GDPR & Patient Data: Aiming at Privacy by Design

GDPR (General Data Protection Regulation) in force in the European Europe since May 2018, regulates how personal/patient data is handled in Europe. The GDPR defines the obligations that data controllers and data processors must comply to.

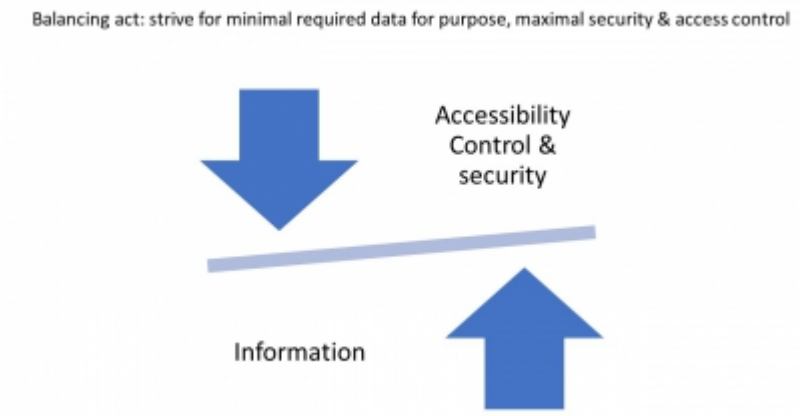
Health data under the GDPR is considered sensitive data, as such, data processing is prohibited unless there is individual's explicit consent, which clearly must define how the data must be processed, by whom and for what. On top of explicit consent, there are yet five additional lawful bases for processing data: Contract, Legal obligation, Vital Interests, Public Task and Legitimate Interest (Art. 9 GDPR). In practice some of these lawful bases are observed in the direct therapeutic relationship.

Yet, because what is lawful might not be necessarily ethical, and by the end of the day the data controller/processor are accountable for any data breach or ethical issues, the role of the Ethical Committee within a health care organization, is often essential to define ethical safeguards and ensure the ethical management of patient data, which will impact security as well.

Essentially, the GDPR aims to safeguard the management of personal data in a lawful, fair and transparent manner, limit the purpose of data, increase integrity and confidentiality and make data controllers/processors accountable for the ethical and lawful utilisation of data.

When it comes to ensure personal privacy, fulfilling legal and ethical obligations can be complex, but is it now understood that along with sound technical and organisational infrastructures and procedures, de-identification methods, (as explorer along this article) can be an important part of meeting these legal and ethical obligations. (M. Hintze, 2016). Health care companies specifically have developed technical and organizational measures intended to protect personal health data by design in their products.

WSI: New Health Data Whole Slide Imaging (WSI) is a relatively new category of patient data. As such, recently, some efforts have been made to better understand how WSIs (whole slide images) can be utilized in a balancing act: maximizing individual and public benefit, while at the same time, restricting and protecting its access, whenever such poses a potential privacy risk and non-compliance with data privacy laws (e.g. GDPR). Although by itself the patient's photographic tissue image falls under the category of de facto anonymity (add note) of the GDPR, the existence of patient-ids and/or other tags attached to the WSI, increase the likelihood of patient identification, and potential privacy issues. (Holub et al., 2022).



The novelty of this type of personal data is revealed when histopathologists describe their knowledge and confidence when dealing with WSIs as personal data. In a survey (n=198) conducted by the

Oxford University Hospitals, addressed to histopathologists members of major pathology associations in the UK, 41% of the respondents did not know when WSIs would fall under relevant legal frameworks, while 47% were not confident “At all” when it came to understand the WSI consent in a research context (Coulter et al.; 2022).

Digital imaging Storage and management standards are widely adopted in the field of Radiology, which facilitates the adoption of sound data compliance practices. When it comes to digital pathology and data management standards adoption differences, alongside with workflow specificities and the novelty of the field, another major difference lies in the role of the pathology professional societies. The ARS took the lead and through the DICOM initiative managed to impose standards and provide clear guidelines for Radiologists and industry. The Pathology societies have not played such an active role yet, and previous efforts to make WSI part of DICOM have not been successful due to the complexity of WSI and differences in pathology clinical workflows. Despite the absence of reference literature from professional pathology societies, general guidelines and use cases published in the recent years focusing on how to lawfully and ethically process WSIs as patient data, point to pseudonymization as a relevant strategy to ensure data compliance, and perhaps most importantly, as a strategy to avoid data breaches and its negative consequences for both patients and organizations. In fact pseudonymization is often part of basic but sound strategies when it comes to protect personal data in general, as explained by Thomas Zerdick (2021).

If you do not need personal data, do not collect personal data (…)if you really need personal data, then start by pseudonymising this personal data. Thomas Zerdick.