SOCIETY OF RADIOGRAPHERS OF SA

POLICY

MANAGEMENT AND ADMINISTRATION OF SOCIAL MEDIA PLATFORMS IN ACCORDANCE WITH GOOD PRACTICES

1. INTRODUCTION

In order to aid in effective communication with SORSA members, most regional branches use social media, especially Facebook. However, we also realise that one needs to be cognisant of the ethical and legal aspects pertaining to administering such platforms. Not only to protect the integrity of SORSA but also to promote and protect its interests. Furthermore, with the latest developments in the South African legal framework, SORSA needs to ensure that members' rights are not infringed thus it is important to implement necessary precautions to protect the rights of members, as well as the public.

2. RATIONALE

The following are guidelines to manage and administer social media platforms in accordance with good practices. This should ensure protection of both members as well as the integrity and interests of SORSA – if adhered to and strictly controlled.

3. APPEARANCE OF THE SOCIAL MEDIA PLATFORM

To maintain the professional standard expected from regional branches the following guidelines should be utilised when setting up a social media page.

3.1 Display picture

The display picture of the page should be the SORSA emblem. It can be colour or black and white.

3.2 Naming the platform

The platform needs to be named to describe and identify the regional branch and its affiliation, for example: SORSA PE BRANCH.

3.3 Privacy of the platform

The Facebook page needs to be a private group. Potential members to this page should request acceptance. Such acceptance shall be at the discretion of the administrators. The administrators should also bear the criteria for acceptance to this group in mind, refer to point 4.3.

3.4 Description section of the platform

A short description of SORSA should be given and the regional branch's committee members and their respective portfolios should be stated. This section should also be updated annually after the AGM of the relevant year by the administrators.

4. ADMINISTRATORS

Two regional branch committee members should be appointed annually as the administrators of the regional branch's Facebook page. These administrators will be responsible:

- To manage and monitor the platform on a regular basis;
- To ensure only members of that regional branch are accepted to the platform;
- To not allow advertisements for locums/vacant posts, etc. ;

- To not allow advertisements of professional matters on the platform from any other individual who is not a current SORSA member; and
- To post and upload relevant regional branch activities and any news related to Radiography.

The management and administration of this platform should also adhere to the terms and conditions of the Facebook platform.

4.1 Facebook pages manager application (App)

In its most basic *modus operandi* the Pages Manager App lets you (administrator) manage up to 50 pages from your smartphone or tablet. You can check page activity, share with your audience and see insights.

Pages Manager has a similar look and feel to the regular Facebook iPhone App, but it is more focused on updating and managing pages. The App allows users to choose from the list of pages they manage and begin posting from it. From the main menu, users can view their lists of pages, view overviews of their pages' insights, look at the list of page admins, visit the help centre, and check out the privacy and legal notices.

4.2 Controlling content appearing on the timeline of the Facebook platform

The administrator has the power to censor or block certain words or content to appear on the platform's timeline. This is done by activating the profanity filter. When words that you have blocked or censored are included in the content individuals posted, the post or comment will be automatically marked as spam.

You can block different degrees of profanity from appearing on your Page. Facebook determines what to block by using the most commonly reported words and phrases marked offensive by the community. To turn on the profanity filter:

1. Click **Settings** at the top of your Page
2. Click **Profanity Filter**

3. Select **Medium** or **Strong**
4. Click **Save Changes**

To block words the following steps must be followed:

1. Click **Settings** at the top of your Page
2. Click **Page Moderation**
3. Type the words you want to block, separated by commas. You'll need to add both the singular and plural forms of the word you want to block.
4. Click **Save Changes**

4.3 Criteria for acceptance of potential members of the platform

At the discretion of the page administrators, any person who demonstrates an interest in radiography or who is affiliated closely with the profession can be accepted as a member of the regional branch's Facebook platform.

4.4 Annual update of social media platform members

Annually, the administrators should update the members of this platform. They will have to do the following:

- Each year, on the 1st of April, get a current database from the secretary or treasurer of the regional branch;
- The social media platform members should be compared to the current database of the regional branch; and
- Those members that are not registered and paid up members of the current year should be deleted from the social media platform.

4.5 Annual timeline screening and clearance of the social media platform

Administrators should screen the social media platform every year to remove irrelevant posts, such as posts of non-registered members of the relevant year et cetera.

5. LEGAL FRAMEWORK

As mentioned previously, to protect the integrity and interests of SORSA and members cognisance must be taken in terms of the legal underpinnings to these communicative means. Furthermore, we need to have a working knowledge of what is permissible on social media platforms, in terms of content related to patients and other members of public.

The following legislation is of paramount importance, to ensure that we act in the best interests of SORSA, its members and the public.

5.1 National Health Act 61 of 2003

The National Health Act states that the use of identifiable information in medical records can only be used for study, teaching or research if it has been authorised by the patient and the head of the health establishment concerned and the relevant health research ethics committee.

5.2 Protection of Personal Information Act 4 of 2013

The Protection of Personal Information (POPI) Act states that no identifiable personal information may be used for study, research or teaching unless the patient [or member of public] has authorised the disclosure for that particular purpose.

A basic overview and explanation of the POPI Act is provided in Table 1 on pages four and five.

6. ETHICAL FRAMEWORK

In accordance with the HPCSA guidelines of good practice, we need to act in the best interests of patients. We can extend this to our members of SORSA as well, since we are all registered with the Professional Board of Radiography and Clinical Technology (PBRCT), and remain professionals. This implies that we may incur liability on the basis of unprofessional conduct from our Professional Board as well if any member of SORSA may be found to act unprofessional. Furthermore, SORSA will also take the necessary disciplinary measures. In terms of content regarding patients that may be placed on social media platforms, the HPCSA prescribes the following:

That a patient's express consent must be obtained before publishing case reports, photographs or other images in media that the public can access. This rule applies regardless of whether the patient can be identified or not (HPCSA, *Confidentiality: Protecting and Providing Information, booklet 10).*

Table 1: The POPI Act: An overview

What is POPI: The Protection of Personal Information (POPI) Act explained

In simple terms, the purpose of the **POPI Act** is to ensure that all South African institutions conduct themselves in a responsible manner when collecting, processing, storing and sharing another entity's personal information by holding them accountable should they abuse or compromise your personal information in any way. The POPI legislation basically considers your personal information to be **"precious goods"** and therefore aims to bestow upon you, as the owner of your personal information, certain rights of protection and the ability to exercise control over:

- when and how **you** choose to share your information (requires your **consent**)
- the type and extent of information you choose to share (must be collected for valid **reasons**)
- transparency and accountability on how your data will be used (limited to the **purpose**) and **notification** if/when the data is compromised
- providing you with **access** to your own information as well as the right to have your data **removed** and/or destroyed should you so wish
- **who** has access to your information, i.e. there must be adequate measures and controls in place to track access and prevent unauthorised people, even within the same company, from accessing your information
- how and where your information is stored (there must be adequate measures and controls in place to **safeguard** your information to protect it from theft, or being compromised)
- the integrity and continued **accuracy** of your information (i.e. your information

must be captured correctly and once collected, the institution is responsible to maintain it)

Examples of "personal information" for an **individual** could include:

- Identity and/or passport number
- Date of birth and age
- Phone number/s (including mobile phone number)
- Email address/es
- Online/Instant messaging identifiers
- Physical address
- Gender, Race and Ethnic origin
- Photos, voice recordings, video footage (also CCTV), biometric data
- Marital/Relationship status and Family relations
- Criminal record
- Private correspondence
- Religious or philosophical beliefs including personal and political opinions
- Employment history and salary information
- Financial information
- Education information
- Physical and mental health information including medical history, blood type, details on your sex life
- Membership to organisations/unions

It must however be noted that some personal information, on its own, does not necessarily allow a third party to confirm or infer someone's identity to the extent that this information can be used/abused for other purposes. The combination of someone's name and phone number and/or email address for example is a lot more significant than just a name or phone number on its own. As such the Act defines a **"unique identifier"** to be data that "uniquely identifies that data subject in relation to that responsible party".

We have to accept that we now live in an information age and along with this progress comes the responsibility for **each person to take care of and protect their own information.** Do not accuse someone else of sharing or compromising your personal information when you publish the very same information on public services like Facebook, LinkedIn, Google+ or public directories. Modern technology makes it easy to access, collect and process high volumes of data at high speeds. This information can then be sold, used for further processing and/or applied towards other ends. In the wrong hands such an ability can cause irreparable harm to individuals and companies. To protect your right to privacy and abuse of your information, data protection legislation is necessary even if it means imposing some social limits on society to balance the technological progress. So remember: **The POPI Act cannot protect you if you do not take care to protect yourself.**

It is important to note though that this right to protection of "personal information" is not just applicable to a natural person (i.e. an individual) but **any legal entity**, including companies and also communities or other legally recognised organisations. All of these entities are considered to be **"data subjects"** and afforded the same right to protection of their information. So this means that while you as a consumer now have more rights and protection, you and your company/organisation are considered "responsible parties" and have the **same obligation to protect** other parties' personal information. As a company this would include protecting information about your employees, suppliers, vendors, service providers, business partners, etc.

The POPI legislation is not a rare or unique phenomenon to South African law. **Many**

countries have similar legislation in place to protect the personal information of their "data subjects", including rules and regulations for international (**cross-border**) transfer and sharing of data. The general consensus seems to be that, apart from an unrealistic implementation period of **one year** and some practical implementation challenges, the POPI Act is well thought out and it borrows from the "best of" other similar international laws, learning from their mistakes and shortcomings.
As usual, **ignorance of the law is no excuse**. Incorporating POPI into the day-to-day operations of a business will most likely require a significant amount of time and effort, including: educating and training staff, updating business processes and implementing or updating technology solutions. **Early action is essential**, especially if you do not have a business nervous system (BNS) to facilitate this. Consider for example that under the POPI Act you could be breaking the law if you do something as simple as synchronising your contacts on your phone, sending an email with sensitive content, taking/sharing a video or photo, using an international mail provider (like Google...) and so forth.
If you are a custodian of personal information it is important that you read our article on "Implementing POPI: How the POPI Act affects you and your business" as there are serious implications for non-compliance. This document also discusses the conditions that apply to processing of personal information in more detail as well as their practical implications and considerations. A more comprehensive Implementation Guide is available to our WorkPool clients and partners to assist them with the transition and provide guidelines on implementing POPI, called "Business Nervous System Architecture and POPI Implementation Guide".

7. CONCLUSION

The regional branch administrators of social media platforms need to bear the following in mind:

- Only SORSA members can be accepted on the page – thus a private group.
- Only SORSA associated business may appear on the page.
- The profile picture must be the SORSA logo
- The purpose of the page/group is to communicate with members
- The page must comply with the terms and conditions of Facebook or other social media criteria (see Facebook's platform policy).
- The legal and ethical underpinnings of social media platforms, related to the protection of individuals and SORSA must be adhered to and proactively practised.

8. SOURCES

http://www.sorsa.org.za/news/information-regarding-use-of-patients-records-radiographs-on-sorsa-social-media

http://www.justice.gov.za/legislation/acts/2013-004.pdf

http://www.gov.za/sites/www.gov.za/files/a61-03.pdf

http://www.hpcsa.co.za/Uploads/editor/UserFiles/downloads/conduct_ethics/rules/generic_ethical_rules/booklet_10_confidentiality_protecting_and_providing_information.pdf

http://www.workpool.co.za/featured/popi/