GDPR Case Studies

Unit 5

2017: Disclosure of sensitive personal data by a hospital to a third party.

- What is the specific aspect of GDPR that your case study addresses?

  Patient's sensitive personal data leakage by a lack of confidentiality principle and accountability principle – unauthorized disclosure of sensitive personal data

  " 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. "

- How was it resolved?
  1) 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
  2) Investigation to establish:
     - how the error had happened
     - what procedures the hospital had in place at the time
     - what the hospital since had done to avoid repetition of this incidents

  3) Complainant requested a formal decision from the Commissioner

- If this was your organisation what steps would you take as an Information Security Manager to mitigate the issue?
    - Appropriate quality control and oversight mechanisms
    - Training of the staff
    - Strict policies and procedures for the staff (already in place)
    - Monitoring by random check-ups (internal audit)
    - Make sure there is no non-window envelopes in the administrative department