Unit 8 Collaborative Discussion 3

Peer Responses

Contents

Response to Shan Swanlow

Hi Shan,

I like the last point you express about involving stakeholders to discuss and anticipate how to meet GDPR requirements and then communicate their approach to visitors on-site or through visual signage. However, in the case of the offending employee, suppose they saw the signage and understood that CCTV footage was recorded and could be used. Would you consider that signage carries the same weight as "consent"? Since the toll company could likely then have won their "legitimate interest" case, leaving the employee worse off, especially given that the event was resolved over two months when the footage was passed to the employer.

Response to Man Sze Wong

Hi Man Sze Wong,

I agree with the steps outlined to stay compliant, "ask for the details or further confirm the purpose". Since the complainant requested four hours' worth of video evidence, is it reasonable for an educational organisation to store so much video footage for each day they operate? Do you think that data storage costs may have played a role in why they could only provide eleven seconds' worth of video footage?

Response to Andrey Smirnov

Hi Andrey,

I enjoyed reading about your chosen case study, which is fascinating. It presents two aspects: one, genuine data entry mistake and two, the organisation owning up to the error, yet the individual affected refuse their acknowledgement (which would ultimately incur penalty against the hospital).

As an information security manager, concerning GDPR, what processes would you implement checks or validations to ensure that postcode details are always entered correctly and linked with hospital patients? This issue seems to be the source of the case study's faux pax, so the affected individual's response does not match the perils of human data entry.

Reply to Michael Justus from Andrey Smirnov

Re: Peer Response

Hi Michael,

Thank you for the question. Because the case study involves unintentional disclosure of a paper medical record, I would probably propose to implement a sort of managerial approval for the release of these kinds of documents. That said, my actual recommendation would largely depend on whether this was an individual occurrence or something indicative of a systemic problem. As we discussed in the Object-oriented Information Systems module, it is impossible to completely eliminate errors that stem from human involvement (Justus, 2021). Interestingly, recent research (Keshta & Odeh, 2021) shows that even today, the majority of physicians prefer dealing with paper records over electronic records, and believe the former

to be more secure. This is not completely unfounded: for example, Kruse et al. (2017) state in their analysis that most health record breaches occur through electronic media.

It is interesting to note that, according to one report (Roberts, 2017), teaching hospitals affiliated with medical schools are especially likely to experience data breaches. This can be attributed to the fact that, due to the requirements of medical research and training, on average more people in these hospitals have access to sensitive patient data compared to "nonteaching" hospitals. While the safeguards at the information security manager's disposal would likely remain the same, it is still important to understand the organizational specifics that can increase the chance of data breaches occurring.

As an additional note, personal experience suggests that organizations sometimes request more information than they strictly require. It might be that some information (e.g., national insurance or social security number) is being requested for no other reason than it being programmed in an information system that happens to be difficult to change or replace (this again ties back to our learnings in the OOIS module). An information security manager should then carefully assess any "legacy" components that deal with the processing of personal data, and ascertain if there are any relics from the past that might inadvertently expose the organization to risks.

References

Justus, M. (2021) Collaborative Discussion 1: Information System Failure: Summary Post. Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=257771 [Accessed 29 January 2022].

Keshta, I. & Odeh, A. (2021) Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal 22(2): 177-183.

Kruse, C., Smith, B., Vanderlinden, H. & Nealand, A. (2017) Security Techniques for the Electronic Health Records. Journal of Medical Systems 41(8): 127.

Roberts, C. (2017) Protect Yourself From a Hospital Data Breach. Available from: https://www.consumerreports.org/health-privacy/the-hospitals-most-at-risk-for-a-data-breach-a1203170826/ [Accessed on 29 January 2022].

Reply to Andrey Smirnov **from** Michael Justus

Re: Peer Response

Hi Andrey,

Thank you for the informative response; I enjoyed reading it. It was enlightening to read the reference to Keshta & Odeh (2021) that medical staff have greater confidence in paper versus technology records. And then, the follow on research by Kruse et al. (2017) made an excellent one-inch punch for confirming trust in physical records due to a greater chance of electronic breaches via electronic media. I thought the two pieces were well researched and you made an excellent argument with them. Also, the point that non-teaching hospitals have greater access to sensitive data than non-teaching hospitals highlights the difficulties of GDPR in such environments.

Your recommendation for a managerial document approval process based on whether the occurrence was once-off or systemic is quite intriguing. An approach that I think can work to resolve such GDPR-related data issues as outlined in the case study. It is fascinating because I wonder if such process flows are part of hospitals due to GDPR and, if so, what impact this has on their operating state. I believe this recommendation will certainly help to entrench a basic level of GDPR-oriented oversight, especially when posting trusted paper records to patients. Your last point about systems requiring too much information I consider you are spot on: systems require data they do not necessarily need but obtain, just in case. But GDPR definitely could prove to be problematic for such legacy components!