

# Information Governance Incidents closed during 1st April to 22nd. May 2018

Published August 2018

**Information and technology**  
**for better health and care**

# Contents

---

<b>Contents</b>	<b>2</b>
<b>Introduction</b>	<b>3</b>
<b>Content of the report</b>	<b>3</b>
<b>Closed level 2 incidents reported during 1<sup>st</sup> April to 22nd. May 2018</b>	<b>4</b>
<b>Appendix A – Incidents closed using the ‘auto closure’ facility 1st. April to 22nd. May 2018.</b>	<b>9</b>

---

## Introduction

This is the published report of closed level 2<sup>1</sup> Information Governance Serious Incidents Requiring Investigation (IG SIRIs) recorded on the IG Toolkit Incident Reporting Tool. This type of report will be published on a quarterly basis as specified in the IG SIRI Publication Statement<sup>2</sup>. It covers IG SIRI level 2 incidents closed during the period of 1<sup>st</sup>.April to 22<sup>nd</sup>. May 2018, following investigation by the local organisation(s) concerned.

Note that the reporting period covered is 7 weeks as the new Data Security and Protection Toolkit (DSPT) replaced the IG Toolkit's Incident reporting tool on the 22<sup>nd</sup> May 2018.

## Content of the report

The report below consists of **15 closed incidents** reported to the Information Commissioner's Office (ICO), Department of Health (DH) and NHS England (NHSE) by Health or Adult Social Care organisations or suppliers (as advised within the [IG SIRI Guidance](#) issued 29<sup>th</sup>. May 2015).

The report contains the organisation name, date the incident was closed, scale (e.g. the number of data subjects affected presented as a range), a description of the incident and data involved. All information displayed below is as reported by the organisation(s) concerned. Where necessary, personal information included within the incidents has been redacted.

An auto closure feature introduced in June 2015 closes all open incidents that have not been updated by the organisation for 90 days<sup>3</sup>. In Appendix A is **1 incident** that has been auto-closed by the system.

### Please note:

- A 'Closed' incident means that the incident has been investigated by the local organisation and no further action is required unless the ICO make a request.
- Closed incidents may still be under review by the ICO and any actions taken will be published on the [ICO website](#).
- This report does not include level 2 incidents which are still marked as open and therefore are still under investigation by the local organisation.
- Any near misses, Level 0 and 1 incidents voluntarily reported by organisations are also excluded as these incidents are not currently being monitored by the Health and Social Care Information Centre (HSCIC) but are useful for gathering intelligence, analysing trends and learning from previous occurrences. Details of such incidents are held by the local organisations.

## Next reports

Future incident reporting data will be via the new DSPT at [www.dsptoolkit.nhs.uk](http://www.dsptoolkit.nhs.uk)

---

<sup>1</sup> Level 2 IG SIRIs are sufficiently high-profile cases or deemed a breach of the Data Protection Act or Common Law Duty of Confidentiality, and hence reportable to the Department of Health and Information Commissioner's Office. Organisations have used the IG SIRI assessment of severity facility to determine this level and report the incident. Further information on this can be found in the 'Checklist Guidance for Reporting, Managing and Investigating IG SIRIs'.

<sup>2</sup> <https://www.igt.hscic.gov.uk/resources/IGIncidentsPublicationStatement.pdf>.

<sup>3</sup> The organisation is notified by email 10 days in advance giving them time to update or close the incident before the auto closure occurs. If the organisation updates the record, it will not be auto closed. The organisation will also receive an email notification within 24 hours after auto closure, and if necessary can reopen the incident.

## Closed level 2 incidents reported during 1<sup>st</sup> April to 22nd. May 2018

ID	Organisation Name	Date of Closure	Details of Incident	Data
IGI/19429	NHS Bedfordshire CCG	09-May-18	Email containing the first names of a patient and his parents plus details of the patient's condition was sent to various partners involved in managing the patient. Included in the email trail was an incorrect recipient who is based at NHS Grampian.	Email
IGI/19307	The Health Centre (M81003)	14-May-18	Practice sends monthly batch of prescriptions to PPA for reimbursement. Discovered on <b>redacted</b> that Royal Mail have only delivered an empty torn envelope to the PPA and returned to the practice the claim form - also torn - prescriptions are missing / destroyed - to be confirmed by royal mail. Practice has complained and flagged up the incident to Royal Mail. Response from Royal Mail - all loose post if cannot be returned is securely destroyed at depot after one month.	Prescriptions for Injections carried out in surgery which are sent by practices for reimbursement via the Prescription Pricing Authority
IGI/19308	JHOOTS PHARMACY GROUP (P3DX)	02-May-18	Parcel contained Names and Addresses and possible medication of approximately 30 patients in report. The parcel was dispatched with the wrong courier collecting a parcel. The Incident was identified when the correct courier called to collect. there has been no success in tracing the parcel.	Data contained Patient Name, Address and Drug Name, Quantity and costing an expensive item report - mainly only one drug per patient
IGI/19336	BRADFORD DISTRICT CARE TRUST	10-May-18	Pay slips lost in transit between New Mill & Millennium Business Park. Contained names, NI numbers, annual salary, tax code. 25 payslips in total.	Paper payslips inc. NI number and employee name and number
IGI/18245	THE NEWCASTLE UPON TYNE HOSPITALS NHS	10-May-18	A member of staff was preparing data which is sent daily to the local Clinical Commission Group as well	Patient data

ID	Organisation Name	Date of Closure	Details of Incident	Data
	FOUNDATION TRUST		as to staff inside of the Trust. They intended to attach a file which had de-identified patient data; in error, they attached a file which contained Name, NHS number, age, ethnicity, reason for attendance.	
IGI/18065	HERTFORDSHIRE PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST	18-May-18	<p>Service user called to report a breach. They believe that their letters from the SW Support &amp; Treatment team have been going to the incorrect address for the past 2 years. Since their engagement with the service, they have received 1/2 of the letters that they believe they should have received. They have recently received a discharge letter following non-response from any correspondence sent from the team. At a meeting with their psychiatrist today, a letter was seen by the service user on the table that was addressed to number 2. They live at number 22.</p> <p>Over the last 2 years the service user has been the victim of identity theft which they mentioned could be linked to this breach.</p>	<p>Demographic details - name, address, NHS number, DOB Child abuse details, sexual information, employment information, medical history, diagnosis, current mental state, current medication, appointment details.</p> <p>It is suspected that letters and reports would have been sent but possibly to the wrong address.</p>
IGI/18040	WALSALL HEALTHCARE NHS TRUST	17-May-18	A letter containing clinical information was sent to the wrong address (although the name of the recipient was correct) and subsequently opened. The letter was regarding the outcome of a child's consultation. The address on the letter was correct but the envelope was typed, and the house digit was entered incorrectly. The name on the envelope was however correct. The letter was received by a neighbour.	Clinical information following on from a child's consultation. Includes child's name, address, hospital unit number, date of birth, GP details and clinical information.
IGI/17984	Langham Place Surgery (K83027)	10-Apr-18	Potential inappropriate access to electronic records. Incident came to light following spot check audit of records on <b>redacted</b> based on suspicion of	NHS Patient data

ID	Organisation Name	Date of Closure	Details of Incident	Data
			inappropriate activity.	
IGI/17929	Rennie Grove Hospice Care	20-Apr-18	<p>Following changes to servers, personalised printer settings were replaced with default settings for users of the Clinical Portal. A clinician inadvertently printed to a printer outside the clinical Safe Haven area but still within the organisation. The resulting document contained names and diagnosis information. The event was reported immediately, and an Internal Incident Report raised. The resulting scoring suggests external reporting is required. The document remained within the organisation and all staff who may have seen it were already required to sign a Code of Conduct, covered by a requirement to treat confidential information appropriately within their contract and appropriately trained. A clinician failed to notice that the personalised printer settings had been changed to default and sent a document to print elsewhere within the organisation. The Director of Fundraising discovered the document and alerted the ICT lead. The document included names of 13 patients and their diagnosis. In separate incidents other less sensitive documents had also been generated in a Non-Safe Haven area. An internal Incident Report was raised and is going through the internal governance process. Following the IG Incident Scoring a rating of 2 resulted so hence external report raised.</p>	6-page document printed. List included GP, Patient Name, Diagnosis, Status of DNACPR and comments relating to 13 patients
IGI/17992	NORTH WEST AMBULANCE SERVICE NHS TRUST	25-Apr-18	Patient Report forms have been lost and the crew do not know where they lost them, if they were in the hospital or from the stretcher when putting it back in the vehicle.	Patient Report Form

ID	Organisation Name	Date of Closure	Details of Incident	Data
IGI/17812	NORTH WEST AMBULANCE SERVICE NHS TRUST	25-Apr-18	The paper payslip had not yet been received by the staff member to whom it belonged. It was taken by a person unknown, photographed and the photographs left in the tool boxes of two other members of staff. The payslip was left in a pigeon hole with others for collection by the supervisor for distribution.	Staff wage slip
IGI/17787	ELYSIUM HEALTHCARE	25-Apr-18	A patient who was discharged from Arbury Court on to another service. The patient informed staff at the new service that they had found a file in their belongings. This was handed to staff, who then called Arbury court to report the incident. The file was locked in a secure location until a staff member from Arbury court went to collect it.	name, date of birth, NHS number, medication details, ward round notes, CPA notes. section papers, referral papers and reason for referral, historical papers, physical observations, funding information, Current patients and discharged patients.
IGI/17762	NHS ARDEN AND GREATER EAST MIDLANDS COMMISSIONING SUPPORT UNIT	16-Apr-18	The spreadsheet that was sent from AGEM which was password protected, and sent to the right person, contained the details of 874 members of staff. We have assurances from the recipient that copies of it have been deleted and the paper copy printed (which alerted them to the incident) have been destroyed securely, and the incident has been securely contained. We are in the process of reviewing this incident, and an RCA is underway to document and identify what happened within AGEMCSU processes, and where learning can take place. The incident itself has been graded as a (Datix) level 3, and AGEMCSU Senior Management team including the SIRO have been informed.	Personal details downloaded from ESR.
IGI/16710	NHS NORTH OF ENGLAND	01-May-18	"On 31 January the Senior Governance Manager (Information Governance) received a call from our	Amongst the items which cover the whole range of Medicines Optimisation service

ID	Organisation Name	Date of Closure	Details of Incident	Data
	COMMISSIONING SUPPORT UNIT		<p>Medicines Optimisation team in the Yorkshire &amp; Humber area asking for advice regarding an electronic folder containing c.75,000 items which they had access to whilst being employed by Yorkshire and Humber CSU and continued to have access to when that service was transferred to NECS. Amongst the items which cover the whole range of Medicines Optimisation service delivery and management activities are staff personnel files and patient details. Although the folder has controlled access to the 36 members of the Medicines Optimisation (MO) team, those team members have access to the whole folder rather than restricted access to the relevant sub folders/files to which they do require appropriate access for their roles.</p>	<p>delivery and management activities are staff personnel files and patient details.</p> <p>Encryption applies to all personnel who use a NECS laptop. However, encryption does not apply if using a desktop computer. Limited access to 36 personnel</p>
IGI/16540	NHS England	05-Apr-18	<p>A telephone call was received by the complaints officer from a complainant advising that the complaints officer had sent his final complaint response to an incorrect address. The complaints officer reviewed and discovered that this was the complainants address which was logged on the database but was a previous one. He notified us of his new address on the consent form he received (via the old address) however, the complaints officer did not update the database and therefore once the complaint progressed and was finalised the complaint response was sent to the previous address. The complainant emailed to state that he was not happy that his "private information was sent to another address breaching my confidentiality"</p>	<p>complaints correspondence which included health and treatment details of the data subject</p>

## Appendix A – Incidents closed using the ‘auto closure’ facility 1st. April to 22nd. May 2018.

ID	Organisation Name	Date of Closure	Details of Incident	Data
IGI/17777	YEOVIL DISTRICT HOSPITAL NHS FOUNDATION TRUST	18-May-18	Patient contacted their GP Practice to report receiving post from YDH which contained letters for 3 additional patients	"Outcome clinic letters containing: PID name, address, dob, NHS number Sensitive and clinical information, reason for attendance and outcome of attendance"