”. Therefore, there may be undefined activities that fall within the Act
19.	**What must one do to comply with POPIA?**	A company must implement a POPIA Policy, have a PAIA manual and appoint and register an Information Officer. Seek professional guidance should you be unsure of this undertaking.
20.	**I am encountering portal issues and receive no responses from Information Regulator when trying to register a company Information Officer.**	Deadline for registration of Information Officers has been removed due to the malfunctioning of the registration portal. The Information Regulator is working on resolving this.
21.	**What do I do about patient details on orders?**	If you do not require the details to invoice, do not collect the details. This would depend on the outcomes of the information and security assessment that Responsible Parties must undertake. POPI prohibits the processing on health information unless you have patient consent/contract or there must be a law compelling you to process the information or exercising or protection of a right. In addition, POPI Conditions of lawful processing also provide that you limit the information you process to your business purpose. Only if the law requires information identifying the patient, then such information must be provided, if not, only the device number and batch number will be required. The reporter must provide the unique identifier of the device in question. SAHPRA requires only initials, age/date of birth and gender – the full name is not required for Adverse Event reporting. Passwords are part of security measures that must be implemented in terms of section 19 of POPI. Implementation of passwords to open documents will depend on the type of information being transmitted, i.e. high risk/medium risk or low risk.