# Freedom of Information Request - 1589

In your request you asked for the following information: -

> Can you tell me how many of the following there have been at your organisation for each of the last three financial years.
>
> · Incidents of lost data
> · Breaches of confidentiality
> · Other security or confidentiality breaches with regards to data
>
> Please include descriptions of each incident.

In response to the above: -

> The Trust records incidents in relation to Information Governance under specific headings (Information Governance Incident Reporting Codes below), incidents are then graded in relation to the harm caused (see page 3), incidents are then investigated and actioned appropriately. It is important to note that not all instances result in a breach of confidentiality i.e. information could be reported missing and later found in a secure location.
>
> Please see pages 4 to 8 for a list of reported actual and suspected breaches of confidentiality and data breaches including year, incident code and harm caused.

Information Governance Incident Reporting Codes

G1A Confidentiality Incident - Within Staff (Verbal)
G1B Confidentiality Incident - Within The Hospital (Verbal)
G1C Confidentiality Incident - Outside The Hospital (Verbal)
G2A Patient Information Inaccurate (Written Or Electronic)
G2B Patient Information Lost Or Missing Sections (Written Or Electronic)
G2C Unauthorised Disclosure Or Use Of Patient Information (Written, Verbal Or Electronic)
G2D Patient Information Left In Unsecure Area Of The Trust
G2E Patient Information Found Outside The Trust
G3A Misfiled/Inaccurate/Illegible Staff Or Corporate Information (Written Or Electronic)
G3B Lost/Missing Staff Or Corporate Information (Written Or Electronic)
G3C Unauthorised Disclosure Or Use Of Staff Or Corporate Information (Written, Verbal Or Electronic)
G4A Unauthorised Destruction Of Information (Written Or Electronic)
G4B Theft Of Information (Written Or Electronic)
G4C Information Incident - Suspicious Request For Information (Written, Verbal Or Electronic)
G4D Information Incident - Breach In Safe Haven Policy/Other IG Policy
G4E Information Incident - Caused By External Provider/Other Party
G5A Password Incident - Unauthorised Use/Disclosure
G5B E-Mail Incident - Incorrect Recipient/Unauthorised Use
G5C Removable Media Incident - Unauthorised Use

The Trust grades the severity of an incident (harm caused) using a table based on the SUI Guidance provided by the Department of Health.

| Governance/ Information Governance | | | | | |
|---|---|---|---|---|---|
| **Descriptor** | **No Harm (Insignificant)** | **Low Harm (Minor)** | **Moderate Harm** | **Major Harm** | **Catastrophic Harm** |
| **Information Governance** | ** Final grading will be determined by the Information Governance Team taking into account the examples below, CFH SUI guidance and guidance issued by the Information Commissioners Office. | | | | |
| | Potential breach of information rights law(s) – no risk e.g.<br>• Potential breach involving encrypted records and/or,<br>• Potential breach involving unencrypted records and or,<br>• Potential breach with less than 5 people affected. | Potential breach or low risk breach of information rights law(s) – low risk e.g.<br>• Breach involving no sensitive personal information and/or,<br>• Breach involving up to 20 people which is unlikely to result in harm or distress. | Breach of information rights law(s) – Moderate Risk e.g.<br>• Involves personal information or sensitive personal information which is likely to result in harm or distress and/or<br>• Affects 21-100 people. | Breach of information rights law(s) – High Risk e.g.<br>• Involves personal information or sensitive personal information which has resulted in harm or distress and/or<br>• Affects 100-1000 people and/or,<br>• Involves significant amount of sensitive personal data up to 100 people. | Breach of information rights law(s) – Very High Risk e.g.<br>• Involves personal information or sensitive personal information resulting in significant harm or distress or with potential for ID theft and/or,<br>• Affects over 1000 people and/or,<br>• Involves significant amount of sensitive personal data relating to more than 100 people. |
| **Inspection/ Statutory Duty** | Small number of recommendations which focus on minor quality improvement issues<br>No or minimal impact or breach of guidance / statutory duty nor concerns in relation to regulatory standards | Minor recommendations which can be implemented by low level of management action<br>Breach of Statutory legislation<br>Enquiry from Regulator<br>Breach of Statutory legislation<br>No audit trail to demonstrate that objectives are being met (NICE; HSE; NSF etc.) | Challenging recommendations which can be addressed with appropriate action plans<br>Single breach of statutory duty<br>Non-compliance with standards 50% of objectives within standards met<br>Moderate SUI reportable to the Regulator<br>Improvement notice served<br>Audit from Regulator | Enforcement notice<br>Information notice<br>Multiple breaches of statutory duty<br>Improvement Notice<br>Critical Report<br>Low performance rating<br>Major non-compliance with regulatory standards | Multiple breaches of statutory duty<br>Prosecution<br>Fine from Regulator<br>Severely critical report<br>Zero performance rating<br>Complete systems change required<br>No objectives / standards being met<br>Damages Claim / Identity Theft<br>Loss of Registration with CQC |

## Information Governance Incidents

Although the tables below show an increase in the number of incidents reported over each financial year; The Trust attributes this increase to the increased awareness around Information Governance as a result of training rather than an actual increase in the number of incidents occurring. Staff are actively encouraged to report all incidents or issues so that lessons can be learned. All incidents are monitored by the Information Governance Team who issued guidance, provide equipment or training to prevent any reoccurrences.

Awareness has increased significantly over the past few years as Information Governance training has becoming mandatory annual training for all staff. By the end of 2012/13 a total of 3496 staff had completed their annual Information Governance training which is approximately 90% of all staff, students and volunteers at the Trust.

The majority of incidents that have been reported at the Trust result in no harm or low harm and are not usually a result of a breach of confidentiality i.e. information could be reported missing and later found in a secure location. Three incidents which resulted in moderate harm have been reported in the three financial years, and further details are provided below. There were no major or catastrophic incidents reported in the last three financial years.

### Incidents resulting in Moderate Harm

### 2011/12 G2C - Unauthorised Disclosure Or Use of patient information

In this incident a staff member issued a set of patient hand held notes which appeared to be blank to a patient. The first half of the notes were blank; however, the second half already contained the details of another patient. This was as a result of a change of documentation. The patient brought the error to the attention of the Trust at their next appointment.

The Trust conducted a Root Cause Analysis to investigate this incident. Additionally, the Trust wrote an apology to both patients involved explaining how the incident occurred. The Trust had already risk assessed this processed and as a result, guidance was available for staff using these notes. In this case the guidance was not followed by the staff member. As a result the guidance was re-issued and appropriate management action was taken against the staff member.

The Trust reported the incident to the ICO who did not take any formal action against the Trust and stated that:

“We welcome the remedial steps taken by the Trust in light of this incident….after careful consideration and based on the information provided, we have decided not to take any formal enforcement action on this occasion. This decision is due to the particular facts of this case and the remedial measures set out by the Trust, which we expect will continue to be implemented in order to prevent any recurrence.”

2012/13 – G2E - Patient Information Found Outside The Trust (2 incidents)

In these incidents handover sheets containing information about in-patients were found in two separate public locations. It is Trust policy that all handover sheets are placed in confidential waste bags at the end of each shift. These two incidents were caused by two separated staff members not following Trust policy.

The Trust conducted a Root Cause Analysis to investigate these incidents. Urgent reminders were issued via email and the intranet to all staff, and posters reminding staff members of their responsibilities were distributed throughout the Trust. The Trust also conducted inspections of Wards to ensure the posters were displayed and shred bags were readily accessible.

The Trust reported the incident to the ICO who did not take any formal action against the Trust and stated that:

"…it is recognised that staff members are not permitted to take handover sheets off Trust premises and are expected to place them into confidential shredding bags before leaving. In doing so, the employees responsible for these losses were in direct breach of the Trust's procedures.

Therefore, after careful consideration and based on the information provided, we have decided not to take any formal enforcement action on this occasion. This decision is due to the particular facts of the case and the current processes in place at the Trust, which we expect will continue to be implemented in order to prevent any recurrences."

| Financial Year | Information Governance Incident Reporting Codes | Actual Impact | Number of Incidents Reported |
|---|---|---|---|
| 2010/2011 | G1A - Within Staff (Verbal) | 1 - No Harm | 1 |
| | G1C - Outside The Hospital (Verbal) | 1 - No Harm | 2 |
| | G2A - Patient Information Inaccurate (Written or Electronic) | 1 - No Harm | 8 |
| | | 2 - Low Harm | 2 |
| | G2B - Patient Information Lost Or Missing Sections (Written or Electronic) | 1 - No Harm | 1 |
| | G2C -Unauthorised Disclosure Or Use Of Patient Information (Written, Verbal or Electronic) | 1 - No Harm | 14 |
| | | 2 - Low Harm | 5 |
| | G2D - Patient Information Left In Unsecure Area Of The Trust | 1 - No Harm | 13 |
| | | 2 - Low Harm | 2 |
| | G3A - Misfiled/Inaccurate/Illegible Staff Or Corporate Information | 1 - No Harm | 2 |
| | G3B - Lost/Missing Staff Or Corporate Information | 1 - No Harm | 3 |
| | G3C - Unauthorised Disclosure Or Use Of Staff Or Corporate Information | 1 - No Harm | 3 |
| | G4B - Theft Of Information (Written or Electronic) | 1 - No Harm | 1 |
| | G4C - Suspicious Request For Inform (Written, Verbal Or Electronic) | 1 - No Harm | 3 |
| | G4D - Breach Of Information Governance Policy/Guidance | 1 - No Harm | 2 |
| | | 2 - Low Harm | 1 |
| | G4E - Caused By External Provider/Other Party | 1 - No Harm | 4 |
| | G5A - Password Incident - Unauthorised Use/Disclosure | 1 - No Harm | 1 |
| | G5B - E-Mail Incident - Incorrect Recipient/Unauthorised Use | 1 - No Harm | 2 |
| | | **2010/2011 Total** | **70** |

| Financial Year | Information Governance Incident Reporting Codes | Actual Impact | Number of Incidents Reported |
|---|---|---|---|
| 2011/2012 | G1A - Within Staff (Verbal) | 1 - No Harm | 2 |
| | G1B - Within The Hospital (Verbal) | 2 - Low Harm | 1 |
| | G1C - Outside The Hospital (Verbal) | 1 - No Harm | 4 |
| | | 2 - Low Harm | 1 |
| | G2A - Patient Information Inaccurate (Written or Electronic) | 1 - No Harm | 16 |
| | G2B - Patient Information Lost Or Missing Sections (Written or Electronic) | 1 - No Harm | 6 |
| | | 2 - Low Harm | 2 |
| | G2C -Unauthorised Disclosure Or Use Of Patient Information (Written, Verbal or Electronic) | 1 - No Harm | 16 |
| | | 2 - Low Harm | 7 |
| | | 3 - Moderate Harm | 1 |
| | G2D - Patient Information Left In Unsecure Area Of The Trust | 1 - No Harm | 21 |
| | | 2 - Low Harm | 2 |
| | G2E - Patient Information Found Outside The Trust | 1 - No Harm | 1 |
| | | 2 - Low Harm | 1 |
| | G3A - Misfiled/Inaccurate/Illegible Staff Or Corporate Information | 1 - No Harm | 1 |
| | G3B - Lost/Missing Staff Or Corporate Information | 1 - No Harm | 1 |
| | G3C - Unauthorised Disclosure Or Use Of Staff Or Corporate Information | 1 - No Harm | 1 |
| | G4C - Suspicious Request For Inform (Written, Verbal Or Electronic) | 1 - No Harm | 2 |
| | G4E - Caused By External Provider/Other Party | 1 - No Harm | 4 |
| | | 2 - Low Harm | 1 |
| | G5B - E-Mail Incident - Incorrect Recipient/Unauthorised Use | 1 - No Harm | 3 |
| | | **2011/2012 Total** | **94** |

| Financial Year | Information Governance Incident Reporting Codes | Actual Impact | Number of Incidents Reported |
|---|---|---|---|
| 2012/2013 | G1B - Within The Hospital (Verbal) | 1 - No Harm | 6 |
| | | 2 - Low Harm | 1 |
| | G1C - Outside The Hospital (Verbal) | 1 - No Harm | 6 |
| | | 2 - Low Harm | 2 |
| | G2A - Patient Information Inaccurate (Written or Electronic) | 1 - No Harm | 18 |
| | | 2 - Low Harm | 3 |
| | G2B - Patient Information Lost Or Missing Sections (Written or Electronic) | 1 - No Harm | 16 |
| | | 2 - Low Harm | 3 |
| | G2C -Unauthorised Disclosure Or Use Of Patient Information (Written, Verbal or Electronic) | 1 - No Harm | 41 |
| | | 2 - Low Harm | 14 |
| | G2D - Patient Information Left In Unsecure Area Of The Trust | 1 - No Harm | 47 |
| | | 2 - Low Harm | 14 |
| | G2E - Patient Information Found Outside The Trust | 1 - No Harm | 1 |
| | | 2 - Low Harm | 2 |
| | | 3 - Moderate Harm | 2 |
| | G3A - Misfiled/Inaccurate/Illegible Staff Or Corporate Information | 1 - No Harm | 1 |
| | | 2 - Low Harm | 1 |
| | G3B - Lost/Missing Staff Or Corporate Information | 1 - No Harm | 5 |
| | | 2 - Low Harm | 1 |
| | G3C - Unauthorised Disclosure Or Use Of Staff Or Corporate Information | 1 - No Harm | 3 |
| | | 2 - Low Harm | 2 |
| | G4C - Suspicious Request For Inform (Written, Verbal Or Electronic) | 1 - No Harm | 3 |
| | G4D - Breach Of Information Governance Policy/Guidance | 1 - No Harm | 7 |
| | | 2 - Low Harm | 3 |
| | G4E - Caused By External Provider/Other Party | 1 - No Harm | 12 |
| | | 2 - Low Harm | 3 |
| | G5A - Password Incident - Unauthorised Use/Disclosure | 1 - No Harm | 2 |
| | G5B - E-Mail Incident - Incorrect Recipient/Unauthorised Use | 1 - No Harm | 7 |
| | | 2 - Low Harm | 2 |
| | G5C - Removable Media Incident - Unauthorised Use | 1 - No Harm | 1 |
| | | **2012/2013 Total** | **229** |

Please feel free to contact me if you would like to discuss your request further. If you are not satisfied with this response, you have the right to appeal. In the first instance, please contact the Trust's Governance Manager who will initiate an internal review. The Trust will then review its decision and respond to your appeal, as soon as possible, but within 20 working days. If, following the review, you are still not satisfied with the way we have handled your request, or if you are unhappy with our response, then under Section 50 of the Act, you are entitled to appeal to the Information Commissioner.