

1. **Reprimand - final**

**DATA PROTECTION ACT 2018 AND UK GENERAL DATA
PROTECTION REGULATION**

REPRIMAND

TO: NHS FIFE

**OF: Hayfield house, Hayfield Road, Kirkcaldy, KY2
5AH**

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

The reprimand

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

- Article 5 (1)(f) which states that 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').

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

1.4 NHS FIFE is as medium sized territorial Health Board consisting of Acute Services, Community Services (Health and Social Care Partnership) and Corporate Services. NHS FIFE are responsible for processing personal data, including special category health data. The alleged incident breach took place within one of the sites NHS FIFE is responsible for, [REDACTED]

- 1.5 The investigation found that NHS FIFE are not compliant with Article 5(1)(f) and Article 32 (2) of the UK GDPR due to an unauthorised individual gaining access to a ward, [REDACTED] [REDACTED] Due to lack of identification checks and an unclear process, the unauthorised individual was handed a document (SBAR) containing personal data of 14 individuals and assisted with administering care to one patient. The personal data on the SBAR included personal identifiers and special category health data. The SBAR was taken off site by the unauthorised individual, and the data has not been recovered to date.
- 1.6 There are failings surrounding the security of the data, specifically the SBAR documents. At the time of the incident there was no procedure in place to document whether SBARs were destroyed correctly or collected at the end of the shift. One of the reasons for the delay in reporting the matter to the ICO was due to NHS Fife being unable to ascertain whether the SBAR document had left the site.
- 1.7 During the course of our investigation, it was noted that the training rate of NHS FIFE as a whole is 42%, although the ICO is aware that ward staff training is at 82%. NHS FIFE state the reason this is not 100% is due to the Covid-19 pandemic. NHS FIFE also stated they complete refresher training every three years, as this was agreed at national level for NHS Scotland Boards.
- 1.8 Furthermore, although CCTV was installed within the hospital and a CCTV policy was in place, the wall socket, which the CCTV was plugged in to, had been accidentally turned off by a member of staff prior to the incident taking place, as part of an energy saving exercise. The ICO understands this has now been rectified. Although CCTV would not have prevented the incident from occurring, the lack of CCTV meant that the police and NHS FIFE have been unsuccessful in identifying the individual and therefore unable to recover the lost data. Due to this, there is a potential on-going risk to the data subjects as the intentions of the unauthorised individual are unknown.
- 1.9 Article 32 (2) states 'the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accident or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted,

stored or otherwise processed.' NHS FIFE did not have adequate measures to ensure the security of the data they were processing. Furthermore, the low training rates and outdated or incorrectly labelled policies can also be considered a contributing factor in this incident and raises concerns about the approach and attitude to data protection at NHS FIFE.

Remedial steps taken by NHS FIFE

1.10 The Commissioner has also considered and welcomes the remedial steps taken by NHS FIFE in the light of this incident. In particular introducing a system on the ward for the documents containing patient data to be signed in and out of each shift.

1.11 Furthermore, although there is still no formal process [REDACTED], the ID process [REDACTED] has been revisited and individuals will not be able to commence their shift until their identification has been verified and cross-referenced. NHS FIFE have stated they are developing a standard operating procedure [REDACTED] and, once complete, this will be implemented on all wards.

Decision to issue a reprimand

1.12 Taking into account all the circumstances of this case, including the remedial steps, the Commissioner has decided to issue a reprimand to NHS FIFE in relation to the infringements of Article 5 (1) (f) and Article 32 of the UK GDPR set out above.

Further Action Recommended

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

1. NHS FIFE should consider improving their overall training rate, inline with current legislation. In the course of the investigation it was noted that refresher training is taken three-yearly. NHS FIFE should consider giving refresher data protection training to all staff more frequently. This should be underpinned by written guidance

for employees to follow and NHS FIFE should satisfy itself that security is discussed within the training and guidance.

2. At the time of the breach, it was noted that NHS FIFE did not have any written guidance or policies in relation to ID verification. NHS FIFE should consider developing the guidance or a policy in relation to bank staff attending the hospitals.
3. NHS FIFE should review all policies available from their intranet. If archived versions are needed on the system these should be clearly marked as a previous version.
4. In order to ensure compliance with Article 33 (1), NHS FIFE should revisit their data breach reporting process and ensure relevant personal data breaches are reported within 72 hours. [UK GDPR data breach reporting \(DPA 2018\) | ICO](#)

1.14 We invite NHS FIFE to provide a progress update of the following measures in six months of the date of this reprimand, ie by **6 June 2024**.

2. The effectiveness of the standard operating procedure in relation to bank staff attending the hospitals.
3. The implementation and effectiveness of the ID process [REDACTED]
[REDACTED]
4. The data protection training rates and the steps taken to improve this.
5. The steps taken to update the relevant policies in line with the UK GDPR.