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

DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

TO: Chief Constable Warwickshire Police

OF: Police Headquarters
Leek Wootton
Warwickshire
CV35 7QB

The Information Commissioner (the Commissioner) issues a reprimand to Chief Constable Warwickshire Police in accordance with Schedule 13(2)(c) of the Data Protection Act 2018 (DPA 2018) in respect of certain infringements of the DPA 2018.

In summary, on 21 June 2021 West Mercia Police and Warwickshire Police erroneously decommissioned a server containing a Warwickshire Police application called [redacted] contained Warwickshire Police [redacted] data from between November 2001 and early 2014. The [redacted] data which has been lost on [redacted] is unrecoverable.

Between March 2012 and March 2020, West Mercia Police and Warwickshire Police were part of a Strategic Alliance (Alliance), which sought to achieve financial benefits and operational efficiencies for both forces by sharing certain functions. Part of this Alliance saw the sharing of IT infrastructure, including the merger and consolidation of data networks and environments.

On 31 March 2020, the Alliance formally ended and the forces shared functions came to an end. However, as the process of separating out and migrating the forces data from the shared IT infrastructure to their own independent IT infrastructures would take a considerable amount of time, the forces entered into a new s22A Collaboration Agreement for Shared ICT and Digital Services (Collaboration Agreement) and IT Shared Services (ITSS) was put in place to manage the shared environment post Alliance. This agreement was in place between 1 April 2020 and 30 September 2021.

Under the Alliance, the forces had established the KCOM project with the over-arching purpose of moving all live services from the legacy network (KCOM provided) to the current network, however it also involved decommissioning servers which were no longer needed. Some of the servers identified by the KCOM project as ready for decommissioning were not decommissioned by the Alliance IT team as the task was initially

parked in favour of more pressing operational priorities. Following the end of the Alliance, the project was passed to ITSS for action.

During 2021, ITSS undertook remedial security tasks to support the forces cyber defence. These security tasks included removal of unsupported servers, including the previously parked KCOM decommissioning list. The server containing [redacted] was included within this list and had been marked by the KCOM project as ready for decommissioning. This resulted in the server being subsequently decommissioned by ITSS on 21 June 2021.

This investigation has determined that for the shared IT function under the Collaboration Agreement, the forces were acting as joint Data Controllers. ITSS was created by both forces and was jointly governed and funded at the time. As the decommissioning of the server was carried out pursuant to the ITSS function set out in the Collaboration Agreement, the Commissioner considers that the forces were acting as joint Data Controllers in respect of the decommissioning.

The reprimand

The Commissioner has decided to issue a reprimand to Warwickshire Police in respect of the following infringements of the DPA 2018:

- Section 40 which states:

"*The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).*".

- Section 66 (1) which states:

"Each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data."

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

- Section 40:

The Commissioner considers that Warwickshire Police has failed to ensure appropriate security, resulting in the destruction of Warwickshire Police [redacted] data.

It is noted that at the time of entering the Alliance, Warwickshire Police 'back record converted' its [redacted] logs from [redacted] into its new system. This was a total of 160,203 sanitised [redacted] logs and the information related to 55,195 nominals. Therefore, the sanitised [redacted] logs from [redacted] can still be viewed by Warwickshire Police, however [redacted] was the only system which contained the unsanitised [redacted] logs and the following information:

- [redacted] source/provenance including names and addresses/location of source.
- Submitting Officer including name, rank, role and shift.
- Unsanitised text including names, addresses/locations, allegations of criminal conduct, previous convictions or cautions, details of relationships and associations.
- Risk assessments regarding the [redacted] including information such as previous convictions of the subject of the [redacted] and/or their associates, details of any further allegations of criminal conduct.

The information which has been lost on [redacted] provided important context and is needed for the assessment of reliability of the [redacted] and the risks associated with it.

- Section 66 (1):

The Commissioner considers that the ITSS decommissioning process which was in place at the time of the decommissioning was inadequate and did not ensure sufficient checks of servers prior to decommissioning.

The documentation which was used by the Alliance KCOM project team and subsequently by ITSS, as authority on the status of servers, was out of date as it incorrectly identified [redacted] as being unused since March 2016. It now seems likely that the documentation was not updated since [redacted] original move in 2016, leading to the KCOM project treating [redacted] as sunset/archive, without further review. The incorrect information was then used by ITSS to schedule and complete the decommissioning. Over-reliance on this documentation led to no cross-checking between applications and server details before decommissioning.

All decommissioning of KCOM servers was agreed by the ITSS Protection of The Live Services (POTLS) process. This included requests for decommissions being emailed out by ITSS to internal technical teams for review. The peer reviewed request would then be sent to all POTLS attendees prior to the meeting and all changes were reviewed and agreed

during POTLS. The technician completing the decommissioning would complete the above process at initial power-down of the server, then wait 30 days to ensure that any user could raise an issue with the decommissioning. After 30 days POTLS would be revisited for permission to decommission the server. This should include a review of any outstanding IT tickets raised by users.

In this instance, the request to decommission the server containing [redacted] did go through POTLS. However, a cut-down version of the decommissioning process was applied, in that the final removal, following the 30 day power-off was pre-approved at the first presentation to POTLS. Although an approved process at the time, this did not reinforce that all IT tickets should have been checked and updated prior to decommissioning. This contributed to ITSS missing an IT ticket which was raised by a user and which would have flagged [redacted] as a system which needed to be retained.

Further to this, POTLS attendance was not mandatory for both forces and required a lot of proactivity by Project Managers to ensure that they attended the correct POTLS. Attendance and meeting minutes were also not recorded at POTLS.

Remedial steps taken by Warwickshire Police

The Commissioner has also considered and welcomes the remedial steps taken by Warwickshire Police in the light of this incident. In particular, Warwickshire Police continued to work with West Mercia Police to determine how the breach occurred. Following the conclusion of West Mercia Police's investigation into this incident, the decommissioning process was strengthened and the POTLS process was replaced by the Change Advisory Board (CAB). Both forces gained from the improvement of this process under the subsequent Hosted Services Agreement which was in place from October 2021.

It is also noted that the Hosted Services Agreement came to an end in March 2022 and that both forces now have their own independent IT infrastructures and IT services.

Decision to issue a reprimand

Taking into account all the circumstances of this case, including the remedial steps, the Commissioner has decided to issue a reprimand to

Warwickshire Police in relation to the infringements of **section 40 and section 66 (1)** of the DPA 2018 set out above.

DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

TO: Chief Constable West Mercia Police

OF: Hindlip Hall
Hindlip
Worcester
WR3 8SP

The Information Commissioner (the Commissioner) issues a reprimand to Chief Constable West Mercia Police (West Mercia Police) in accordance with Schedule 13(2)(c) of the Data Protection Act 2018 (DPA 2018) in respect of certain infringements of the DPA 2018.

In summary, on 21 June 2021 West Mercia Police and Warwickshire Police erroneously decommissioned a server containing a Warwickshire Police application called [redacted] contained Warwickshire Police [redacted] data from between November 2001 and early 2014. The [redacted] data which has been lost on [redacted] is unrecoverable.

Between March 2012 and March 2020, West Mercia Police and Warwickshire Police were part of a Strategic Alliance (Alliance), which sought to achieve financial benefits and operational efficiencies for both forces by sharing certain functions. Part of this Alliance saw the sharing of IT infrastructure, including the merger and consolidation of data networks and environments.

On 31 March 2020, the Alliance formally ended and the forces shared functions came to an end. However, as the process of separating out and migrating the forces data from the shared IT infrastructure to their own independent IT infrastructures would take a considerable amount of time, the forces entered into a new s22A Collaboration Agreement for Shared ICT and Digital Services (Collaboration Agreement) and IT Shared Services (ITSS) was put in place to manage the shared environment post Alliance. This agreement was in place between 1 April 2020 and 30 September 2021.

Under the Alliance, the forces had established the KCOM project with the over-arching purpose of moving all live services from the legacy network (KCOM provided) to the new network, however it also involved decommissioning servers which were no longer needed. Some of the servers identified by the KCOM project as ready for decommissioning were not decommissioned by the Alliance IT team as the task was initially

parked in favour of more pressing operational priorities. Following the end of the Alliance, the project was passed to ITSS for action.

During 2021, ITSS undertook remedial security tasks to support the forces cyber defence. These security tasks included the removal of unsupported servers, including the previously parked KCOM decommissioning list. The server containing [redacted] was included within this list and had been marked by the KCOM project as ready for decommissioning. This resulted in the server being subsequently decommissioned by ITSS on 21 June 2021.

This investigation has determined that for the shared IT function under the Collaboration Agreement, the forces were acting as joint Data Controllers. ITSS was created by both forces and was jointly governed and funded at the time. As the decommissioning of the server was carried out pursuant to the ITSS function set out in the Collaboration Agreement, the Commissioner considers that the forces were acting as joint Data Controllers in respect of the decommissioning.

The reprimand

The Commissioner has decided to issue a reprimand to West Mercia Police in respect of the following alleged infringements of the DPA 2018:

- Section 40 which states:

"*The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).*".

- Section 66 (1) which states:

"Each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data."

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

- Section 40:

The Commissioner considers that West Mercia Police has failed to ensure appropriate security, resulting in the destruction of Warwickshire Police [redacted] data.

It is noted that at the time of entering the Alliance, Warwickshire Police 'back record converted' its [redacted] logs from [redacted] into its new system. This was a total of 160,203 sanitised [redacted] logs and the information related to 55,195 nominals. Therefore, the sanitised [redacted] logs from [redacted] can still be viewed by Warwickshire Police, however [redacted] was the only system which contained the unsanitised [redacted] logs and the following information:

- [redacted] source/provenance including names and addresses/location of source.
- Submitting Officer including name, rank, role and shift.
- Unsanitised text including names, addresses/locations, allegations of criminal conduct, previous convictions or cautions, details of relationships and associations.
- Risk assessments regarding the [redacted] including information such as previous convictions of the subject of the [redacted] and/or their associates, details of any further allegations of criminal conduct.

The information which has been lost on [redacted] provided important context and is needed for the assessment of reliability of the [redacted] and the risks associated with it.

- Section 66 (1):

The Commissioner considers that the ITSS decommissioning process which was in place at the time of the decommissioning was inadequate and did not ensure sufficient checks of servers prior to decommissioning.

The documentation which was used by the Alliance KCOM project team and subsequently by ITSS, as authority on the status of servers, was out of date as it incorrectly identified [redacted] as being unused since March 2016. It now seems likely that the documentation was not updated since [redacted] original move in 2016, leading to the KCOM project treating [redacted] as sunset/archive, without further review. The incorrect information was then used by ITSS to schedule and complete the decommissioning. Over-reliance on this documentation led to no cross-checking between applications and server details before decommissioning.

All decommissioning of KCOM servers was agreed by the ITSS Protection of the Live Services (POTLS) process. This included requests for decommissions being emailed out by ITSS to internal technical services for review. The peer reviewed request would then be sent to all POTLS attendees prior to the meeting and all changes were reviewed and agreed

during POTLS. The technician completing the decommissioning would complete the above process at initial power-down of the server, then wait 30 days to ensure that any user could raise an issue with the decommissioning. After 30 days POTLS would be revisited for permission to decommission the server. This should include a review of any outstanding IT tickets raised by users.

In this instance, the request to decommission the server containing [redacted] did go through POTLS. However, a cut-down version of the decommissioning process was applied, in that the final removal, following the 30 day power-off was pre-approved at the first presentation to POTLS. Although an approved process at the time, this did not reinforce that all IT tickets should have been checked and updated prior to decommissioning. This contributed to ITSS missing an IT ticket which was raised by a user and which would have flagged [redacted] as a system which needed to be retained.

Further to this, POTLS attendance was not mandatory for both forces and required a lot of proactivity by Project Managers to ensure that they attended the correct POTLS. Attendance and meeting minutes were also not recorded at POTLS.

Remedial steps taken by West Mercia Police

The Commissioner has also considered and welcomes the remedial steps taken by West Mercia Police in the light of this incident. In particular, West Mercia Police conducted an internal investigation to determine how the breach occurred, including a review of the ITSS decommissioning process. Following this review, the process was strengthened and the POTLS process was replaced by the Change Advisory Board (CAB). Both forces gained from this improvement under the subsequent Hosted Services Agreement which was in place from October 2021.

It is also noted that the Hosted Services Agreement came to an end in March 2022 and that both forces now have their own independent IT infrastructures and IT services.

Decision to issue a reprimand

Taking into account all the circumstances of this case, including the remedial steps, the Commissioner has decided to issue a reprimand to West Mercia Police in relation to the infringements of **section 40 and section 66 (1)** of the DPA 2018 set out above.