DATA PROTECTION ACT 2018

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: The Tavistock & Portman NHS Foundation Trust

Of: 120 Belsize Lane, London, NW3 5BA

I. INTRODUCTION

1. The Information Commissioner ("the Commissioner") has decided to issue the Tavistock and Portman NHS Foundation Trust ("the Trust") with a penalty notice pursuant to section 155(1) of the Data Protection Act 2018 ("DPA"). This penalty notice imposes an administrative fine on the Trust, in accordance with the Commissioner's powers under Article 83 of the General Data Protection Regulation[1] ("GDPR"). The amount of the penalty is £78,400 (seventy eight thousand four hundred pounds).

2. The penalty is being issued in respect of certain infringements of the GDPR, as described below.

3. The penalty notice arises out of an incident which took place on 6 September 2019, affecting personal data of a specific group of patients being processed by the Trust. The Trust estimates that 1,781 data subjects were affected by the incident.

[1] See also Section 115(9) DPA and Articles 58(2)(i) and 83 GDPR.

4. The provisions of the DPA and GDPR apply to the processing of personal data by the Trust by virtue of section 207(2) of the DPA and Article 3(1) GDPR.

5. For the reasons set out further below, the Commissioner considers that the Trust failed to process personal data in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures as required by Article 5(1)(f) and Article 32 GDPR.

6. The Commissioner has decided to give a penalty notice on the basis that, in all the circumstances, and having regard to the matters listed in Article 83(1) and (2) GDPR, the infringements constitute a serious failure to comply with the GDPR.

II. LEGAL FRAMEWORK

7. 'Personal data' is defined by Article 4(1) GDPR to mean:

Information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

8. 'Processing' is defined by Article 4(2) of the GDPR to mean:

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

9. The Commissioner considers that the Trust is the controller of its patients' personal data within the meaning of section 6 DPA and Article 4(7) GDPR. This is because the Trust determines the purposes and means of processing. By, inter alia, performing operations or sets of operations on personal data such as collecting, storing, organising and using the personal data of its individual patients, the Trust is processing personal data within the meaning of section 3(4) DPA and Article (4)(2) GDPR.

10. Controllers are subject to various obligations in relation to the processing of personal data, as set out in the GDPR and the DPA. They are obliged by Article 5(2) to adhere to the data processing principles set out in Article 5(1) of the GDPR.

11. Article 9 GDPR prohibits the processing of special categories of personal data unless certain conditions are met[2]. The special categories of personal data subject to Article 9 include '*personal data […] concerning health […] and sexual orientation'*.

[2] See also Section 10 & Schedule 1, Part 1 DPA

12. Section 155 DPA provides that, if the Commissioner is satisfied that a person has failed or is failing as described in Section 149(2) DPA, the Commissioner may, by written notice (a penalty notice), require the person to pay to the Commissioner an amount in sterling specified in the notice.

13. Section 149(2) materially provides:

(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following –
(a) a provision of Chapter II of the GDPR or Chapter 2 of part 3 or Chapter 2 of Part 4 of this Act (principles of processing);
(b)…
(c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors);…

14. Article 5(1) of Chapter II GDPR sets out the principles relating to the processing of personal data, including that:

Personal data shall be:
*…(f) 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)

15. Article 5(2) GDPR makes it clear that:

the *"controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1* (Accountability).

16. Article 32 GDPR (Security of processing) materially provides:

1. *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

    (a) The pseudonymisation and encryption of personal data;
    (b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    (c) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    (d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

2. *In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

III. THE COMMISSIONER'S POWERS OF ENFORCEMENT

17. The Commissioner is the supervisory authority for the UK, as provided for by Article 51 of the GDPR.

18. By Article 57(1) of the GDPR, it is the Commissioner's task to monitor and enforce the application of the GDPR.

19. By Article 58(2)(d) of the GDPR the Commissioner has the power to notify controllers of alleged infringements of GDPR. By Article 58(2)(i) he has the power to impose an administrative fine, in accordance with Article 83, in addition to or instead of the other corrective measures referred to in Article 58(2), depending on the circumstances of each individual case.

20. When deciding whether to give a penalty notice to a person and when determining the amount of any penalty, section 155(2)(a) DPA requires the Commissioner to have regard to the matters set out in Article 83(1) and 83(2) GDPR to the extent that the notice concerns a matter to which the GDPR applies, so far as relevant.

21. Article 83(1) requires any penalty in each individual case to be *"effective, proportionate and dissuasive"*.

22. Article 83(2) requires the Commissioner to have due regard to the following matters when deciding to impose an administrative fine and deciding on the amount of the administrative fine in each individual case:

    (a) The nature, gravity, and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

    (b) The intentional or negligent character of the infringement;

    (c) Any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) *The degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*

(e) *Any relevant previous infringements by the controller or processor;*

(f) *The degree of co-operation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*

(g) *The categories of personal data affected by the infringement;*

(h) *The manner in which the infringement became known to the supervisory authority, including whether, and if so to what extent, the controller or processor notified the supervisory authority of the infringement;*

(i) *Where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject matter, compliance with those measures;*

(j) *Adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and*

(k) *Any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, directly or indirectly from the infringement.*

IV. THE COMMISSIONER'S REGULATORY ACTION POLICY

23. Pursuant to section 160(1) DPA, the Commissioner published his Regulatory Action Policy ("RAP") on 7 November 2018.

24. The process the Commissioner will follow in deciding the appropriate amount of penalty to be imposed is described in the RAP from page 27 onwards. In particular, the RAP sets out the following five step process:

a. Step 1. An 'initial element' removing any financial gain from the breach.
b. Step 2. Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2)–(4) DPA.
c. Step 3. Adding in an element to reflect any aggravating factors. A list of aggravating factors which the Commissioner would take into account, where relevant, is provided at page 11 of the RAP. This list is intended to be indicative, not exhaustive.
d. Step 4. Adding in an amount for deterrent effect to others.
e. Step 5. Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship). A list of mitigating factors which the Commissioner would take into account, where relevant, is provided at page 11-12 of the RAP. This list is intended to be indicative, not exhaustive.

V. REASONS WHY THE COMMISSIONER PROPOSES TO GIVE A PENALTY NOTICE

Factual background to the incident

25. The Gender Identity Clinic ("GIC") is a clinic within the Trust which accepts UK wide referrals for people with matters relating to gender. According to the Trusts' website it is the largest and oldest gender clinic in the UK, dating back to 1966.

26. The purpose of the Trust's [redacted] team is to increase involvement in all aspects of service planning and delivery by working collaboratively with patients, public stakeholders and Trust employees. In the latter part of 2019 the [redacted] became involved in the promotion of an art competition, the aim of which was to engage GIC patients in the clinic's refurbishment based on a need identified by patients in previous feedback to the service.

27. The Trust's intention was to send a bulk email relating to an art competition to approximately 5,000 GIC patients. The distribution list was extracted from the Trust's electronic patient record system using a specific set of search criteria which ensured recipients were active patients of the GIC and had consented to be contacted by email in certain circumstances. The output report produced from the system was then manually split into batches of around 1,000 addresses each.

28. At 14:22 on 6 September 2019 a member of staff in the [redacted] used Microsoft Outlook to generate an email communication which was initially sent to a total of 1,781 GIC patients. The email was sent in two batches comprising 912 and 869 email addresses respectively. In both batches the email addresses were copied from the output report and entered into the "To" field instead of the "Blind carbon copy" ("Bcc") field. The recipients of each email could therefore see the email addresses of the other recipients of that email. Four of the emails were returned as undeliverable and so potentially 1,777 emails were delivered and opened.

29. The email was an image-based advertisement for the upcoming arts competition. It is clear from the content that it was a competition welcoming submissions from the Trust's GIC patients and was

intended to assist with increasing the participation of this particular patient group.

30. The staff member who sent the email noticed the error straight away and attempted, albeit unsuccessfully, to recall both the emails. They also contacted the Trusts' Information Management and Technology Service Desk to report the breach. The remaining 3,000 or so emails were not sent.

31. The Trust took the following steps to notify the breach:

    a. 6 September 2019 at 15:56: The Trust sent an email to all affected data subjects about the incident, including an apology and contact details for recipients to seek support or make a formal complaint and a request to delete the message that had been sent at 14:22;
    b. 6 September 2019 within approximately 2 hours of the breach: Notification message posted on the Trust's website;
    c. 6 September 2019 at 16:41: The Trust notified the Information Commissioner's Office.

Nature of personal data involved

32. The personal data that was the subject of the breach comprised the email addresses of 1,781 data subjects revealed to others on the distribution list. An email address which clearly relates to an identified or identifiable living individual is considered to be personal data. The Trust confirmed that the majority of the email addresses are on public domains with either the first name or last name or initials in some way visible in the address.

33. Further research on any of the email addresses may, in any event allow for identification of a person via search engines, links to social media sites or similar.

34. Regarding the content of any email, this will not automatically contain additional personal data unless it includes information which reveals something about that individual or has an impact upon them.

35. In this case, it is considered that the nature of the email content, combined with the identity of the organisation sending the email, does reveal information about the recipients. Namely, that the recipients are identified as active patients of the GIC who have been invited to participate in an upcoming art competition hosted run by the Trust. Consequently, and to the extent to which the 1,781 individuals can be identified by the email distribution list, special category data can be inferred to a reasonable degree insofar as the disclosure of the email addresses connects those individuals with an organisation which provides gender identity related services. As such the data should be treated with the utmost care and afforded an elevated level of protection.

36. The Commissioner is minded to take the further view that even if the email addresses and the content of the email itself cannot be deemed to constitute special category data, it is clear there are particular sensitivities around the nature of the personal data being processed that the Trust should have considered in line with the Commissioner's guidance on Special Category Data[3].

[3] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

The Contravention

37. The Commissioner has considered whether the facts above constitute a contravention of the data protection legislation.

38. For the reasons set out below, and having carefully considered the Trust's representations, the Commissioner's view is that from 25 May 2018 to 6 September 2019, the Trust failed to comply with Chapter II GDPR, specifically Articles 5(1)(f), and 32(1) & (2) ("the infringement").

Article 5(1)(f) and Article 32(1) & (2) GDPR

39. The Commissioner finds that the Trust has failed to comply with the requirements of Article 5(1)(f) GDPR, including to process personal data *"in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing, using appropriate technical or organisational measures".* At the time of the infringement the Trust had in place some measures including:

    a. Availability of a Caldicott Guardian and IG Lead available for advice.

    b. A suite of policies, including "Email, Text and Internet Use Procedure" which states: *"To avoid inadvertently sharing other people's email addresses, recipients should be selected in the 'Bcc' box, not the 'To' box".*

c. Data security and protection training was available to all staff with measures in place to update this at timely intervals.

Whilst the measures above were in place prior to the personal data breach, they were insufficient in the circumstances, and particularly when the Trust was sending bulk emails that contained special category data and/or involved a high-risk group of patients.

40. The Trust has also failed to comply with the requirements of Article 32(1) and (2) GDPR. In particular:

a. Article 32(1)(b) GDPR required the Trust to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. By reason of such obligations, the Trust was required to ensure confidentiality of the personal data of its GIC patients. It failed to do so in this case.

b. Article 32(1)(d) GDPR required that the Trust had a process for regular testing, assessing and evaluating the effectiveness of technical and organisational controls for ensuring the security of processing. In 2017 the Trust experienced two incidents in a different, but similar, department which led to changes of process relating to multi-patient communications (further see paragraph 41(c) below). The Commissioner considers these incidents should have led the Trust to review the effectiveness of technical and organisational controls more widely across the Trust, and specifically relating to multi-patient communications to patients receiving gender related services, however it failed to do so.

41. By Article 32(1) GDPR, *"the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk",* taking into account *"the state of the art".*

As to *"the state of the art"*:

a. The state of the art includes knowledge, actual and constructive, of the current risks associated with this type of special category data at the date of the personal data breach, and whether the measures taken to protect the data are adequate in line with the state of current technologies.

b. The inadvertent use of the "To" rather than "Bcc" field in Outlook to insert email addresses for bulk communications has, for some time, been a known security risk. In this case the Trust was aware that it was sending bulk communications where the majority of the group email messages contained the names of clinic users. The recipients of the emails could infer that other recipients were also clinic users, which is confidential and special category data. The Trust should have been aware that there was a risk that staff working for the Trust could enter the group email addresses into the wrong field.

c. This is particularly so given that the Trust experienced two similar incidents on 15 September 2017 and 11 December 2017 involving a separate, but not dissimilar service: the Gender Identity Development Service ("GIDS"), which supports children and adolescents. The first incident involved an email sent to approximately 50 individuals and

the second was an email sent to 23 parents of patients. Both incidents involved the use of "To" rather than "Bcc" fields. At that time an action plan was completed, a change of process implemented for the sending of multi-patient communications within GIDS including management review and approval of any multi-patient communications, and additional training for all GIDS administrative staff. However, these processes were not implemented in other services across the Trust, including the GIC.

d. The Commissioner also notes that The Gender Recognition Act 2004 ("GRA") (which came into effect on 4 April 2005) describes that it is an offence for a person who has acquired protected information in an official capacity to disclose the information to any other person. Whilst the Commissioner is unaware whether protected information is involved in this case, the very existence of the GRA, aside from data protection legislation, should have highlighted the need for very stringent measures to protect the personal data of these individuals.

42. In view of the aforesaid, the Trust ought reasonably to have known that the group email addresses would be vulnerable to a security breach in the absence of appropriate technical and organisational measures.

43. The Trust failed to comply with the requirements of Article 5(1)(f) GDPR to process personal data in a manner that ensures appropriate security, including because it had not put in place appropriate measures to negate the risk of using the incorrect field when inputting patient email addresses into bulk communications.

The Commissioner considers the Trust should have addressed the following:

a. The Trust should have recognised the inherent risks in relying upon Outlook and "Bcc" for bulk communications involving special category data and/or high-risk groups of patients and should have used an alternative and more appropriate method of sending the emails, for example by procuring software with the capability of sending individual emails. Had the Trust implemented an alternative method of sending bulk emails following the 2017 incidents then this incident may well have been averted.

b. At the time of the incident the Trust's email server did not have a maximum recipient limitation policy applied to Outlook. The Trust could have applied a maximum number of emails which were able be sent at any one time.

c. The Trust failed to share the learning from previous incidents in 2017 or change the processes within similar services, such as GIC. For instance, before sending an email the Trust could have built in a double check procedure whereby an email instigated by one member of staff is cross checked by another. Such a procedure, alongside specific staff training, was implemented in GIDS following the 2017 incidents, however was not shared and implemented more widely amongst similar services, including GIC.

44. In regard to the requirement under Articles 32(1) and (2) of the GDPR to implement a level of security appropriate to the risk when processing data, the Commissioner considers that the Trust failed to

do so in this instance. The GDPR does not prevent an organisation from sending mass emails involving special category data. Rather, the GDPR requires that each organisation assess the risks arising in the context of their own circumstances and put controls in place to protect the personal data that it processes. The Trust has shown limited learning from the previous incidents in 2017 and has not evidenced that it deployed appropriate and proportionate controls to manage this risk more widely across the Trust, and in particular to clinics offering similar services including GIC.

VI. NOTICE OF INTENT

45. On 13 December 2021, in accordance with section 155(5) and paragraphs 2 and 3 of Schedule 16 DPA, the Commissioner issued the Trust with a Notice of Intent to impose a penalty under section 155 DPA. The Notice of Intent described the circumstances and the nature of the personal data breach in question, explained the Commissioner's reasons for a proposed penalty, and invited written representations from the Trust.

46. On 14 February 2022, the Trust provided substantial written representations, together with supporting documentation in relation to its finances.

47. On 30 March 2022 the Commissioner held a 'representations meeting' to thoroughly consider the representations provided by the Trust. At that meeting it was decided that a monetary penalty remained appropriate in all of the circumstances.

48. The Commissioner's view remains that the Trust has failed to comply with Articles 5(1)(f) and 32 GDPR. These failures fall within the scope of section 149(2) and section 155(1)(a) DPA.

VII. FACTORS RELEVANT TO WHETHER A PENALTY IS APPROPRIATE, AND IF SO THE AMOUNT OF THE PENALTY

49. The Commissioner has considered the matters listed in Articles 83(1) and (2) GDPR in coming to the view that a penalty notice is appropriate, and when determining the amount of such penalty. Without prejudice to the factual account above, the Commissioner has taken into account the following matters:

a. The nature, gravity and duration of the failure

i. This was a significant contravention of the GDPR. The Trust sent bulk emails to a total of 1,781 recipients, of which potentially 1,777 were delivered and opened. The majority of the email addresses contained the names or part of names of the affected data subjects. Email addresses can also be searched via social networks and search engines. It would therefore be possible for the unauthorised recipients of each respective email to identify the affected individuals.

ii. The recipients of the emails could infer from the email content that the other recipients were patients of GIC. This is confidential and special category data.

iii. The Trust failed to take more robust action after the GRA in 2005, and after the two previous breaches in 2017. These should have served as sufficient warning to the Trust to put in place more stringent measures regarding group emails, particularly regarding this group of individuals, however the weaknesses in the

process as highlighted above prevailed, including from 25 May 2018 (the advent of GDPR) until after this incident (6 September 2019).

iv. The consent booklet operated by the Trust did not clearly show that personal data may be used for engagement activities not directly related to clinical issues. It did not provide explicit consent for this particular type of bulk non-medical communication.

v. In terms of the assessment of damage suffered by affected data subjects, the Commissioner has regard to recital 85 GDPR which explains that "*physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned*".

vi. The Commissioner finds that the infringement is likely to cause distress to the service users who knew that their names had been disclosed to unauthorised recipients, who could infer that they were receiving support from the Trust with regard to gender identity matters. Further the service users would be distressed by justifiable concerns that their data has been further disseminated or misused by those who had access to it, even if those concerns do not

actually materialise. The Commissioner considers that such distress was likely to be substantial having regard to the number of affected individuals and the nature of the personal data involved.

vii. Approximately 30 minutes after the Trust sent the email, a recipient mentioned it via Twitter, and immediately thereafter the Trust's communications team received a phone call from a journalist who had been alerted to the infringement. The Trust confirmed that one Tweet it had viewed included a screenshot of one of the emails in which some email addresses were partially visible on screen.

viii. Newspaper articles reporting the infringement include quotes from affected individuals and refer to the incident as a "*horrendous breach of privacy*" which could impact people's lives, for example by "outing" individuals who had not informed their family or their community as to their gender status, where there may be "*a risk to them being known to be trans. That could be hugely dangerous to their wellbeing and safety*."

ix. The Trust received a total of 30 formal complaints made by or on behalf of 31 individuals. One of the complaints expresses concern that the Trust has exposed the individual to another who may cause ongoing harassment over email, and two contain content that the incident has had an impact on their mental health and wellbeing. Legal claims against the Trust have been brought by ten individuals as a

direct result of this incident (including a group claim of four). Five of these claims have been settled.

b. The intentional or negligent character of the infringement

i. The Commissioner accepts that the personal data breach was not intentional or deliberate. However, the Trust displayed a lack of consideration to protect personal data and was negligent.

ii. The Trust used Outlook to send bulk emails to 1,781 GIC service users. Therefore the Trust must have been aware that there was a risk that staff could enter the group email addresses into the wrong field, particularly after the previous security incidents in GIDS in 2017. In the circumstances the Trust ought reasonably to have known that the group email addresses would be vulnerable to a security breach in the absence of appropriate technical and organisational measures.

iii. The Trust recognised that there was an inherent risk in using Outlook to send bulk emails in 2017 given that at that time it changed the process within GIDS and implemented specific training for GIDS staff. The Trust therefore ought to have recognised the need to share the learning from these previous incidents and change the process within similar services including GIC.

iv. These issues should also have been considered alongside the Trust's responsibilities under the GRA which describes that it is an offence for a person who has acquired protected information in an official capacity to disclose the information to any other person. Whilst the information disclosed in this incident is not protected information per se, the very existence of this legislation should have highlighted the need for the Trust to have in place very stringent measures to protect the personal data of those individuals.

v. The Trust could have taken reasonable steps to prevent the contravention despite being aware of the risks, such as procurement of a more secure system for sending mass emails, introduction of a maximum number of emails capable of being sent at one time, and a system of double checking emails with associated staff training. The Trust failed to take any of those steps.

c. Any action taken by the controller to mitigate the damage or distress suffered by the data subjects

i. The staff member who sent the emails noticed the error immediately and attempted, albeit unsuccessfully, to recall the emails.

ii. Within one and a half hours of the infringement the Trust sent an email to all affected individuals notifying them of the incident. The emails issued an apology and a request that all recipients immediately

delete the previous email. It also provided contact details in the event concerned recipients wished to discuss or complain about the incident. Within about two hours of the incident the Trust issued a statement on its website.

iii. The Trust commenced an internal investigation into the incident.

d. The degree of responsibility of the controller or processor

i. The Trust failed in its obligations under Article 5(1)(f) to process personal data in a manner which ensured appropriate security of personal data and to take into account the considerations detailed in Article 32.

ii. In that regard, it is noted that the Trust was entirely responsible for implementing security measures to protect any personal data held by them and ensure technical and organisational measures appropriate to the risk were in place to protect personal data.

e. Relevant previous infringements

i. The Trust has confirmed there were two similar incidents on 15 September 2017 and 11 December 2017, both involving GIDS. In both instances the "To" rather than the "Bcc" fields were used to send multi-patient emails. At that time an action plan was agreed, and a change of process implemented within GIDS, along with additional staff training. The

learning from these incidents was not shared, nor change of process implemented more widely across the Trust, and in particular for clinics offering similar services such as GIC. Had this occurred this incident may well have been averted.

f. Degree of cooperation with the Commissioner

i. The Trust has fully co-operated with the Commissioner during this investigation and has provided evidence upon request.

ii. The Trust notified both the Commissioner and the affected data subjects promptly.

g. Categories of personal data affected

i. Email addresses of 1,781 data subjects were revealed to others on the email distribution list. Criteria for inclusion within the distribution list ensured the recipients were active patients of the GIC.

ii. The Trust confirmed that the majority of the email addresses have either the first name or last name or initials in some way identifiable. Further research on any of the email addresses may, in any event, allow identification of an individual via search engines or links to social media sites.

iii. By virtue of the content of the email it can be inferred that the other recipients were also service

users of GIC and thus an inference as to gender status can be drawn. In these circumstances the email addresses are special category data.

h. Manner in which the Infringement became known to the Commissioner

i. The Trust reported this incident to the ICO at 16:41 on 6 September 2019.

i. Compliance with any measures referred to in Article 58(2) having previously been ordered against the controller or processor

i. Not applicable.

j. Adherence to approved codes of conduct or certification mechanisms

i. Not applicable

k. Other aggravating factors applicable

i. The Trust had access to a technology solution in relation to marketing material which has the capability of addressing bulk emails to individual email accounts. It is not known why this was not in use in other areas of the Trust.

l. Other mitigating factors applicable

i. The Trust apologised to the recipients and has taken remedial action following the incident, including implementation of a secure mass-mailing platform in September/October 2019 which is utilised by the GIC, technical changes to its email system to limit the amount of external email recipients to 50 per email, and procurement of a new software facility for the sending of bulk emails which ensures recipient identities are hidden. The Trust has recently implemented new secure email software in the areas of highest risk, including gender services in February 2022, and which was intended to be deployed across the remainder of the Trust by late March 2022.

ii. At the time of the incident the Trust had established customs and practices surrounding public and patient involvement activities including an evidenced practice to blind copy individuals in bulk communications.

iii. At the time of the incident the Trust had a suite of policies, including the 'Email, Text and Internet use procedure' which states: *"To avoid inadvertently sharing other people's email addresses, recipients should be selected in the 'Bcc' box, not the 'To' box"*. 'Email Safety Top Tips/Guidance' includes mention of double-checking email addresses and what to do if an email is sent in error. This guidance has been refreshed and reissued specifically identifying risks of bulk emails. Staff are now encouraged to use an email send delay to enable staff to retrieve emails from their Outbox within the set delay period. The Trust has also published a new standard operating

procedure for staff communicating with patients which sets a specific process to follow to ensure bulk emails are sent securely.

iv. The Trust had measures to ensure all staff undertook data security and protection training at the commencement of their employment and routinely thereafter which covered information governance and data security, including the requirement to use the "Bcc" function" in any multi-patient communication. The staff member who sent the email had received this training.

v. The Trust has demonstrated data protection awareness in that a standardisation process took place in 2018 (following takeover by the Trust of the service from another provider in April 2017), and a revised consent form implemented for new patients from January 2019.

vi. The Trust has evidenced that consent was considered prior to sending the email and that some consents were in place. The Trust's Informatics team were involved in identifying individuals within the correct parameters of consent in order to communicate by email (albeit the consents did not explicitly cover bulk non-medical communications).

vii. The staff member who sent the email had previously sought guidance from the Trust's ICT team about how to send the bulk email to the intended 5000 or so recipients.

viii. Legal actions against the Trust have, or may, result in financial penalties for the Trust.

ix. The GIC is a UK wide based service so the likelihood of individuals knowing or identifying each other is reduced as the service is not provided to a small or localised geographical area.

x. There will be a significant impact on the Trust's reputation as a result of this security breach.

50. Taking into account all of the matters above, and in accordance with the Commissioner's Regulatory Action Policy[4], the Commissioner considers that the imposition of a penalty in this case is appropriate and would be effective, proportionate, and dissuasive in accordance with Article 83(1) GDPR. The nature, gravity, and scope of the breach were considerable, and a significant penalty would be an effective and dissuasive response to the failures by the Trust identified above in respect of the protection of its patient's personal data.

VIII. SUMMARY & PENALTY AMOUNT

51. For the reasons set out above, the Commissioner has decided to impose a financial penalty on the Trust. The Commissioner has taken into account publicly available information regarding its finances, together with further documentation provided by the Trust as to its financial position. He is mindful that the penalty must be effective, proportionate and dissuasive.

[4] https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf

52. As to the amount of the penalty:

a. The infringement of Article 5(1)(f) GDPR falls within Article 83(5)(a) GDPR.

b. There are no aggravating factors beyond the matters already taken into account above which lead the Commissioner to consider that the amount of the penalty should be increased further.

c. Considering the need for deterrent effect, the Commissioner notes that it is likely processing of this nature, and involving similar risks, is regularly undertaken in other similar environments, including those organisations serving public health needs. However it is considered that an administrative penalty itself will serve as a deterrent and that no further additional amount is required to achieve this outcome.

d. There are no mitigating factors beyond the matters already taken into account above which lead the Commissioner to consider that the amount of the penalty should be reduced.

e. The Commissioner has considered the financial impact upon the Trust as a result of the penalty.

f. Based on the scale and severity of the infringement, and having regard to the factors set out above, a penalty of **£78,400 (seventy eight thousand four hundred pounds)** is considered to be appropriate and proportionate.

53. Given the seriousness, nature and extent of the contraventions described above, the penalty imposed could have been significantly higher, up to £784,400 (seven hundred and eighty four thousand, four hundred pounds). However, in determining the amount of the final penalty in this case the Commissioner has taken into account the circumstances of the contravention and the public role of the organisation. This should not be taken as an indication that the Commissioner will always reduce a penalty in such circumstances. The Commissioner considers that this is a penalty that will be effective, proportionate and dissuasive, in accordance with Article 83 GDPR.

Payment of the penalty

54. The penalty must be paid to the Commissioner's office by BACS transfer or cheque by **9 July 2022** at the latest. The penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

55. There is a right of appeal to the First-tier Tribunal (Information Rights) against:

(a) the imposition of the monetary penalty and/or;

(b) the amount of the penalty specified in the monetary penalty notice.

56. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice.

57. Information about appeals is set out in Annex 1.

58. The Commissioner will not take action to enforce a monetary penalty unless:

- the period specified within the notice within which a monetary penalty must be paid has expired and all or any of the monetary penalty has not been paid;

- all relevant appeals against the monetary penalty notice and any variation of it have either been decided or withdrawn; and

- period for appealing against the monetary penalty and any variation of it has expired.

59. In England, Wales and Northern Ireland, the monetary penalty is recoverable by Order of the County Court or the High Court. In Scotland, the monetary penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

Dated the **9th** day of **June** 2022

Stephen Eckersley
Director of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

ANNEX 1

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 55B(5) of the Data Protection Act 1998 gives any person upon whom a monetary penalty notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.

2. If you decide to appeal and if the Tribunal considers:-

a) that the notice against which the appeal is brought is not in accordance with the law; or

b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

General Regulatory Chamber
HM Courts & Tribunals Service
PO Box 9300
Leicester
LE1 8DJ
Telephone: 0203 936 8963
Email: grc@justice.gov.uk

a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.

b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);

b) an address where documents may be sent or delivered to you;

c) the name and address of the Information Commissioner;

d) details of the decision to which the proceedings relate;

e) the result that you are seeking;

f) the grounds on which you rely;

g) you must provide with the notice of appeal a copy of the monetary penalty notice or variation notice;

h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may

conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (Information Rights) are contained in section 55B(5) of, and Schedule 6 to, the Data Protection Act 1998, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).