The GDPR is an essential legal framework needed to protect the personal data of all EU/EEA individuals (Calder, 2020). Health data – all data pertaining to health (Bincoletto, 2021) – is one such area of personal data that is of a particularly sensitive nature, and taking the proper precautions necessary to ensure its protection and proper handling are vital.

The hospital I work at does a lot right when it comes to master data management and personal data protection, such as: pseudonymization and anonymization of data used for research; using an eHealth cloud-based system with a high degree of interoperability, restricted user access, and a focus on up to date and accurate data; and implementing the GDPR framework into their own IT code of conduct. However, things can and do still go wrong.

In the incident in my initial post, there were several failures to meet the standards for personal data protection set in the GDPR. The failures were largely due to human error, which I suggested could be remedied by an increase in education for hospital personnel. My peers suggested the error could be remedied by regular risk assessments for data handling procedures (HITRUST, 2019) and by better master data management practices when it comes to user authorization (Nielsen, 2018). While the use of a cloud-based system within the hospital allows for ease of access to patient data for any authorized individual, the transfer of authorization from one department to another can go wrong, and this error is what caused the death of a patient.

When it comes to the management and protection of personal data, I as a healthcare and computing professional have a responsibility to ensure I am familiar with the legal, ethical, and social ramifications of data breaches and data mishandling. While some companies simply suffer from fines due to data breaches (Datatilsynet, 2020), some mistakes result in irreversible consequences. It is necessary to combine employee education, best practices within master data management, and compliance with the data protection regulations such as the GDPR to protect personal data.

References:

Bincoletto, G. (2021) *Data Protection by Design in the E-Health Care Sector*. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG. Available from: https://directory.doabooks.org/handle/20.500.12854/74528 [Accessed 22 June 2023]

Calder, A. (2020) *EU GDPR – An international guide to compliance*. Ely: IT Governance Publishing. Available from: https://learning.oreilly.com/library/view/eu-gdpr/9781787782549/ [Accessed 23 June 2023]

Datatilsynet. (2020) Administrative fine to Østfold HF Hospital. Available from: https://www.datatilsynet.no/en/news/2020/administrative-fine-to-ostfold-hf-hospital/ [Accessed 20 June 2023]

HITRUST. (2019). Risk Analysis Guide for HITRUST Organizations & Assessors. Unknown: HITRUST Alliance. Available from: https://hitrustalliance.net/content/uploads/RiskAnalysisGuide.pdf [Accessed 25 June 2023]

Nielson, M. (2018) How Master Data Management Supports Data Security. Available from: https://www.stibosystems.com/blog/how-master-data-management-supports-data-security [Accessed 25 June 2023]