Maidstone and Tunbridge Wells NHS Trust

Ref: FOI/GS/ID 7143

Please reply to:
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone, Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net
www.mtw.nhs.uk

25 January 2022

Freedom of Information Act 2000

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to the inappropriate access to medical records by staff.

You asked:
1. Please provide the attached details of any member of staff who has been discovered to have inappropriately accessed any medical records within your Trust from 1 January 2019 to today's date. I have attached a table for completion with the specific information required.
a. how did the trust become aware of inappropriate access to medical records
b. staff group (medical, nursing etc) of member of staff responsible
c. number and type of medical records accessed (e.g. –2 x family members, own records, 1 x work colleague etc)
d. did the staff member use any information obtained from this access for any purpose? if yes, what purpose?
e. was the incident dealt with using the trust's disciplinary policy? if not, why not?
f. did a trust investigation take place?
g. was this referred to a trust disciplinary panel? if not, why not?
h. what was the outcome of the investigation and/or disciplinary panel?
i. what sanctions were placed on the staff member? e.g. – dismissal, warning, re-training
j. was the staff member reported to a professional body? e.g. – gmc/nmc?
2. Please provide a copy of your latest Trust wide Information Governance Audit showing the level of staff knowledge, understanding and adherence to the relevant legislation.
3. Please provide details on how often your Trust carries out audits to identify inappropriate access to medical records by staff.

Trust response:
1. Please see the following table:

How did the trust become aware of inappropriate access to medical records	Complaint received	Noticed by MTW employee	Concern raised by staff member	Concern raised by staff member	Concern raised by staff member	Concern raised by staff member	Concern raised by staff member	Concern raised by staff member
Staff group (medical, nursing etc) of member of staff responsible	Admin and Clerical	Admin and Clerical	Nursing	Admin and Clerical	Admin and Clerical	Nursing	Nursing	Medical
number and type of medical records accessed (e.g. –2 x family members, own records, 1 x work colleague etc)	1x Family Member	1x Family Member	1x Colleague	1x Colleague	1x Colleague	1x Colleague	1x Colleague	1x Family Member
Did the staff member use any information obtained from this access for any purpose? if yes, what purpose?	Yes	Yes	No	No	No	No	No	No
Was the incident dealt with using the trust's disciplinary policy? if not, why not?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
did a trust investigation take place?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Was this referred to a trust disciplinary panel? if not, why not?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
What was the outcome of the investigation and/or disciplinary panel?	Formal action taken following investigation	Formal action taken following investigation	Formal action taken following investigation	Formal action taken following investigation	Formal action taken following investigation	Formal action taken following investigation	Formal action taken following investigation	Formal action taken following investigation
What sanctions were placed on the staff member? e.g. – dismissal, warning, re-training	Final Written Warning	First written warning	Final Written Warning	Final Written Warning	Final Written Warning	Dismissal	Final Written Warning	Dismissal
Was the staff member reported to a professional body? e.g. – gmc/nmc?	No	No	No	No	No	No	No	No

2.
Information Governance – Staff Awareness Survey – 2020/21

	Description	Agree	Disagree
1.	Leadership – I feel data security and protection are important for my organisation	96.92%	3.08%
2.	Policies – I know the rules about who I share data with	98.46%	1.54%
3.	Policies – I know who to ask questions about data security in my organisation	86.15%	13.85%
4.	Policies – I am happy data is used legally and securely in my organisation	84.62%	15.38%
5.	Sharing data securely – I know how to transmit data securely	95.38%	4.62%
6.	Using data legally and securely – I feel that patient confidentiality is more important than sharing information for individual care	61.90%	38.10%
7.	Processes – The tools and processes used by my organisation make it easy to use and transmit data securely	85.71%	14.29%
8.	Raising concerns – I can raise concerns about unsecure or unlawful uses of data, and I know that these will be acted on without personal recrimination	82.54%	17.46%
9.	Laws and principles – I understand the important laws and principles on data sharing, and when I should and should not share data	96.92%	3.08%
10.	Data sharing – If I have a question about sharing data lawfully and securely I know where to seek help	87.50%	12.50%
11.	Personal responsibility – I take personal responsibility for handling data securely	98.46%	1.54%
12.	Training – The data security training offered by my organisation supports me in understanding who to use data lawfully and securely	92.31%	7.69%
13.	Access to information – The level of access I have to IT systems holding sensitive information, is appropriate	95.38%	4.62%
14.	Reporting – I know how to report a data security breach	86.15%	13.85%
15.	Incidents – When there is a data security incident my organisation works quickly to address it	85.94%	14.06%
16.	Learning lessons – When there is a data security incident, or near miss, my organisation learns lessons and makes changes to prevent it happening again	81.97%	18.03%
17.	Contingency plan – If a data security incident was to prevent technology from working in my organisation I know how to continue doing the critical parts of my job	81.25%	18.75%

3. Audits are conducted at least annually and on an ad-hoc basis as required.