DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

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

On 13 June 2019, NHS Highland, on behalf of [redacted] sent an email to data subjects. The attachment to the email included an invitation to a meeting taking place the following week. [redacted] opened a previous group email and copied the recipient list and emailed the newsletter to a group of patients, without using the Blind Carbon Copy ('BCC') option thereby revealing email addresses to all recipients. Attempts were made to recall the email, but this was not successful. The email was sent to 37 data subjects and most of the email addresses included first name and surname or part of the name.

Later the same day NHS Highland received a number of phone calls from recipients and a patient also attended a clinic advising all email addresses were visible.

The incident placed the personal data of 37 individuals at risk. With a reasonable degree of certainty, recipients of the email would have been able to identify a person on the list as being a person who is a member of [redacted] and therefore likely to be accessing HIV services.

Identifying an individual as receiving HIV services could lead to inferences being made about them that fall within Article 9 of the GDPR (special category data concerning their health). Therefore, the email addresses revealed in this incident are, in this context, likely to constitute special category data.

NHS Highland had an email policy that stated, "use the 'bcc' field if you email many people at once" and this was available to all staff on the NHS Highland intranet site. As such, the use of 'BCC' was accepted practice, despite the risks posed by its use.

The disclosure of email addresses alone, even within a group of individuals who are linked by virtue of their connection to the [redacted], is likely to be distressing and/or damaging to the affected data subjects, both in relation to the exposure of their details, and also in relation to their confidence in the service provided. There was also the risk that the disclosure of the email addresses could have resulted in unsolicited

contact between individuals affected by the incident. One data subject stated they were able to identify at least four people, one of whom was a previous sexual partner. There was potential for the incident to cause the recipients distress if they felt that other people knew about their health status (which could potentially include HIV status). The ICO's investigation has determined that the distress and damage that may have been caused could be significant. Two patients submitted formal complaints to NHS Highland. One of these patients made more than one complaint.

The reprimand

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

- **Article 5(1)(f)** which states that personal data 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 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 …"

- **Article 25 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…"

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

Article 5(1)(f)

Based on the findings of this investigation, the ICO considers reliance on 'BCC' for communication to this group of individuals was not the most secure way to manage communications and other methods could have been adopted. For example, sending one email to one person at a time or procuring a software package that would facilitate the sending of bulk communications by way of individual emails.

Article 32(1)

The usual way of sending group emails was by 'BCC' and this approach was detailed in NHS Highland's induction and induction checklist. Based

on the findings of this investigation, the ICO deems that this is not the most appropriate way to manage emails sent to this group. As such, the ICO has concluded that there was a lack of technical and organisational measures to prevent the disclosure.

Article 25

The consent was not in place to allow for NHS Highland to send emails on behalf of [redacted] and it did not explicitly mention non-medical related information.

NHS Highland's policies state "BCC" should be used when sending group emails.

Both these factors suggest a lack of consideration, in respect of data protection, when setting up the arrangement with [redacted]. For NHS Highland to engage in contacting patients on behalf of any community or patient groups, even if clinical data was not involved, robust and clear consent should have been in place.

In this incident, the sensitivity of the email addresses should have been considered when the arrangement was made to forward emails on behalf of [redacted] due to the inference that could be made regarding access to HIV services and HIV status.

Mitigating factors

In the course of our investigation, we have noted that it was relatively unusual for group emails to be sent by this department and the member of staff involved was working to a tight timescale in a busy office.

Remedial steps taken by NHS Highland

The Commissioner has also considered the remedial steps taken by NHS Highland in the light of this incident. In particular, escalation protocols were followed with the senior manager and Senior Information Risk Owner (SIRO) being advised of the incident. Additionally, attempts were made to contact the data subjects; this was undertaken by [redacted]. 19 patients were successfully contacted by telephone and the remaining 17 who did not answer their telephones were contacted by email. All data subjects who were contacted by telephone were requested to delete the email and not to disseminate the information any further. A Significant Adverse Events Report took place and was overseen by a suitably qualified independent chair from another health board. Moreover, NHS Highland has ceased sending emails on behalf of [redacted] and the [redacted] no

longer sends group emails to patients, making a repeat of such an error less likely.

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 Highland in relation to the infringements of **Article 5(1)(f), Article 32(1) and Article 25** of the UK GDPR set out above.

The ICO considered notifying NHS Highland of its intention to impose an administrative penalty in the amount of £35,000. However, since June 2022 the ICO has adopted a revised approach to public sector enforcement and, on this occasion, we have decided not to impose an administrative penalty.[1]

Further Action Recommended

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

1. In order to ensure ongoing compliance with Article 5(1)(f) and Article 32(1), NHS Highland should ensure that relevant policies, such as the data protection policy and email policy, are reviewed in relation to the use of group emails and updated where necessary.

2. When sending group emails to patients, particularly when these contain special category data, NHS Highland should satisfy itself that security is considered, and that appropriate technical and organisational measures are utilised. This may involve conducting a Data Protection Impact Assessment to identify and address any security risks. This would reduce the risk of a recurrence of this type of incident and assist compliance with Article 5(1)(f) and Article 32(1) and Article 25.

3. If not already in place, NHS Highland should consider conducting an internal assessment in relation to UK GDPR training compliance. This should include ensuring that any training is regularly reviewed and updated as necessary, with refresher training being provided as appropriate (the ICO recommends yearly). Ideally training will

[1] ICO sets out revised approach to public sector enforcement | ICO.

include NHS Highland's expectations of how to send group emails and will assist compliance with Article 5(1)(f) and Article 32(1).

NHS Highland should provide the ICO with a progress update on the above recommendations in three months' time.

It has been noted that NHS Highland has confirmed that the above recommendations have been added to its Information Governance action plan.