Document filename: **Annual Information Governance (IG) Incident Trends (2015-2016)**

| | | | |
|---|---|---|---|
| **Directorate / Programme** | NHS Digital External IG Delivery | **Project** | IG Incident Reporting |
| **Document Reference** | | | |
| **Project Manager** | James Burleigh | **Status** | Final |
| **Owner** | Marie Greenfield | **Version** | 1.0 |
| **Author** | James Burleigh | **Version issue date** | 15/09/2016 |

# Annual Information Governance (IG) Incident Trends (2015-2016)

# Contents

# Executive Summary

## Background

In June 2013 the Department of Health (DH) mandated all organisations providing or supporting Health and Care services in England to report incidents relating to data protection breaches[1] via the IG Incident Reporting Tool (part of the Information Governance Toolkit). This was mandated through a requirement in the IG Toolkit.

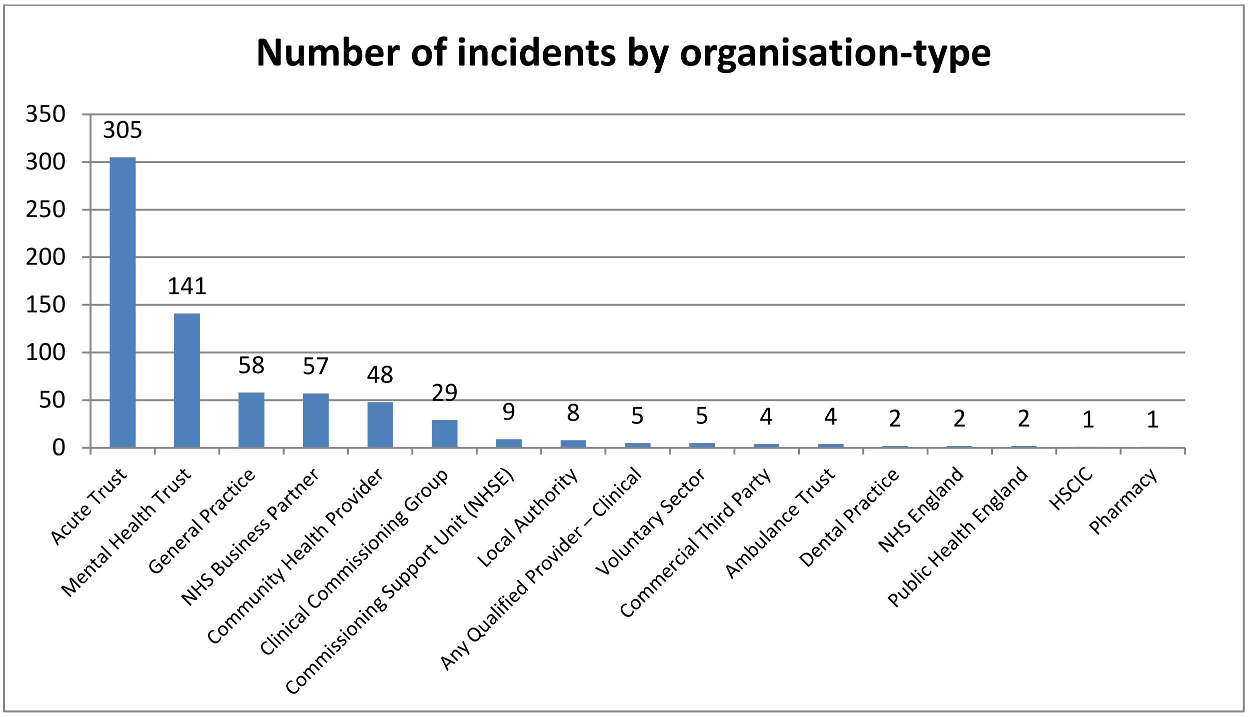
Where an incident's severity rating is assessed as serious the Information Commissioner's Office (ICO), NHS England (NHSE) and DH are informed by automatic e-mail. (Note that the new EU General Data Protection Regulation which may come into force in 2018 will make the reporting of data protection breaches within 72 hours of occurrence a legal requirement).

A scoring mechanism agreed with the Information Commissioner's Office helps organisations identify those incidents which are serious enough to report and helps populate the incident reports with the details.

Reporting of trivial incidents and near misses is optional and can be recorded in the Reporting Tool but it is not mandatory to do so and there are significant issues relating to burden and the difficulty of defining what is actually a near miss that makes standardisation problematic.

The body of this report details the numbers and types of incidents reported by Health and Adult Social Care organisations in England using the IG Incident Reporting Tool during the period 1 June 2015 to 31 May 2016.

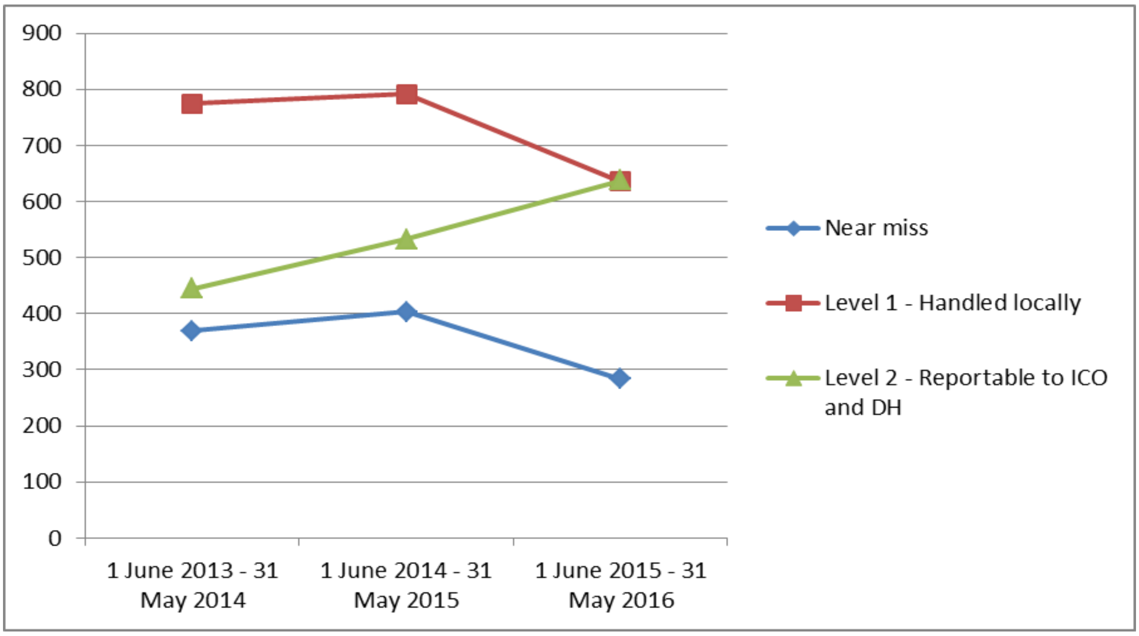
## What have we seen?



[1] From May 2015 cyber security incidents, which may or may not be data protection breaches (e.g. web site defacement) must also be reported but the numbers reported are very low and we do not have comparable figures for earlier years. It is probable that CareCert will collect more meaningful data on these types of incidents.

- Reportable data protection breaches increased to 681 last year compared to 533 in 2014-15 and 445 in 2013-2014. Most are reported by NHS Trusts.
- The 'top 3' types of data protection breaches, accounting for 77% of incidents, were all due to human error or criminal intent:
  - 'Disclosed in error' (50%)
  - 'Lost or stolen paperwork' (14%)
  - 'Unauthorised access/disclosure' (13%)

- These top 3 incident types have accounted for over 75% of all incidents reported in each of the past 3 years.
- The large data protection breaches resulting from loss of unencrypted lap tops and memory sticks prevalent in 2008-2011 appear to have been eliminated.
- Less than 1% of breaches were cyber security related, perhaps a reflection that most cyber incidents impact on service delivery rather than data, but under reporting may also be a factor.



## What does this tell us? What actions are required?

- More organisations are using the Reporting Tool each year. The increased level of reporting, however may not fully account for the increased number of reported incidents i.e. the actual number of incidents may be increasing.
- We cannot distinguish between organisations having few breaches due to their business model (e.g. pharmacies have no reason to put data at risk) and those that "under-report".
- From May 2015, at the request of Department of Health (in the context of the early Cyber Security Programme), cyber security incidents, which may or may not be data protection breaches, must also be reported – the numbers reported are very low and we do not have comparable figures for earlier years.

  **Recommended action**: Work is required in partnership with NHS England and the Local Government Association to mandate/encourage reporting in a consistent manner across the health and care system maybe by improving contractual arrangements.

- Human error and criminal activity account for the great majority of incidents. These must be tackled by local organisations through cultural change, training, policies, reviewing procedures and effective monitoring of internal performance.

  **Recommended action**: IG training that all staff must undertake should be updated to focus on practical steps to reduce human errors and support the cultural change required. This should be linked to plans for implementing the recommendations from the National Data Guardian (NDG) review.

- The new security standards recommended by the NDG review, supported by independent assurance, should harden health and care sector defences on data security and we need to ensure that this will help prevent data protection breaches due to human error or criminal activity as well.

  **Recommended action**: The elements of the IG Toolkit that address cultural change, training, policies, procedures and local codes of conduct should be strengthened and better focussed on best practice and avoiding human error.

- Analysis of incidents and the way that local organisations have scored them using the Incident Reporting Tool should be reviewed especially as we move to legally required incident reporting (EU General Data Protection Regulation) which is likely from 2018-19 onwards.

  **Recommended action**: The guidance on incident scoring needs to be reviewed in conjunction with ICO and DH policy colleagues.

## Summary

The number of incidents reported is increasing annually. This may be because an increasing number of organisations are becoming aware of the need to report incidents or may indicate an increase in the number of incidents.

The most common data breach is ‘disclosed in error’ and the highest level of reporting is by NHS Trusts.

Steps should be taken to implement recommendations made in the NDG review to re-inforce messages about the need to improve data management and security and also to encourage greater reporting, including where near misses have occurred.

# 1. Introduction

This is the second annual report produced by NHS Digital to highlight trends in reporting of Information Governance (IG) incidents (some typical incidents are provided as examples in Annex B). This report covers the period 1 June 2015 to 31 May 2016 and provides statistics of IG incidents reported by Health and Adult Social Care organisations in England using the 'IG Incident Reporting Tool'[2].

The Reporting Tool is a component of the IG Toolkit and enables health and social care staff to gauge the potential impact of incidents using standardised criteria (described in the Reporting Tool) for measuring volume and sensitivity of the data affected. The criteria determine the severity level rating. Where an incident's severity rating is assessed as serious the Information Commissioner's Office (ICO), NHS England and the Department of Health (DH) are informed by automatic e-mail. Incidents are categorised by type (see Annex A).

The criteria were developed in partnership with the ICO and a serious incident is likely to be a breach of the Data Protection Act 1998 and will involve information about identifiable or potentially identifiable individuals. Where data is extremely sensitive this may be information about a single identifiable individual, however, an incident involving fifty individuals might still be classed as serious (even if no confidential clinical information is involved). Note that from 2018 it is likely that the reporting of data protection breaches within 72 hours of occurrence will become a legal duty as a result of the new EU Data Protection regulation coming in to force (England will not leave the EU before this comes in to force).

The ICO has the enforcement powers to fine organisations that commit serious breaches of the Data Protection Act up to £500,000 for each breach, but this maximum will increase when the new Regulation comes into effect. During 2015-16 two monetary penalties were imposed in the health and care sector:

- Blackpool Teaching Hospitals NHS Foundation Trust inadvertently published the private details of 6,574 members of staff, including their National Insurance number, date of birth, religious belief and sexual orientation. The Trust has been fined £185,000.
- Chelsea and Westminster Hospital NHS Foundation Trust was fined £180,000 after revealing the email addresses of more than 700 users of an HIV service.

Incident reporting is mandatory for all organisations that must complete the IG Toolkit, which covers NHS Trusts, those working under NHS national contracts and pharmacies. It is not mandatory for GP Practices, Local Authorities or others that complete the IG Toolkit on a voluntary basis. Nevertheless, the mandatory incident reporting for many Health and Social Care bodies in England provides a higher level and more reliable and complete reporting allowing a comprehensive picture of the causes and trends of breaches of personal data than is available in other sectors.

The reasons for the high level of reporting are acknowledged in the ICO Data Security Incident Trends[3] "*The health sector continued to account for the most data security incidents. This was due to the combination of the NHS making it mandatory to report incidents, the size of the health sector, and sensitivity of the data processed*". We might add to that the high risk environment that many parts of the care sector work within e.g. in people's homes, open access buildings, peripatetic working etc also contribute to the volume of incidents.

[2] The IG Incident process is contained in the document 'Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation' at https://www.igt.hscic.gov.uk/resources/IGIncidentsChecklistGuidance.pdf.

[3]: Data security incident trends. Information Commissioners Office: https://ico.org.uk/action-weve-taken/data-security-incident-trends/

# 2. Scope

The report covers the IG incidents reported by Health and Adult Social Care organisations in England using the IG Incident Reporting Tool for the period 1 June 2015 to 31 May 2016.

The report covers reportable data protection breaches but separately considers what may be learned from near misses and incidents that are not significant enough to report. Whilst a very small number of cyber security incidents also involve data protection breaches and are included in this report, cybersecurity analysis and reporting is out of scope for this report.

# 3. Reported Incidents 2015-16

### 3.1 Total incidents reported with the previous 2 years for comparison

| | Year to 31 May 2016 | Year to 31 May 2015 | Year to 31 May 2014 |
|---|---|---|---|
| **Reported Incidents** | 681 | 533 | 445 |

Approximately 28,000 organisations are currently required to report IG incidents through the Reporting Tool but outside of the large NHS Trusts who undergo internal audit each year there is no policing of the system.

The number of reported incidents suggests that the position is worsening year on year. The increasing number of organisations using the reporting tool each year only partially explains the overall increase as the majority of incidents are reported by long standing large NHS organisations, not those new to reporting. The reasons for the increase are also unknown.

### 3.2 Total incidents reported by organisation type

| Organisation Type | No. | Organisation Type | No. |
|---|---|---|---|
| Acute Trust | 305 | Voluntary Sector | 5 |
| Mental Health Trust | 141 | Commercial Third Party | 4 |
| General Practice | 58 | Ambulance Trust | 4 |
| NHS Business Partner | 57 | Dental Practice | 2 |
| Community Health Provider | 48 | NHS England | 2 |
| Clinical Commissioning Group | 29 | Public Health England | 2 |
| Commissioning Support Unit (NHSE) | 9 | NHS Digital | 1 |
| Local Authority | 8 | Pharmacy | 1 |
| Any Qualified Provider – Clinical | 5 | | |

The number of reported incidents – 681 – from some 28,000 organisations mandated to use the Reporting Tool suggests that the majority do not have a reportable incident in the course of an average year and that even those that do will have no more than a small number. It can be argued that the NHS operates necessarily in a high risk way with services being delivered in people's homes, mobile clinics etc and with hospitals permitting members of the public to access many parts of the estate and therefore that a number of incidents is inevitable. Nevertheless the target should always be zero.

We cannot distinguish between organisations having few breaches due to their business model (e.g. pharmacies have no reason to put data at risk) and those that under report (FOI requests from the privacy lobby indicate that Local Authorities have as many incidents as the NHS but do not report them via the Reporting Tool).

### 3.3 Types of reported incident

| Incident Type | No. | Incident Type | No. |
|---|---|---|---|
| Disclosed in Error | 319 | Technical security (Cyber) | 7 |
| Unauthorised Access/Disclosure | 110 | Uploaded to website in error | 5 |
| Lost or stolen paperwork | 92 | Inability to recover digital data | 5 |
| Lost In Transit | 29 | Non-secure Disposal – hardware | 2 |
| Non-secure Disposal – paperwork | 33 | Other | 62 |
| Lost or stolen hardware | 17 | | |

The large data protection breaches resulting from loss of unencrypted lap tops and memory sticks prevalent in 2008-2011 appear to have been eliminated. Less than 1% of breaches were cyber security related, perhaps a reflection that most cyber incidents impact on service delivery rather than data, but under reporting may also be a factor.

Whilst a sizeable number of incidents were reported as ‘other’, analysis of these suggests that the majority should have been assigned to one of the existing categories.

The ‘top 3’ types of data protection breaches, accounting for 77% of incidents, were all due to human error or criminal intent, i.e. Disclosed in error (47%), Unauthorised access/disclosure (16%) and Lost or stolen paperwork (14%). These top 3 incident types have accounted for over 75% of all incidents reported in each of the past 3 years.

### 3.4 Organisation type mapped to incident type

| Incident Type / Organisation Type | Disclosed in Error | Unauthorised Access/Disclosure | Lost or stolen paperwork | Lost In Transit | Non-secure Disposal – paperwork | Lost or stolen hardware | Technical security (Cyber) | Uploaded to website in error | Inability to recover digital data | Non-secure Disposal – hardware | Other | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Acute Trust | 145 | 39 | 41 | 13 | 21 | 8 | 5 | 2 | 2 | 2 | 27 | 305 |
| Mental Health Trust | 65 | 35 | 19 | 4 | 3 | 4 | | | 1 | | 10 | 141 |
| General Practice | 29 | 9 | 5 | 4 | 4 | 1 | 2 | 1 | 1 | | 2 | 58 |
| NHS Business Partner | 31 | 8 | 4 | 1 | 1 | | | | | | 12 | 57 |
| Community Health | 17 | 7 | 12 | 4 | 2 | 1 | | | | | 5 | 48 |
| CCG | 16 | 5 | 3 | | 1 | | | 1 | | | 3 | 29 |
| CSU | 5 | 1 | 2 | 1 | | | | | | | | 9 |
| Local Authority | 3 | 1 | 1 | 1 | 1 | | | | | | 1 | 8 |
| AQP Clinical | 3 | 1 | | | | 1 | | | | | | 5 |
| Voluntary Sector | | 1 | 1 | | | 1 | | | 1 | | 1 | 5 |
| Commercial Third Party | 3 | | | | | | | 1 | | | | 4 |
| Ambulance Trust | 1 | 1 | 2 | | | | | | | | | 4 |
| Dental Practice | | 1 | | | | 1 | | | | | | 2 |
| NHS England | 1 | | 1 | | | | | | | | | 2 |
| Public Health England | | 1 | | 1 | | | | | | | | 2 |
| NHS Digital | | | | | | | | | | | 1 | 1 |
| Pharmacy | | | 1 | | | | | | | | | 1 |
| | 319 | 110 | 92 | 29 | 33 | 17 | 7 | 5 | 5 | 2 | 62 | 681 |

It is clear that the preponderance of incidents caused by human error and criminal intent is not confined to the large NHS Trusts but reflects the profile of all organisations.

# 4. Incidents that did not meet the criteria for reporting

Organisations are not currently mandated to report incidents that do not score as significant in the Reporting Tool or which might be classed as ‘near misses’. Nevertheless, some, though not all, organisations capture low level incidents and at least some near misses as they use the tool as a local incident management support system.

### 4.1 Number of low level and near miss incidents recorded 2015-16 by organisation type

| Organisation Type | Near miss | Non reportable |
|---|---|---|
| Acute Trust | 83 | 303 |
| Mental Health Trust | 135 | 189 |
| General Practice | 19 | 61 |
| NHS Business Partner | 34 | 72 |
| Community Health | 6 | 8 |
| CCG | 12 | 21 |
| CSU | 0 | 2 |
| Local Authority | 3 | 14 |
| AQP Clinical | 2 | 20 |
| Voluntary Sector | 3 | 7 |
| Commercial Third Party | 2 | 3 |
| Ambulance Trust | 0 | 4 |
| Dental Practice | 0 | 2 |
| NHS England | 0 | 0 |
| Public Health England | 0 | 0 |
| NHS Digital | 1 | 1 |
| Pharmacy | 2 | 1 |
| **Totals** | **303** | **709** |

Although any analysis of these figures needs to be undertaken with caution due to the uncertainty about the level of reporting, some tentative conclusions can be drawn. The pattern follows that of reported incidents very closely. As with the reported incidents the great majority of low level and near misses resulted from human error or criminal intent.

### 4.2 Number of low level and near miss incidents recorded 2015-16 by incident type

| Breach Type | Near miss | Non reportable |
|---|---|---|
| Disclosed in Error | 149 | 378 |
| Lost or stolen paperwork | 48 | 94 |
| Unauthorised Access/Disclosure | 31 | 87 |
| Other | 28 | 88 |
| Lost In Transit | 13 | 28 |
| Non-secure Disposal – paperwork | 15 | 11 |
| Lost or stolen hardware | 10 | 13 |
| Technical security (cyber) | 2 | 3 |
| Uploaded to website in error | 5 | 2 |
| Inability to recover electronic data | 1 | 3 |
| Non-secure Disposal – hardware | 1 | 2 |
| **Totals** | **303** | **709** |

# 5. Additional Considerations

Analysis of the detail of incidents classed as non-reportable has revealed inconsistencies with some organisations scoring similar incidents differently. A consistency check was run with a small number of organisations and it became clear that some scored sample incidents lower than was warranted.

# 6. Conclusions

More organisations are using the reporting tool each year. The increased level of reporting, however may not fully account for the increased number of reported incidents i.e. the actual number of incidents may be increasing.

Most organisations report no or very few incidents each year – this inevitably impacts on local understanding, experience and capability for managing and reporting incidents. Perhaps as a consequence of this, analysis of incidents and the way that local organisations have scored them using the Reporting Tool highlights significant discrepancies. This has particular relevance given the likely move to legally required incident reporting from 2018-19 onwards.

We cannot distinguish between organisations having few breaches due to their business model (e.g. pharmacies have no reason to put data at risk) and those that under report (FOI requests from the privacy lobby indicate that Local Authorities have as many incidents as the NHS but do not report them via the Reporting Tool). Work is required in partnership with NHS England and the Local Government Association to mandate/encourage reporting in a consistent manner across the health and care system.

Human error and criminal activity account for the great majority of incidents and have done so for the past 3 years. These must be tackled by local organisations through training, policies, procedures and effective monitoring of internal performance. The mandatory IG training that all staff must undertake should be updated to focus on the practical steps to reduce human errors and protect premises and information assets.

The new security standards recommended by the National Data Guardian should harden health and care sector defences against cyber-attack but there is no evidence that this will help prevent data protection breaches due to human error or criminal activity. The elements of the IG Toolkit that address training, policies, procedures and local codes of conduct should therefore be strengthened and better focussed on best practice and avoiding human error.

## Annex A - Breach Type - Definitions

| Breach Type | Examples / incidents covered within this definition |
|---|---|
| **Lost in transit** | The loss of data (usually in paper format, but may also include CD's, tapes, DVD's or portable media) whilst in transit from one business area to another location. May include data that is:<br>• Lost by a courier<br>• Lost in the 'general' post (i.e. does not arrive at its intended destination)<br>• Lost whilst on site but in situ between two separate premises / buildings or departments<br>• Lost whilst being hand delivered, whether that be by a member of the data controller's staff or a third party acting on their behalf<br><br>Generally speaking, 'lost in transit' would not include data taken home by a member of staff for the purpose of home working or similar (please see 'lost or stolen hardware' and 'lost or stolen paperwork' for more information). |
| **Lost or stolen hardware** | The loss of data contained on fixed or portable hardware. May include:<br>• Lost or stolen laptops<br>• Hard-drives<br>• Pen-drives<br>• Servers;<br>• Cameras<br>• Mobile phones containing personal data<br>• Desk-tops / other fixed electronic equipment<br>• Imaging equipment containing personal data<br>• Tablets<br>• Any other portable or fixed devices containing personal data<br><br>The loss or theft could take place on or off a data controller's premises. For example the theft of a laptop from an employee's home or car, or a loss of a portable device whilst travelling on public transport. Unencrypted devices are at particular risk. |
| **Lost or stolen paperwork** | The loss of data held in paper format. Would include any paper work lost or stolen which could be classified as personal data. Examples would include:<br>• Medical files<br>• Letters<br>• Rotas<br>• Ward handover sheets<br>• Employee records<br>• Work diaries<br>The loss or theft could take place on or off a data controller's premises, so for example the theft of paperwork from an employee's home or car or a loss whilst they were travelling on public transport would be included in this category. |
| **Disclosed in error** | This category covers information which has been disclosed to the incorrect party or where it has been sent or otherwise provided to an individual or organisation in error such as:<br>• Communication containing patient data sent to wrong person, address or organisation |

| Breach Type | Examples / incidents covered within this definition |
|---|---|
| | • Patient has received another patients notes or patient identifiable data<br>• Email sent to the wrong organisation, address , person or in an insecure manner<br>• Faxes sent to wrong organisation or person<br>This would include situations where the information itself hasn't actually been accessed. Examples include:<br>Letters / correspondence / files sent to the incorrect individual;<br>• Verbal disclosures made in error (however wilful inappropriate disclosures / disclosures made for personal or financial gain will fall within the s55 aspect of reporting)<br>• Failure to redact personal data from documentation supplied to third parties<br>• Inclusion of information relating to other data subjects in error<br>• Emails or faxes sent to the incorrect individual or with the incorrect information attached<br>• Failure to blind carbon copy ('bcc') emails<br>• Mail merge / batching errors on mass mailing campaigns leading to the incorrect individuals receiving personal data<br>• Disclosure of data to a third party contractor / data processor who is not entitled to receive it |
| **Uploaded to website in error** | This category is distinct from 'disclosure in error' as it relates to information added to a website containing personal data which is not suitable for disclosure. It may include:<br>• Failures to carry out appropriate redactions<br>• Uploading the incorrect documentation<br>• The failure to remove hidden cells or pivot tables when uploading a spread-sheet |
| **Non-secure disposal – paperwork** | The failure to dispose of paperwork containing personal data to an appropriate technical and organisational standard. It may include:<br>• Failure to meet the contracting requirements of principle seven when employing a third party processor to remove / destroy / recycle paper<br>• Failure to use confidential waste destruction facilities (including on site shredding)<br>• Data sent to landfill / recycling intact – (this would include refuse mix up's in which personal data is placed in the general waste) |
| **Technical security failing (including hacking)** | This category concentrates on the technical measures a data controller should take to prevent unauthorised processing and loss of data and would include:<br>• Failure to appropriately secure systems from inappropriate / malicious access<br>• Failure to build website / access portals to appropriate technical standards<br>• The storage of data (such as CV3 numbers) alongside other personal identifiers in defiance of industry best practice<br>• Failure to protect internal file sources from accidental / unwarranted access (for example failure to secure shared file spaces)<br>• Failure to implement appropriate controls for remote system access for employees (for example when working from home) |

| **Breach Type** | **Examples / incidents covered within this definition** |
|---|---|
| | In respect of successful hacking attempts, the ICO's interest is in whether there were adequate technical security controls in place to mitigate this risk. |
| **Corruption or inability to recover electronic data** | Avoidable or foreseeable corruption of data or an issue which otherwise prevents access which has quantifiable consequences for the affected data subjects e.g. disruption of care / adverse clinical outcomes, for example:<br>• The corruption of a file which renders the data inaccessible<br>• The inability to recover a file as its method / format of storage is obsolete<br>• The loss of a password, encryption key or the poor management of access controls leading to the data becoming inaccessible |
| **Unauthorised access/disclosure** | The offence under section 55 of the DPA - wilful unauthorised access to, or disclosure of, personal data without the consent of the data controller.<br><br>**Example**<br>An employee with access to details of patients, who have sought treatment following an accident, sells the details to a claims company who then use this information to facilitate lead generation within the personal injury claims market. The employee has no legitimate business need to view the documentation and has committed an offence in both accessing the information and in selling it on. |
| **Other** | This category is designed to capture the small number of occasions where a breach occurs which does not fall into the aforementioned categories. These may include:<br>• Failure to decommission a former premises of the data controller by removing the personal data present;<br>• The sale or recycling of office equipment (such as filing cabinets) later found to contain personal data;<br>• Inadequate controls around physical employee access to data leading to the insecure storage of files (for example a failure to implement a clear desk policy or a lack of secure cabinets).<br>This category also covers all aspects of the remaining data protection principles as follows:<br>• Fair processing<br>• Adequacy, relevance and necessity<br>• Accuracy<br>• Retaining of records<br>• Overseas transfers |

# Annex B - Examples of Incident breach types

## Disclosed In Error

### Trust Letters to a GP Copied to Patient But Sent to Wrong Address

A Trust sent letters to a patient's GP and copies of the same letters to the patient. A typing error in the address (No 2 instead of 22) meant the copies meant for the patient went to a neighbour instead. The neighbour opened the letters and took them to the General Practice shown in the letters which then alerted the Trust. The subsequent investigation found that the letters contained sensitive information regarding the patient (a minor) and included results of genetics tests with references to the mother.

### Maternity Discharge Summaries on Reverse Side of Patient Letters

A member of staff noticed that confidential information was printed on the reverse side of a patient letter. The information was maternity discharge summaries for another patient. A trawl was carried out of 1,000 letters ready for despatch which found that confidential information of 7 patients (5 mothers and 2 babies) had been printed on the back of 59 letters (the same information being repeated on more than one letter). Of the 59 letters, 48 were sent to other patients and 11 to GPs.

### Commissioning Data Sent to Wrong NHS Recipient

An email sent over the nhs.net mail system containing NHS number, local identifier, gender and ethnicity of 110,000 individuals was sent from a Foundation Trust to a CSU in error. The error was immediately noticed and the emails and data deleted.

## Unauthorised Access/Disclosure

### Patient Took Other Patient's Notes from Office

A Community Psychiatric Nurse reported that an in–patient had admitted going into the Staff Office and Nursing Station and taking clinical papers relating to a number of patients and refused to say what had been done with them.

### Estranged Wife Given Husband's Medical Information

A Trust received a phone call from the estranged wife asking for information relating to her husband for Court Proceedings involving child custody. A letter from the Consultant Psychologist was released including details under the following headings: reason for referral, presenting problems, safeguarding information. There was no fair or lawful basis for disclosing the data. The Trust met with the client to advise him of the breach and provided him with redacted information of what had been disclosed. The estranged wife's legal representative agreed not to use the information.

### Extract From GP Systems Without Data Sharing Agreement

A batched patient data extract (containing detailed demographic data and lists of Read Codes) of 210,000 individuals was taken by a clinical systems provider from 70 GP Practices and passed to a CSU approved as an interim "Safe Haven" holding Section 251 approval. Agreements were in place for extracts but not for batched extracts. 55 of the GP Practices had withdrawn consent in 2014 and 15 GP Practices had never consented to batched extracts taking place. The error occurred because the existing data sharing agreements with the GP Practices had not been checked to make sure the new extract had been agreed.

## Lost or Stolen Paperwork

### Clinical Handover Notes in Street

A clinical handover sheet containing details of 29 children (bed number, unit name and unit days, date of birth and age, diagnosis, date of arrival on the unit and source, notes and name of consultants) was found in a city centre street. The sheet was found by a member of staff who informed his manager and completed an incident reporting form.

### Parent Details Stolen From Car

The car of a Community Midwife Support Worker was broken into and work bag stolen from the boot. The bag contained folders relating to 249 patients who have been invited to use the parent-craft services since 2013. The data included parents' names, telephone numbers, name of allocated midwife and expected date of delivery.

## Lost In Transit

### GP Letters Lost Within Trust Internal Mail

A consultant securely packaged up a batch of approximately 50 referral letters (clinical/care case notes and social care notes) from GPs and a Dictaphone (no patient information on the Dictaphone) and sent them in the hospital internal mail across site to his medical secretary. The package never arrived and could not be found despite searches of post rooms as well as the originating department without success.

## Corruption or Inability to Recover Electronic Data

### Change of PC Operating System Led To Loss of Digital Records

After Windows 7 was installed onto all of the Podiatry PC's the patient record system used for patients attending for a podiatry musculoskeletal assessment failed to function correctly. ICT were thought to have resolved the issue and the system was used again but it was subsequently discovered that the records were not being saved and the data was lost.

## Lost or Stolen Hardware

### Unencrypted Laptop Stolen From Parked Vehicle

An unencrypted work laptop was stolen from a parked vehicle during early evening. 130 employees' personal data (mostly dates of birth as well as a small number of National Insurance number, salary details and private addresses) in employee spreadsheets was held on the laptop hard drive was also present.

## Corruption or inability to recover electronic data

### Loss of Digital Cardiology Data Due To Hardware Failure

A hardware failure on the GE Image Archive resulted in the complete loss of 102,554 angiograph images; attempts to recover the data through a specialised data recovery company confirmed that the data was non-recoverable. The GE Image Archive system processes Cardiology diagnostic angiography data (containing both still and moving images).

## Lost or Stolen Hardware

### Loss of Data Cartridge

A data cartridge containing electronic copies of scanned paper, handwritten patient report forms was stored in a fireproof safe at organisational base. The cartridge was needed as part of a routine data retrieval request but was not in the safe. The cartridge contained the electronic copies of scanned paper patient report forms of approximately 42,000 patients. The scanned Patient Report Forms were in TIFF image format containing patient demographics and complaint / treatment given.

## Non-Secure Disposal – Paperwork

### Confidential Waste Placed In Incorrect Disposal Bag

Confidential waste waiting for shredding was mistakenly picked up and placed in general recycling waste. The papers included community daily printed diary including patient identifiable information, health status, allergy alerts, core drugs, journal entries and a copies of GP summaries.

## Technical Security Failing (Including Hacking)

### Patient Data Accessible On Shared Intranet Folder

A number of unprotected files / folders including patient identifiable data and staff identifiable data were stored in a 'Common Room' folder on a Trust's intranet site. The patient data consisted of dates of birth, address details, medication details, PiMS numbers / hospitals numbers, test results and correspondence as well as staff data including payroll, expenses claims, full name details and address details.

## Non-Secure Disposal – Hardware

### Hardware Containing Patient Data Sent To Auction

An ophthalmology medical device from a Trust's eye clinic was sent for sale at auction. The auctioneers inspected the device and found 2,850 patient records including names, DOB and ophthalmology readings. They informed the Trust's data protection officer.

## Uploaded to website in error

### Sensitive Patient Data Accessible Via Google

An IVF patient contacted the hospital and said that information about IVF patients was publicly available through google.co.uk. The hospital investigation found that a breach had taken place at the transcription company. The Trust made demands made to the transcription company to take immediate steps to reduce the risk of the data remaining accessible on the internet and an urgent request was made to Google to remove the data.