DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

TO: University Hospitals of Derby and Burton NHS Foundation Trust (UHDB)

OF: Uttoxeter Road
Derby
DE22 3NE

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

The reprimand

1.2 The Commissioner has decided to issue a reprimand to UHDB 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').

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

1.4. UHDB is a hospital trust which was created following the merger of the Derby Teaching Hospital NHS Foundation Trust and Burton Hospitals NHS Foundation Trusts in July 2018. UHDB comprises of five hospitals which are situated in Burton, Derby, Tamworth and Lichfield. The alleged infringement was first detected at The Florence Nightingale Community Hospital in Derby.

1.5. UHDB routinely process patient (data subjects) referrals for outpatient appointments containing personal data including health data, which is considered special category data. The referrals are received by UHDB from General Practitioners (GP's) via an electronic referral system

(e-RS). Referrals are intended to be processed within a nationally set timeframe. The maximum wait time for non-urgent, consultant-led treatments is 18 weeks from the day the appointment is booked.

1.6. On 6 September 2019, UHDB was informed by NHS England of an issue with e-RS whereby after 180 days had passed, referrals dropped off the worklist. Staff were still able to retrieve the referral from e-RS and readd to the worklist. However, if the referral remained on e-RS for over 550 days the information was lost to the hospital. NHS England provided guidance to UHDB on 'A Guide to using NHS e-RS data extracts to identify unactioned appointments more than 180 days old' and the 'Management of appointment slots'. Staff were then provided with guidance on how to manage their drop offs from the worklist using an internally generated report which was shared with each medical team.

1.7. UHDB explained that as this was considered to be a routine task, no specific training was provided to staff. The internal report which was generated as a result of this issue was emailed to relevant teams and marked as 'Important'. The report was originally only available to supervisors, however in some cases this task was delegated to staff. The process involved manually reinstating the referrals back onto the e-RS worklist recording the best action that fitted that patient's scenario.

1.8. The total number of data subjects affected by this incident was 4,768. 4,199 of those data subjects had their referrals delayed which had the potential to cause distress and inconvenience. The remaining 569 data subject's referrals were not actioned for so long their data disappeared from e-RS. Some data subjects had to wait for over two years for medical treatment to be arranged.

1.9. To put this in context UHDB processes 1.7 million referrals per year. However, the investigation found that UHDB failed to have appropriate organisational measures in place to prevent the accidental loss of personal data. As this involves the processing of special category data UHBD should have ensured extra measures were put in place.

1.10. The investigation found UHDB failed to implement a formal process or apply a suitable level of security when processing special category data in relation to the processing of referrals on e-RS. The use of email and reliance on staff to manually reinstate referrals did not provide an

effective system or adequate protection which may have prevented the loss of personal data.

1.11. Following the incident, UHDB has reviewed the Trust's Privacy Impact Assessment and Data Protection Impact Assessment (DPIA) register and can find that no risk assessment has ever been carried out in relation to the handling of drop offs of referrals. Had this been carried out UHDB may have identified and been able to minimise any data protection risks which may have prevented the loss of personal data.

1.12. UHDB stated the alleged infringement had occurred due to staff failing to follow all the manual steps recorded in a Standing Operating Procedure (SOP) and that this had been occurring since January 2020. However, the investigation found prior to a SOP being created the process in place involved staff receiving an emailed instruction informing them of the drop offs. This would not be considered an effective way of managing reinstatement of referrals.

1.13. Furthermore, UHDB failed to have any formal oversight in place to ensure referrals were being effectively managed and reinstated onto the worklist.

Remedial steps taken by UHDB

1.14. The Commissioner has also considered and welcomes the remedial steps taken by UHDB in the light of this incident. In particular;

- UHDB conducted a full internal investigation and an external review.

- UHDB has attempted to contact all affected data subjects. Where possible all data subjects have been added to the list and appointments are being actioned appropriately.

- UHDB has created a new fully documented SOP which has been shared with the relevant staff.

- The process has now been centralised and a robotic process automation (RPA) has been introduced which will eliminate human error and speed up the process.

Decision to issue a reprimand

1.15 Taking into account all the circumstances of this case including the remedial steps, the Commissioner has decided to issue a reprimand to UHDB in relation to the infringements of the UK GDPR set out above.

Further Action Recommended

1.16 The Commissioner recommends that UHDB should take certain steps to ensure its compliance with UK GDPR. With particular reference to article 5 (1)(f) of the UK GDPR, the following steps are recommended:

1. Continue to provide any necessary support to help mitigate any potential detriment to the affected data subjects where applicable.

2. Assess any new processes and procedures that have been put in place as a result of this incident and continue to monitor these over a period of time to ensure that they are effective and to prevent another occurrence of this incident in the future.

3. Ensure the learning from any breach is shared across the organisation - not just the departments where breaches have occurred - to embed lessons learnt from any breach incidents