DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

The Information Commissioner (the Commissioner) issues a reprimand to NHS Lanarkshire in accordance with Article 58 (2)(b) of the UK General Data Protection Regulation (the UK GDPR) in respect of certain infringements of the UK GDPR.

In brief, on 24 March 2020 a [redacted] within one [redacted] Team in NHS Lanarkshire created a WhatsApp Group (the WhatsApp Group) in which staff shared personal data of patients on the [redacted] Team's caseload.

26 staff had access to the WhatsApp Group during its lifespan and between 1 April 2020 and 25 April 2022, there were a minimum of 533 entries within the WhatsApp Group that included patient names, comprising of both adults and children. Of those entries, a minimum of 215 included phone numbers, 96 included date of birth [redacted] and 28 included addresses. 15 images, three videos, and four screenshots were also shared, which included personal data of patients and clinical information, therefore including special category data in the form of health data as defined by Article 9 (1) of the UK GDPR.

In respect of the minimum 533 entries that included patient names, some data subjects may have been mentioned more than once during the lifespan of the WhatsApp Group and NHS Lanarkshire considers it probable that some entries were deleted when no longer relevant.

Further to the above, [redacted] was added to the WhatsApp Group in error and had access from [redacted] resulting in an inappropriate disclosure to an unauthorised individual. The personal data shared in the WhatsApp Group during this period included four students' names and student numbers, one child's name, and two children's names and addresses, with an entry regarding one of the children whose name and address was shared also stating [redacted]

As part of NHS Lanarkshire's internal investigation into this matter, other communications were identified whereby staff in the [redacted] Team involved had used WhatsApp. This was found to be a one to one discussion with either; (a) a practitioner [redacted], or (b) [redacted] to their GP mentor in respect of a prescribing course. NHS Lanarkshire could not provide the ICO with further information regarding the other communications referenced above, as WhatsApp had been deleted on the

phone retained during its investigation due to changes in phone numbers being recycled, which resulted in the inadvertent loss of the data.

WhatsApp was not approved by NHS Lanarkshire for processing personal data of patients, rather, the use of WhatsApp was an approach adopted by the [redacted] Team involved without organisational knowledge. It was used by the [redacted] Team as a substitute for communications that would have taken place in the clinical office[redacted], after the team reduced office attendance due to the COVID-19 pandemic.

The events set out above have resulted in personal data being shared via unauthorised means and secondly, an inappropriate disclosure when [redacted] was added to the WhatsApp Group in error.

The reprimand

The Commissioner has decided to issue a reprimand to NHS Lanarkshire in respect of the following infringements of the UK GDPR:

- Article 5 (1)(f) which states personal data shall be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

- Article 25 (1) which states "…the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures…"

- Article 32 (1) which states "…the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…"

The reasons for the Commissioner's findings are set out below.

Article 25 (1) of the UK GDPR

The ICO understands that following an executive meeting and as part of the COVID-19 Gold Command Group meeting on 11 March 2020, "...it was determined that WhatsApp should be made available to allow a Gold Command WhatsApp group to be created." Following this decision, WhatsApp was made available on NHS Lanarkshire's portal for download within NHS Lanarkshire's device estate on the same date.

NHS Lanarkshire confirmed there is and always has been an approved process for applications being deployed onto NHS Lanarkshire's portal for end users to download. This process was being followed with regards to WhatsApp and requests were being rejected and requested to go through NHS Lanarkshire's governance process. However, at the time of WhatsApp's deployment there was no formally approved process in place and NHS Lanarkshire was adopting a new platform for managing mobile devices. An informal process was adopted whilst the formal process was being finalised; WhatsApp fell under the process and was not an application that was approved but was considered as an essential tool during the COVID-19 pandemic and therefore considered necessary, with the understanding that only basic information was communicated.

No Data Protection Impact Assessment (DPIA) was in place and no risk assessment relating to personal data processing was completed in respect of WhatsApp, as WhatsApp was not approved by NHS Lanarkshire for the sharing of personal data relating to patients.

Therefore, the ICO considers the lack of a formal approval process in place at the time of deployment and absence of an assessment of potential risks relating to personal data prior to the deployment of WhatsApp has resulted in an infringement of Article 25 (1) of the UK GDPR.

Articles 5 (1)(f) and 32 (1) of the UK GDPR

It is understood all staff who could access the WhatsApp Group were deemed by NHS Lanarkshire as appropriate in handling the caseload and therefore would be privy to the personal data shared as part of their professional role. Staff also used WhatsApp on their work-issued phones which were subject to security controls. However, in terms of photographs and videos, no staff would have access to this in normal practice as there is no secure clinical image transfer system in NHS Lanarkshire and no screenshots of clinical records are permitted. It is understood staff should not have taken, received, stored, or shared any images or videos.

In relation to the above, although NHS Lanarkshire followed the national policy which the ICO understands is adopted by Health Boards in Scotland, namely Recording (Photography and Video) for Clinical and Service Use Policy, it did not have a local policy specific to NHS Lanarkshire's practices.

NHS Lanarkshire provided copies of policies in place prior to and during the lifespan of the WhatsApp Group as part of the ICO's investigation, such as its Use of Social Media Policy. However, the ICO considers the policies in place should have been more specific to prevent an incident such as this occurring. Specifically policies did not clearly reference

messaging applications such as WhatsApp and there was no specific policy in place directly for WhatsApp.

NHS Lanarkshire's internal investigation found that "the guidance wasn't clear on the use of WhatsApp when some staff enquired about this to their managers and as the [redacted] at the time was part of the group an assumption was made that it was ok to use." NHS Lanarkshire's internal investigation also found that policies rarely mentioned smartphones as mediums for storing information, and many staff and witnesses interviewed during its investigation advised of difficulty finding up to date accessible and clear information regarding phone applications supported by NHS Lanarkshire. Additionally, staff reported that as WhatsApp stated it was an encrypted platform, they thought it would be secure.

The ICO considers the above demonstrates that information governance expectations regarding WhatsApp were not understood by staff involved in the WhatsApp Group.

In addition to the above, the ICO is aware that there were no additional communications sent to staff regarding working remotely which related to data protection and/or the security of personal data when the COVID-19 pandemic began.

NHS Lanarkshire confirmed that as there was no contract in place with WhatsApp, there is no guarantee of data security for any information shared. However, it is noted that NHS Lanarkshire confirmed WhatsApp's security policy confirms that no messages are stored on a central server, with messages only saved on the user's phone, and the ICO understands phone numbers have been recycled which has deleted the chat.

As the responsible controller, the ICO considers measures that on the balance of probabilities may have reduced the likelihood of this matter occurring if implemented by NHS Lanarkshire could have included the following:

- Completing a risk assessment prior to making WhatsApp available to download via NHS Lanarkshire's portal, to identify any potential risks relating to personal data such as the risk that staff use the application to inappropriately share personal data.
- Issuing communications to staff when WhatsApp was made available to download, to outline expectations regarding the handling of personal data via official and approved channels ie email.
- Developing a standard operating procedure, guidance, or policy for WhatsApp prior to it being made available to download, or alternatively ensuring existing policies and procedures specifically

set out expectations regarding messaging applications such as WhatsApp.
- Issuing communications to staff at the outset of the COVID-19 pandemic to outline expectations regarding the handling of personal data when working practices became more remote.

Therefore, the ICO considers NHS Lanarkshire did not implement appropriate technical and organisational measures to ensure the security of the personal data involved in this matter. As a consequence, personal data was shared via an unauthorised means and an inappropriate disclosure occurred which has resulted in infringements of Article 5 (1)(f) and 32 (1) of the UK GDPR.

Other points of note

The ICO has identified that there is a delay in reporting this matter to the ICO [redacted] Further, the event whereby [redacted] was added to the WhatsApp Group in error was not reported to the appropriate line manager or reported internally within NHS Lanarkshire.

As stated above, the use of WhatsApp was initially used to communicate at the onset of the COVID-19 pandemic, where staff were advised to work remotely. Information provided by NHS Lanarkshire as part of this investigation indicates there were issues with IT systems and staff workload at that time.

With exception to data subjects whose personal data was shared when [redacted] was added to the WhatsApp Group in error, data subjects have not been informed of this matter. In respect of NHS Lanarkshire's rationale, in brief the ICO understands this decision is based on the staff having access would be expected to have access to this data as part of their role, NHS Lanarkshire is confident the personal data has not gone further due to data only being held on the end-user's phone, and to make affected data subjects aware "…would likely cause undue stress and anxiety when in reality the data had remained with the [redacted] team."

In relation to the above, based on the information provided by NHS Lanarkshire, the ICO notes there is potential for distress to be caused to data subjects if they were to be made aware of this matter ie concerns that their personal data has been processed inappropriately and a lack of trust with the [redacted] Team and NHS Lanarkshire overall, which could discourage them from using its services. It is also noted that the images and videos were not held on any clinical systems.

Mitigating factors

The ICO understands that [redacted] had access to the [redacted] until they transferred to [redacted] on 30 August 2021, therefore had access to appropriate systems which were authorised to hold patient information.

Additionally, some photographs were shared with [redacted] proactively by parents and information submitted by NHS Lanarkshire stated that as GPs request photographs to be sent to them, parents assumed they could do the same with the [redacted]. However, it is also understood that some staff took the photographs and/or videos themselves.

Remedial steps taken by NHS Lanarkshire

The Commissioner has also considered the remedial steps taken by NHS Lanarkshire in the light of this matter.

Specifically, on [redacted] NHS Lanarkshire contacted staff regarding this matter and on [redacted], communications were sent to both all staff and [redacted] Teams with the instruction not to use WhatsApp for sharing personal data. NHS Lanarkshire subsequently seized the phones of staff involved which was completed by [redacted]. All phones were deprovisioned which NHS Lanarkshire confirmed deleted the chat and staff have been issued with new phones.

A formal internal investigation has been undertaken which resulted in an investigation report being produced that included recommendations for improvement. These recommendations included re-training staff, requesting staff sign that they had read and understood NHS Lanarkshire's information governance policies, developing standard operating procedures, reviewing all policies, alongside others. An action plan of remedial measures including progress has been provided to the ICO during its investigation.

Additionally, it is noted NHS Lanarkshire planned to undertake work to explore how videos and photographs are stored as part of the clinical record.

Decision to issue a reprimand

Taking into account all the circumstances of this case including the mitigating factors and remedial steps, the Commissioner has decided to issue a reprimand to NHS Lanarkshire in relation to infringements of

Article 5 (1)(f), Article 25 and Article 32 (1) of the UK GDPR set out above.

Further Action Recommended

The Commissioner recommends that NHS Lanarkshire should take certain steps to ensure its compliance with the UK GDPR. With particular reference to Article 5 (1)(f), Article 25 (1) and Article 32 (1) of the UK GDPR unless otherwise specified, the following steps are recommended. NHS Lanarkshire should:

1. Complete any outstanding remedial actions outlined in NHS Lanarkshire's action plan submitted to the ICO on 10 March 2023, if not done so to date.

2. Consider whether it is necessary and/or required to implement a secure clinical image transfer system, as part of NHS Lanarkshire's exploration regarding the storage of images and videos within a [redacted] care setting. If any new system is implemented, it is recommended that:

    2.1 NHS Lanarkshire ensures appropriate organisational and technical measures are in place to ensure a level of security of personal data appropriate to the risk.
    2.2 As part of the above, appropriate policies and procedures for the system are developed and circulated to employees.
    2.3 Employees are asked to confirm understanding of policies and procedures developed.

3. Ensure the following steps are taken before deploying new applications via NHS Lanarkshire's device estate:

    3.1 Risks relating to personal data are considered.
    3.2 The requirement to assess and mitigate risks relating to personal data is included in any documented process regarding the approval and deployment of applications.
    3.3 Explicit communications, instructions and/or guidance are issued to employees that explain data protection responsibilities where applicable for any new application deployed. NHS Lanarkshire should make it clear when applications are not approved for processing personal data.

4. Review all organisational policies and procedures relevant to the circumstances of this matter and amend where appropriate, if not done so to date.

5. Ensure all staff are aware of their responsibilities to report personal data breaches internally without delay to the relevant team in NHS Lanarkshire, so NHS Lanarkshire can consider whether it is required to report the personal data breach to the ICO in line with Article 33 of the UK GDPR.

NHS Lanarkshire should provide a progress update on the above recommendations within six months of the date of this reprimand, ie by **14 January 2024**.