The General Data Protection Regulation (GDPR) is a legal framework created by the European Union that sets requirements for the protection of personal data that must be met by member states of the European Union (Calder, 2020). As defined by the GDPR, personal data is "…any information relating to an identified or identifiable natural person…" (Regulation (EU) 2016/679, 2016). The protection of personal data is important as it concerns the fundamental human right to privacy. As I work in a public hospital, the focus of this post will be the protection of health data. While the GDPR is concerned about the protection of all personal data, health data has additional restrictions to its access and processing. Health data also has a very broad definition, with many organizations arguing over what it encompasses. According to the GDPR, health data includes biometric data, genetic data, and data concerning health (Bincoletto, 2021).

The hospital I work at implements GDPR regulations and has a strong emphasis on the protection of personal health data. Personal data used within the hospital by healthcare workers is kept on a cloud-based eHealth system with restricted access. Although the system is provided by a third party, the hospital itself is the data controller, or the one that determines the purposes and means of the processing of personal data (Calder, 2020). As this system is adopted by most healthcare workers in Norway, healthcare professionals can update patient data in real time and share accurate information on the patient's current well-being quickly and securely. Data used for scientific research is kept on two different secure servers, with researchers having access to one server that has both pseudonymized data – data that is connected to a construed ID that can link a pseudonym with a specific data subject with a key – or anonymized data – data that is irreversibly altered so the data subject is no longer identifiable (Data Protection Commission, 2019). The key document is kept on the other secure server, which the researchers do not have access to. Patient data is also not shared via email, but only via the eHealth system in place.

While these practices help prevent data breaches or malicious use of personal health data, unfortunately errors do happen. One such incident involved an elderly dementia patient that was to be discharged shortly after being moved from one department (referred to henceforth as 'X') to another department (referred to henceforth as 'Y'). This patient was moved from X to Y the morning they were to be discharged. All their discharge papers and information were in order, and the taxi to take them home was arriving in only a few hours. Y received all the health data about the patient but did not get the data concerning communication with next of kin. X had sent that data to the wrong recipients. Y wrongly assumed that X had already informed the next of kin about the patient's discharge and sent the elderly patient home – supposedly to the patient's relatives – in the taxi. The patient froze to death in the Norwegian winter, right outside their home. They suffered from dementia and did not know how to get into their house, and they might not have even known the house was theirs. Improper data handling has steep consequences within the healthcare industry. From breaches leading to leaked national identification numbers (Datatilsynet, 2020), to massive financial losses and identity theft (O'Connor, 2023), to even death.

In this incident, there are two main issues. The first is that X sent the data to the wrong place. This could have been solved by the healthcare worker in X taking a bit more time and care with the handling of the patient's personal data. The second issue is that the worker in Y did not notify anyone about the lack of data concerning the patient's next of kin. The pressure to get the patient out of the department quickly to ensure more empty beds, plus the large number of tasks a healthcare worker must juggle, might have contributed to this human error. However, both these issues could be solved with education and training about the importance of proper data handling and the consequences of not doing so. While healthcare workers understand how important handling data is, more frequent refreshers on the topic are needed in the hospital I work at.

As a healthcare worker, I am accustomed to the responsibility of managing patient data and keeping myself updated on the laws and regulations surrounding health data. However, as a budding computing professional I am learning more about the responsibilities data professionals have and the laws that must be upheld when it comes to processing, accessing, and sharing personal data in all fields. Personal data is extremely important, and as my story shows, it can be a matter of life and death.

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]

Data Protection Commision. (2019) *Guidance on Anonymisation and Pseudonymisation*. Available from: https://www.my-course.co.uk/pluginfile.php/941084/mod_page/content/17/Harvard%20Referencing%20Guide.pdf [Accessed 20 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]

GDPR Regulation at: Regulation (EU) 2016/679. European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504 [Accessed 20 June 2023]

O’Connor, B. (2023) Health Care Data Breach: What to Know About Them and What to Do After One. Available at: https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ [Accessed 21 June 2023]