Western Cape Government

Department of Health
Dr Melvin Moodley
Director: Health Intelligence
Melvin.Moodley@westerncape.gov.za
Tel: 021 483 9366

Date: 18 February 2022

Circular No. H16/2022 POPIA Compliance: Guidelines on the use of Whatsapp and other free multiplatform messaging applications to transmit identifiable personal information.

To: All heads of divisions, directorates, chief directorates, heads of institutions, regions, districts, and sub-structures

The Protection of Personal Information (POPI) Act (No. 4 of 2013) came into force on 1 July 2020, and the 12-month grace period for implementation expired on 1 July 2021. The POPI Act now holds South African organisations accountable for the responsible processing of the personal information of data subjects (i.e., the person to whom the personal information relates). Responsible parties such as Western Cape Government: Health (WCG:H) are now required by law to protect personal information from unauthorised access, processing, modification, or destruction.

Background

The use of WhatsApp is ubiquitous in the Department of Health and around the world. In countries such as South Africa, which have data protection laws, it has become necessary to specifically address the issue of Whatssapp utilisation as a form of communication.

The use of Whatssapp in the United Kingdom and United States.

It is important to note that both the United Kingdom and the United States do not allow the use of Whattsapp for communication of identifiable information in their respective health settings.

Position of the Information Regulator

The Information Regulator of South Africa has not issued any guidance or a directive on the use of WhatsApp to process personal information or special personal information.

Legal opinion on the use of Whatssapp

To aid us with this policy, the Department of Health has obtained a legal opinion on the utilisation of Whatssapp in the Western Cape Department of Health:

1. WhatsApp groups may be used to co-ordinate clinical care aspects, resource allocation as well as social and administrative functions that do not share identifiable patient information.
2. It is recommended that it is not used to share identifiable patient information to ensure that patient confidentiality is maintained.

3. If health care practitioners use WhatsApp to share identifiable patient information, they need to ensure that they have the written informed consent of patients. In addition, they need to ensure that controls are put in place to mitigate the risks identified. This includes, amongst others, ensuring password protection on the device being used to access WhatsApp, as well as ensuring that notifications and pop-ups for Whatssapp are turned off to prevent messages from appearing on locked screens.

Recommendations on the use of WhatsApp

1. Whatssapp can be used for the transfer of non-identifiable information.

2. Whatssapp must not be used for the transfer of identifiable information except under the conditions set out in point 3.

3. Whatsapp may be used for the transfer of identifiable information under the following conditions:

    - The data subject has provided written informed consent for the use of their personal information on Whattsapp, and

    - the device being used must be password protected, and

    - all Whatssapp notifications and pop-ups must be disabled to prevent messages from appearing on the screens of locked devices.

Can I use any other free multiplatform messaging system to transmit personal identifiable information?

It is recommended that WhatsApp or any other free multimessage system inter alia Telegram Messenger, Messenger, Google Hangouts, WeChat etc. is only used when **non identifiable personal information is shared** between healthcare professionals or employees in the Department of Health. Please study the attached addendum which explains what constitutes personal information and unique identifiers.

Important Exclusion: This circular does not apply to the Vula Mobile Application.

Additional security concerns

WhatsApp does not require a password to access messages on a user's device, unless specifically enabled. Therefore, if a device is lost or stolen the information may be compromised. A study conducted in Ireland reports that 30% of medical interns interviewed had lost their smartphones in the preceding year.

Images and videos may be stored directly to the photo cache of the device, which may result in sensitive images being inadvertently downloaded onto the owner's personal computer or uploaded to an online cloud storage service. We recommend that you adjust your device settings to prevent images from Whatssapp from being stored directly to the photo cache. If this is not possible, we recommend deleting the relevant photos from your photo cache.

Pop-up messages may appear on locked screens unless the functionality is specifically disabled, thereby increasing the possibility that confidentiality may be breached if patient-identifiable information is shared. We recommend adjusting your device settings so that notifications and pop-ups do not appear on locked screens.

For queries and assistance, please contact us at DOH.POPIA@westerncape.gov.za.

Regards

DR M MOODLEY, Director: Health Intelligence

ADENDUM

Helpful Definitions

"personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

(a) **information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;**

(b) i**nformation relating to the education or the medical, financial, criminal or employment history** of the person;

(c) any i**dentifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier** or **other particular assignment** to the person;

(d) the **biometric information**[1] the person;

(e) the **personal opinions, views or preferences** of the person;

(f) **correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;**

(g) **the views or opinions of another individual about the perso**n; and

(h) **the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;**

"Unique Identifier", as defined in POPIA, means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party. Examples include **bank account numbers or any account number, policy numbers, identity numbers, employee numbers, student numbers, telephone or cell phone numbers, or reference numbers.**

[1] **"biometrics"** means a technique of personal identification that is based on physical, physiological, or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition.