**Discussion Forum 3 – Initial Post**

* What is the specific aspect of GDPR that your case study addresses?
* How was it resolved?
* If this was your organisation what steps would you take as an Information Security Manager to mitigate the issue?

**H. Disclosure of sensitive personal data by a hospital to a third party**

Whilst the General Data Protection Regulation (GDPR) had been adopted by the European Union in 2016, this directive only became enforceable from 25th May 2018 (European Data Protection Supervisor, N.D.). GDPR was not enforceable at the time of this case study in 2017, however the principles of GDPR can still be used to demonstrate the privacy risks involved.

The incident in question involved a hospital disclosing personal health data to a third party and contravenes the GDPR in several ways (Data Protection Commission, 2020). The disclosure occurred due to an incorrect address being used to send documents to the data subject. This breaches Article 5 which states that personal data should be kept accurate and up to date (EUR-Lex, 2016). In a further breach of Article 5, the business did not employ appropriate security measures to protect the personal data in transit, such as using mail tracking. Furthermore, sensitive data categories, such as health data, require an additional lawful basis for processing under Article 9 and this was not met.

The resolution of this case was that the Information Commissioner’s Office made a formal decision that the hospital had breached the Data Protection Acts enforced at the time of the incident.

Recommended steps to mitigate these issues in future include implementing clear, documented procedures for managing all personal data processing, including processes for securely sharing personal data with data subjects. In addition, the human error involved in this case suggests that the staff have a lack of awareness of data protection principles. Therefore, GDPR training should be a prerequisite for all staff involved in data processing operations as this is a mandated responsibility of the Data Protection Officer under the GDPR.

References

Data Protection Commission (2020) Pre-GDPR Case Studies. Available from: <https://www.dataprotection.ie/en/pre-gdpr/case-studies#201705> [Accessed 23 June 2021].

EUR-Lex (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434> [Accessed 23 June 2021].

European Data Protection Supervisor (N.D.) The History of the General Data Protection Regulation. Available from: <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> [Accessed 23 June 2021].

“We received a complaint concerning the alleged unauthorised disclosure of a patient’s sensitive personal data by a hospital to a third party. The complainant had attended the hospital for medical procedures and informed us that the medical reports for these procedures were received to their home address in an envelope that had no postage stamp. The envelope had a hand-written address on it which included the name of a General Practitioner (GP) and also included the home address of the complainant’s neighbour. A hand-written amendment had been made to the address, stating that it was the wrong address. The complainant informed us that they had made enquiries with their neighbour in relation to the correspondence and the neighbour had stated that they had received the correspondence a number of days prior but that it had not been delivered by a postman. The neighbour further advised the complainant that they opened the envelope and viewed the contents in an effort to locate the correct recipient/address.

Following the initial complaint, the complainant provided us with correspondence which they subsequently received from the hospital apologising that correspondence containing the complainant’s medical results had been inadvertently sent to the wrong address. The hospital indicated that this appeared to have been due to a clerical error confusing part of the GP’s address and part of the complainant’s address. We commenced an investigation to establish how the error had happened, what procedures the hospital had in place at the time and what the hospital since had done to avoid repetition of this incident.

The hospital informed us that their normal procedure is to issue medical reports in batches to the relevant GP so that multiple sets of medical reports for different patients are placed in a windowed envelope, which shows the relevant GP’s address in the window. In this case however, the medical report was put in a nonwindowed envelope and the address was hand-written on the front. In doing so, the staff member who had addressed the envelope manually, erroneously intermixed the GP’s name, part of the GP’s address and part of the complainant’s address on the envelope. The hospital also informed us that the envelopes containing results to be dispatched to GPs are franked by the hospital post room. However, in this case because the envelope containing the complainant’s medical information was not franked, the hospital concluded that it was unlikely that it had been sent out directly from their post room and indicated that it could have been sent on via the relevant GP, although they acknowledged that they could not be certain about this this. We were unable to establish during the course of the investigation the precise manner in which the envelope containing the complainant’s medical reports came to be delivered to the complainant’s neighbour’s house. The hospital informed us that administrative staff had since been briefed on the correct procedure for issuing medical reports and that non-window envelopes would no longer be used for this purpose.

The complainant rejected the apology from the hospital made by way of an offer of amicable resolution and instead requested a formal decision from the Commissioner. In her decision, the Commissioner found that the hospital had contravened Section 2(1)(b) (requirement to keep personal data accurate, complete and up to date), Section 2(1)(d) (requirement to take appropriate security measures) and Section 2B(1) (requirement for a legal basis for processing sensitive personal data) of the Data Protection Acts 1988 and 2003 when it processed the complainant’s sensitive personal data by way of disclosing their personal data inadvertently to a third party.

This case illustrates how a seemingly innocuous deviation by a single staff member from a standard procedure for issuing correspondence can have significant consequences for the data subject concerned. In this case, highly personal medical information was accessed by a third party in circumstances which were entirely avoidable. If the hospital had had in place appropriate quality control and oversight mechanisms to ensure that all staff members rigidly adhere to its standard procedures it unlikely that this unauthorised disclosure of sensitive personal data would have occurred.”

G. Use of CCTV footage in a disciplinary process

L. Personal data of a third party withheld from an access request made by the parent of a minor