



Requester's Copy

Ref no: 01/REA/22/000076

Name: ICO

Date: 30/09/2022

# Internal Review

Potential



Date of Report: August 2022

EEAST: [REDACTED]  
August 2022, v1

[www.eastamb.nhs.uk](http://www.eastamb.nhs.uk)

#WeAreEEAST 

Requester's Copy  
Ref no: 01/REA/22/000076  
Name: ICO  
Date: 30/09/2022

## Investigation Report

WEB Reference ID	[REDACTED]
Name of investigator	[REDACTED]
Date of incident	November 2021 - April 2022
Outcome	Formal Disciplinary

All names in this report have been anonymised other than the author – referenced documents, evidence and full names can be found attached to the original Datix.

## Details of Incident

In April 2022, via the [REDACTED], the Trust became aware of a closed social media (Facebook Messenger) group with a core membership of 30 individuals (other individuals had joined and left at various stages). The core membership consisted of Trust staff [REDACTED]. The contents of this group included the sharing of person identifiable (patient) information, comments and images that may bring the Trust into disrepute, as well as negative comments about colleagues.

It is reported that the group was initially created around October/November 2021 with the intention of using it to arrange social events, but this soon evolved into a wider forum covering broader topics.

Upon becoming aware that details of their conversations had been escalated to the Trust, the individuals left the group, and it was closed.

A Datix incident was raised ([REDACTED]), and, following an initial fact-finding exercise, the staff involved were [REDACTED] pending further investigation under the Trust's formal disciplinary process.

On 17<sup>th</sup> May 2022, the Trust's Chief Executive Officer shared a video briefing message regarding the [REDACTED] of the staff following an initial fact-finding exercise. All staff were asked to watch the communication, which was followed by an all staff briefing email containing the same message. The message reiterated the Trust's values and policies, encouraged staff to consider their roles and behaviours and to speak up if they were aware of such behaviours.

The individual formal investigation reports cover all areas of concern; however, this report focuses solely on the breaches of personal information.

## Investigation process

The Trust obtained a download of the group messages between the period of 4<sup>th</sup> November 2021 and 8<sup>th</sup> April 2022. The chat consisted of approximately 60,000 messages, 2,016 images, 484 videos and 150 voice notes.

Due to the varying levels of involvement and content matter, a decision was made to complete individual formal investigation reports for each member of staff involved.

The incident was reported to the Information Commissioner's Office (ICO) (reference IC-170897-L7Y4) and NHS Digital (reference 28029) on 16<sup>th</sup> May 2022, scoring a total of 6. On 19<sup>th</sup> May the Trust

informed the ICO that it had increased the level of the score to a 12, following further reviews of the information. The scoring is as follows:

4 – It is highly likely that there will be an adverse effect

3 – Information potentially contained within the public domain

That rationale for the increase was due to the risk linked to the loss of control of personal data (potentially within the public domain).

The contents of the chat download have been reviewed by the panel of investigators, with support and oversight from the Information Governance team. Initially, the Trust was only able to access the messages and were not able to view the images, voice notes and videos. Once this technical issue had been overcome, the review discovered 13 data subjects that could potentially be identifiable by the information disclosed. That these disclosures were likely to be classed as personal data protection breaches, as defined by Article 4(12) of the UK GDPR.

*“Personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

Under UK Data Protection Legislation, personal data is defined as information that identifies or can be used to identify a natural person. This includes identifiers such as name, address, location details, phone numbers etc. (This list is not exhaustive).

A further review of this information was undertaken by the Information Governance team and a risk assessment conducted against each data subject. Please see Appendix 1.

## Review of incident

The images shared largely consist of photographs and screenshots of the Trust’s MDT screen. This is the screen within the ambulance vehicles that displays details of the incidents they are attending as well other information, such as directions etc. Information about an incident will only appear on the screens of the vehicles assigned to attend that incident. In several cases where information was shared, the individuals had redacted some level of personal data from the screenshots/photographs.

One of the images shared (Data Subject 10 within Appendix One) is a photograph of the crew’s iPad containing a partially completed electronic Patient Care Record (PCR). The data subject’s home environment (photograph taken inside the patient’s home) and [REDACTED] are visible.

Data Subject 9 relates to an image taken within a hospital ward. The photograph has been taken from a distance and includes the patient’s face. No further identifiable information can be seen.

During the initial review process the Information Governance team determined that the number of data subjects affected (likely to be identified from the disclosures) reduced from 13 to 11. This was due to the level of information disclosed and accounted for any redactions the individual(s) sharing the images had applied, prior to posting them.

The employees [REDACTED] involved in this incident were all working within patient-facing roles and would have legitimately had access to the disclosed information as part of those roles.

#### **Risk Assessment of data subjects**

As detailed within Appendix One, the level of personal data disclosed includes age, gender, reason for the 999 call (health information), location of the emergency (possibly home address) and one data subject's full name. In addition, in some cases, the time of incident and Trust Computer Aided Dispatch (CAD) unique reference numbers are also disclosed.

The CAD numbers would be classed as pseudonymised information; only those with access to the Trust's CAD system would be able to identify the data subjects using that reference number.

Having identified 11 data subjects, the Trust's Information Governance team scored the level of the breach using the matrix of likelihood of identification (by external individuals) x potential detriment to give a total risk score. Please see the Key within Appendix One.

Following the initial assessment of the disclosures, further investigations were undertaken, including the use of Open-Source Intelligence (OSINT) to assess whether this may impact upon the risk and/or detriment level. These findings have been reflected in the Impact on Scores and Total columns.

The scoring used was based upon several factors, which included the following:

1. Due to the nature of the information disclosed (personal and special category) the minimum score of detriment was determined as 3 - potentially some adverse effect.
2. All the disclosures relate to vulnerable persons (patients in need of medical care) and in some circumstances are of a particularly sensitive nature. Therefore, there may be a higher risk of detriment to those individuals, should they be made aware of the breach of their personal data.
3. In some cases, multiple identifiers have been disclosed, which, if coupled with OSINT, could increase the chances of identification.
4. In some cases, limited and pseudonymised information has been disclosed. Therefore, it is unlikely that the data subjects would be identifiable without either prior knowledge of them and/or access to Trust systems.

Details of the data subjects affected by the breach are being reviewed with by the Trust's Caldicott Guardian. The Right to be Informed will be considered against the Serious Harm Test with the outcomes and rationales clearly documented.

#### **Training and compliance**

This incident appears to have resulted from several rogue employees, who have failed to follow the training and guidance provided around the use of social media and handling patient data. These actions have resulted in a breach of the UK Data Protection Legislation.

The Trust has several policies in place around the handling of personal data and the use of social media, including the Social Media Policy, Information Governance Policy, Data Protection Policy and Confidentiality Code of Conduct. All staff are required to comply with these policies as a condition of

their employment with the Trust. Trust policies are readily available to all staff via the Trust's internal document library and Trust website.

The Trust also aligns with the Health Care Professions Council (HCPC) code of conduct.

Key messages from the Trust's policies are incorporated within both induction and mandatory Data Security Awareness and Social Media training.

Trust staff are required to complete the social media training every three years. At the point of the incident, 88.9% of the staff members involved were compliant with this training. Most having completed this training between February – April 2021. To date compliance with this training, for these individuals, stands at 92.6%.

The content of the data security awareness training is based upon guidance from NHS Digital and is required to be completed on an annual basis. The Trust monitors data security awareness training compliance at the Information Governance Group (IGG) and Compliance and Risk Group (CRG).

The current total data security awareness training compliance of those involved is at 62%, with several staff having completed their mandatory training in May 2022. At the point of the incident, 38% of those staff involved were compliant with their mandatory data security awareness training.

The Trust strives to comply with the Data Security Protection Toolkit (DSPT) requirement of 95% overall compliance for data security training. Since Covid-19, the Trust has been operating under extreme pressure (Resource Escalation Action Plan or REAP Level 4) and remains at this level to date. Compliance with the 95% data security training requirement is featured on the Trust's DSPT improvement plan and several actions are being taken to try to address this.

## Outcome

Most of the disclosures involve the capturing and sharing of images taken directly from the MDT screen within the ambulance vehicles. The ability to take a photograph of a screen is challenging and very difficult to prevent, but the Trust is always looking to reduce or mitigate such risks.

The information shared was available to those individuals legitimately through their roles within the Trust. That their actions in sharing this information with others via a non-Trust social media platform have breached Data Protection Legislation, Trust policies, the Trust's values and potentially their contracts of employment, which require staff to handle personal data appropriately and securely.

The individual outcomes for each member of staff involved is being determined by the disciplinary panel. To date, several of the cases have now closed with outcomes including [REDACTED]. The remaining few have hearings are scheduled to take place and due to be completed by the end of October 2022.

It should be noted that following the staff briefing message from the Trust's CEO, some high-level articles around the suspension of staff over social media misuse did feature on a few online news websites.

The Trust continues to work with the relevant registration and regulatory bodies, such as the Health Care Professions Council (HCPC) and Information Commissioner's Office (ICO) to support their investigations.

## Proposed Actions

1. Following the review of data subjects with the Trust's Caldicott Guardian, any individuals being notified about the breach will need to have their details checked against the Summary Care Record / National Spine, prior to contact. This is to take into account any changes of health status (e.g. if a patient has since passed away) and to ensure that we are using the correct registered contact details.
2. Social media is a rapidly changing environment, and the Trust should continue with the current review and strengthening of its Social Media Policy.
3. The Trust should continue to raise awareness / training with all staff around workplace culture.
4. Consideration should be given to undertaking an access audit on the records/patient details that have been disclosed.

Requester's Copy

Ref no: 01/REA/22/000076

Name: ICO

Date: 30/09/2022

**Appendix 1 – Risk Matrix**

Data Subject	Data source	Types of data disclosed	Likelihood of identification (external)	Potential detriment	Notes	Impact on score - identification	Impact on score - detriment	Total	Right to be Informed decision and rationale
1	MDT	Reason for call Type of patient Time of incident Full location (potentially address)	3	3	Several potential identifiers disclosed, which, if coupled with open-source intelligence, makes identification of the data subject more likely.	Increase - 4	None - 3	12	
2	MDT	Age Gender Reason for call Full location (potentially address)	3	4	Several potential identifiers disclosed, which, if coupled with open-source intelligence, makes identification of the data subject more likely.	Increase - 4	None - 4	16	
3	MDT	Age Gender Time of incident Reason for call Full location (potentially address)	4	3	Several potential identifiers disclosed, which, if coupled with open-source intelligence, makes identification of the data subject more likely.	Increase - 4	None - 3	12	
4	MDT	Full name Age Gender Reason for call	3	3	Several potential identifiers disclosed. It is likely that one would require some knowledge of the data	None - 3	None - 3	9	



					subject and/or area to be able to identify them from the information disclosed.				
5	MDT	Reason for call Time of incident Full location (potentially address)	3	3	Full location disclosed but no other person identifiable information. This would make it trickier to identify the data subject concerned.	None - 3	None - 3	9	
6	MDT	Age Gender Reason for call Full location (potentially address)	3	3	Several potential identifiers disclosed, which, if coupled with open-source intelligence, makes identification of the data subject more likely.	Increase - 4	None - 3	12	
7	MDT	Partial CAD number Reason for call Time of incident Partial location (potentially address)	2	3	Partial identifiers disclosed. One would either require access to the Trust's systems or prior knowledge of the data subject to further identify them.	None - 2	None - 3	6	
8	MDT	Partial CAD number Reason for call Time of incident Full location (potentially address)	3	3	Limited and identifiers disclosed. One would either require access to the Trust's systems or prior knowledge of the data subject to further identify them.	None - 3	None - 3	9	
9	Unconfirmed	Full location	2	3	Limited information	None - 2	None - 3	6	

		(potentially address)			disclosed making it difficult to identify the data subject without access to Trust systems.				
10	PCR	Full CAD number Reason for call Patient's pet	2	4	Limited information disclosed making it difficult to identify the data subject without access to Trust systems.	None - 2	None - 4	8	
11	Photograph	Image of a patient in a hospital bed. Their face can be seen.	3	4	The image has been taken from some distance, so it would be difficult for a member of the public to identify the individual.	None - 3	None - 4	12	

**Key:**

Likelihood of identification	Score
Not possible (anonymous information)	1
Unlikely (pseudonymous information – would require access to information held on Trust systems)	2
Potential (limited potential identifiers disclosed – would require access to open-source intelligence)	3
Likely (multiple potential identifiers disclosed – would require access to open-source intelligence)	4

Occurred (data subject is fully identifiable)	5
---	---

Potential detriment	Score
No adverse effect	1
Potentially some minor adverse effect	2
Potentially some adverse effect	3
High risk of pain/suffering	4
Adverse effect has occurred	5

Requester's Copy  
 Ref no: 01/REA/22/000076  
 Name: ICO  
 Date: 30/09/2022

Requester's Copy  
Ref no: 01/REA/22/000076  
Name: ICO  
Date: 30/09/2022