Task 3 - Francis Denton

Personal data refers to any kind of data which can be used to potentially find out the identity of a person, this can be either personal attributes such as name, address and medical data or technical data such as an I.P address. Whilst something like a name alone might not be enough to identify someone, when used in combination with other kinds of personal data it becomes easier to identify an individual[3]. There are many concerns around the collection and use of personal data, from private or public companies using such data for marketing means without consent or other individuals using personal data such as biometric data or location/GPS data for malicious purposes such as cyber and real life stalking or identity fraud. Data protection refers to the fair and proper use of information about people, it's about building trust between the people and organisations[1]. Organisations have a duty to protect personal data and to prevent leaking and breaches of such data, and are required to follow a set of guidelines. Some ways in which personal data can be protected is through the use of encryptions or anti-hacking tools as well as the deletion or destruction of personal data once there is no longer a use for it.

The GDPR outlines a set of guidelines that are required to be followed by those who possess personal data. Under the GDPR personal data is required to be processed lawfully, fairly and in a transparent manner in relation to individuals[2]. The majority of the data provided to us would class as personal or sensitive data, and thus I would be under obligation to follow the GDPR to its fullest extent. When a patient is assessed, it is required that we disclose to them what data we are collecting and what it is to be used for. It also must be processed in a way that helps keep the data secure and protected against unauthorised access to the data. As I am working with sensitive health data and potentially vulnerable patients, there should be a split between medical and personal data which makes it harder to link the two together, using an ID system instead of a name system for a table about medical data should be used as it makes it harder for an unauthorised user to link a patient and their sensitive information. The organisation would be required to carry out a Data Protection Impact Assessment and data breach response[6], in order to evaluate the potential risks to individuals should their medical data be breached, and to set up a plan of action and notify individuals when such a thing has occurred.

The NHS is required to employ a data protection officer who's role it is to give advice, monitor compliance and act as a point of contact in matters regarding how the organisation functions using personal data. Where the NHS stores personal data, it is mostly held as codes instead of words in order to make such data more secure[5]. When working with other organisations, the NHS requires those organisations to go through a process referred to as the 'Data Access Request Service' that makes sure that organisation will store the data safety and legally and provide justifications of the health benefits that arise from the use of the data. The NHS promises that information is never shared to either marketing or insurance companies without consent from an individual[4]. In our case, as a critical care unit, it is likely that are patients are highly vulnerable, making them a potential target for medical insurance companies. We should set out to replicate the processes carried out by the NHS in regards to the GDPR as we are using also using medical data of a highly sensitive degree.

References

[1] Anon (2018) *Some basic concepts*. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/[Accessed 16 April 2021].

[2] ICO (2017) Essential guide to the General Data Protection Regulation (GDPR). *The Pharmaceutical Journal*. doi:10.1211/pj.2017.20203048[Accessed 15 April 2021].

[3] Anon (2018) *What is personal data and why is it so important?* Available from: https://www.redscan.com/news/personal-data-important-keep-safe/ [Accessed 20 April 2021].

[4] (NHS Digital, 2021) *Transparency notice: how we use your personal data - NHS Digital*. Available from: https://digital.nhs.uk/about-nhs-digital/our-work/keeping-patient-data-safe/gdpr/gdpr-register[Accessed 20 April 2021].

[5]Anon (2018) GDPR: What Is It and How Might It Affect You? *YouTube* [online]. Available from: https://www.youtube.com/watch?v=j6wwBqfSk-o[Accessed 20 April 2021].

[6]Anon (2017) *What are the most important elements of the GDPR? | Experian*. Available from: https://www.experian.co.uk/blogs/latest-thinking/data-quality/what-are-the-most-important-elements-of-the-gdpr/ [Accessed 19 April 2021].

[7]Anon (no date) *NHS England and NHS Improvement Data Protection Policy* [online]. Available from: https://www.england.nhs.uk/wp-content/uploads/2019/10/data-protection-policy-v5.1.pdf[Accessed 15 April 2021].

[8]Anon (2019) *What is personal data?* Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/ [Accessed 19 April 2021].