PENSAR ENFERMAGEM
Revista Científica | Journal of Nursing

Data Security and Protection in Nursing

Helena Castelão F. C. Pestana[1]
orcid.org/0000-0001-7804-2989

Catarina Domingues David[2]
orcid.org/0009-0000-5585-1601

Mónica Alexandra M. Pereira[3]
orcid.org/0000-0002-2070-959X

[1] Master's degree. Nurse Manager. Hospital de Curry Cabral, Unidade Local de Saúde São José, Lisboa. Centro Clínico Académico de Lisboa, Lisboa, Portugal.

[2] Degree in Nursing. Hospital de Santo António dos Capuchos, Unidade Local de Saúde São José, Lisboa. Centro Clínico Académico de Lisboa, Lisboa, Portugal.

[3] Degree in Nursing. Nurse Manager. Hospital de Santa Marta, Unidade Local de Saúde São José, Lisboa, Portugal.

Abstract

Introduction
New technologies supported by digital solutions have been developed in both public and private health systems. In healthcare, these technologies enable surveillance, screening, prevention, treatment, and rehabilitation, among other activities. Given the importance and value of health data, we questioned the validity of collecting personal data (its amount and type), its processing, sharing, and subsequent use for purposes other than those for which it was initially collected. These concerns raise ethical-legal issues and the need to understand the complexity of data security and protection in nursing.

Objectives
To analyze the impact of the legal framework of data security and protection on nursing care practices.

Development
Personal data protection has long been recognized as a fundamental right in Portugal, gaining new significance with the General Data Protection Regulation (GDPR). The GDPR considers health-related data as sensitive personal data, which requires special handling regarding its processing and access by third parties, further supported by the Public Administration Access to Documents Law. Reflecting on the impact of this legal framework on healthcare in Portugal, in conjunction with the Nursing Code of Ethics, formed the premise for this article.

Conclusion
Information systems are crucial globally. Information systems are crucial globally. Data sharing is critical to health information systems' functioning and essential for delivering care and supporting organizational operations. Data collection, storage, sharing, and use concerns are entirely legitimate in this context. The legal framework for data security and protection affects various health domains, particularly nursing, across its multiple dimensions, including care provision, education, research, and auditing.

Keywords
Access to Information; Confidentiality; Nursing; Privacy; Data Protection; Information Security.

Corresponding author:
Helena Pestana
E-mail: hcpestana@gmail.com

Received: 21.03.2024
Accepted: 30.09.2024

How to cite this article: Pestana HCFC, David CD, Pereira MAM. Data Security and Protection in Nursing. Pensar Enf [Internet]. 2024 Sept; 28(1): 82-88. Available from: https://doi.org/10.56732/pensarenf.v28i1.322

Introdução

The rapid technological evolution has created the need for a coherent and robust legal framework for data protection across the European Union. The increase in data collection and sharing by individuals[1] in a public and global manner raises several questions regarding the right and ownership of data. Additionally, much personal data is stored in unstructured and uncontrolled formats, posing a significant challenge.

Currently, the fundamental rights of freedom and the principles recognized in the Charter of Fundamental Rights of the European Union—such as respect for private and family life, protection of personal data, freedom of expression, and information—are upheld by an international legal framework that has led to a profound transformation in the paradigm of data collection, processing, circulation, sharing, and protection. These aspects were also recently enshrined in the Portuguese Charter of Human Rights in the Digital Age[1] in the context of the digital environment.

To ensure data security, maintenance, integrity, and confidentiality, all consultation, dissemination, transmission, and replication of nominative information should only be performed by others, particularly in healthcare, within the scope of professional competencies and their respective roles and responsibilities. Institutions must adopt technical and organizational measures that ensure the lawful, transparent, and fair processing of personal data regarding the subject to whom the data pertains. Professionals are responsible for protecting data against unauthorized or unlawful processing and also against accidental loss, destruction, or damage.

This global imperative applies to various contexts, particularly in healthcare, where it was necessary to integrate the current legislative framework into care delivery. This process becomes even more complex due to the multidisciplinary nature of healthcare teams, with a high level of data production and an essential need for access to personal data for care provision, pre- and post-graduate training, research, and management.

As healthcare professionals, nurses also face the challenge of maintaining confidentiality and protecting the data of those they care for, which arises from the legislative context and the profession itself, as reflected in their code of ethics. Bearing some of these concerns in mind, we will conduct a more detailed analysis of each aspect. Our objective is to reflect on the impact of the legal framework for data security and protection on nursing care practices.

Data Security and Protection

Various regulations govern data protection in healthcare; however, we will focus on the following key legal frameworks:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of individuals regarding the processing of personal data and the free movement of such data (General Data Protection Regulation - GDPR)[2];
- Law on Access to Administrative Information (LADA)[3], Law No. 65/93, of August 26.

This national legal framework for data protection serves as the foundation to defend citizens' privacy, family life, and self-determination regarding their personal data. The GDPR, published in 2016, came into force on May 25, 2018, to establish rules for protecting individuals about the processing of personal data and the free movement of such data while safeguarding fundamental rights and freedoms. However, a new legal framework was necessary for the GDPR's application to the national context. This framework was established on August 8, 2019, with the publication of Law No. 58/2019, which "*ensures the implementation in the national legal order of Regulation (EU) 2016/679 (…) regarding the protection of individuals with respect to the processing of personal data and the free movement of such data*"[4(p. 3)] and Law No. 59/2019, which *"approves the rules on the processing of personal data for the purposes of prevention, detection, investigation, or prosecution of criminal offenses or the execution of criminal sanctions*".[5(p.1)]

Despite a legal framework, the emergence of the GDPR has brought attention to daily nursing care practice due to the ease of systematic access to individuals' and their families' data. Although professionals are aware that they should only access clinical data in the context of their therapeutic interventions, this is not always the case in clinical practice.

This strong legislative regulation has imposed limits on this matter, making it essential that all professionals fully adopt this framework, ensuring the required levels of data security. When analyzing this issue in light of general care nurses' competencies, the importance of communication and interpersonal relationships in the information transmission process becomes evident. This transmission must be accurate and understandable, ensuring it is delivered promptly and clearly to appropriately address the questions and concerns of the individual receiving care.[6 e 7]

The competencies of nurse managers also highlight the importance of upholding values, professional ethics, and legal practices, respecting ethical rules and legal regulations concerning the consultation, access, and transmission of information. From this perspective, the manager's role is emphasized as a promoter of team training and compliance with the legal framework underlying data security in healthcare.[8]

Leadership plays a fundamental role in ensuring that professionals and teams embrace and become aware of this

Note: "Person" is defined within the quality standards of nursing care by the Order of Nurses. In the consulted literature, the terms "individual," "patient," "user," and "client" emerge with similar meanings. The authors decided to retain the original terminology, as they did not consider themselves authorized to standardize the term.

DOI: 10.56732/pensarenf.v28i1.322

new healthcare data protection paradigm and implement it in daily practices.

The GDPR[2] defines *personal data* as any information related to an identified or identifiable individual (for example: a name, associated with an address, or a tax ID or social security number, an email address, physical identity elements, genetic or physiological data, data obtained through electronic devices (IP address), geolocation data, financial data, social preferences…).

However, specific data, by their nature, require enhanced protection and are referred to as sensitive data under the GDPR.[2] Examples include data related to racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, sexual orientation, and health data. Health data is defined as: "*personal data related to the physical or mental health of an individual, including the provision of health services, which reveal information about their health status*." (Clause 15 of Article 4).[2]

In this context, protecting an individual's sensitive personal data and safeguarding healthcare professionals' confidentiality face new challenges under the current legal framework. Regarding data protection issues, this framework has emphasized the importance of citizens' rights and freedoms concerning their personal data, requiring institutions to implement a series of new measures, including:

- Appointment of a Data Protection Officer (DPO);
- Procedures for obtaining consent;
- The duty to inform and provide access, with an enhanced list of information types to be provided, as well as legal deadlines to be met;
- Registration of personal data processing activities;
- Technical and organizational measures to ensure data security and protection, including confidentiality, integrity, and availability/accessibility of personal data;
- Data portability;
- Data protection impact assessments;
- Management and control of subcontractors or joint controllers involved in personal data processing;
- Notification of personal data breach incidents to the relevant supervisory authority and/or the concerned data subjects.

The Data Protection Officer must ensure that "*subcontractors, and all individuals involved in any data processing operation, are bound by a duty of confidentiality in addition to the professional secrecy obligations provided by law*" (Law No. 58/2019, August 8, 2016, Article 10, No. 2).[4]

Moreover, data controllers and joint controllers are required, within their roles and responsibilities, to adopt the technical and organizational measures (Article 25 of Law No. 59/2019, August 8, 2019)[5] capable of ensuring that personal data processing is conducted lawfully, fairly, and transparently concerning the data subject, limited to the purpose of the data collection and its processing. These measures are intended to ensure data security, maintenance of its integrity and confidentiality, and protection against unauthorized or unlawful processing, as well as accidental loss, destruction, or damage.[3] A personal data breach may occur if there is a security failure that causes the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data that has been transmitted, stored, or otherwise processed.

The GDPR[2] also addresses the rights that must be ensured for personal data subjects, including:

- Right to transparency (Article 12): Institutions must respond appropriately to provide information to data subjects in a concise, transparent, intelligible, and easily accessible manner, using clear and straightforward language.
- Right to be informed (Articles 13 and 14): Data subjects have the right to be informed about their data, regardless of whether it was collected directly from them or another source.
- Right of access (Article 15): Data subjects have the right to obtain confirmation from the data controller on whether their data is being processed and access and request a copy.
- Right to rectification (Article 16): Data subjects have the right to request the correction of any inaccurate personal data concerning them.
- Right to erasure (Article 17): Also known as the right to be forgotten, data subjects have the right to request the deletion of their personal data when it is no longer necessary for the purpose for which it was collected or if there is no legal obligation to retain it. This also applies when the subject withdraws consent on which the data processing was based.
- Right to restriction of processing (Article 18): Data subjects have the right to limit the processing of their personal data, meaning it cannot be communicated to third parties, transferred internationally, or deleted without their consent.
- Right to notification (Article 19): Data controllers must notify data subjects of any rectification, erasure, or restriction of processing unless such notification is impossible or would require disproportionate effort.
- Right to data portability (Article 20): Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format and to transmit it to another controller. They also have the right to have their data transferred directly between controllers whenever technically feasible.
- Right to object (Article 21): Data subjects have the right to object to the processing of their data at any time and for reasons related to their specific situation. The controller must cease processing unless compelling legitimate grounds for the processing override the interests, rights, and freedoms of the data subject, such as during the COVID-19 pandemic.
- Right not to be subject to automated decisions (Article 22): Data subjects have the right not to be subject to decisions based solely on their data's automated processing.

- Right to lodge a complaint (Article 77): Data subjects can file a complaint with the National Data Protection Commission if they believe their personal data has been processed in violation of GDPR standards.

To ensure compliance with these rights, the GDPR enforces sanctioning measures in cases of non-compliance. The regulation grants data subjects the right to compensation and holds data controllers accountable for damages caused by violations of the GDPR[2] and national data protection laws. Fines for breaches can reach up to 20 million euros, or for a company, up to 4% of its annual turnover.[2]

Law No. 58/2019[4] and Law No. 59/2019[5] outline the offenses and crimes related to personal data breaches, establishing the respective fines and sanctions, which include fines of up to 240 days and prison sentences of up to 2 years. The following are considered crimes related to personal data breaches.[1, 2]

- Use of data in a manner incompatible with the purpose for which it was collected;
- Unauthorized access to data;
- Data misappropriation;
- Breach of confidentiality;
- Non-compliance (failing to meet GDPR[2] obligations, such as not interrupting, ceasing, or blocking unlawful data processing; not deleting/destroying data when legally required; or refusing to cooperate without just cause when legally demanded);
- Data falsification or destruction;
- Insertion of false data;
- Illegal interconnection of data;
- Aggravated non-compliance (imposing harsher penalties on those who fail to comply with legal obligations after the deadline set by the supervisory authority). Legislators introduced aggravated penalties to encourage compliance with the law.

Regarding access to clinical information, GDPR[2] emphasizes that the individual owns an individual's personal data, with access to this nominative information restricted to.[4]

- The individual themselves;
- The legal representative of a minor or incapacitated person;
- A third party with written authorization from the data subject;
- A third party without written authorization but with a direct, personal, legitimate, and constitutionally protected interest sufficiently relevant according to the principle of proportionality.

In healthcare, concerns about respecting individuals' privacy, confidentiality, and dignity about protecting and using their personal data remain a critical issue today. Access to health data for care delivery is strictly for that purpose. In this regard, the quality and safety of care require healthcare professionals to access health information responsibly.

Thus, healthcare professionals must ensure the confidentiality and security of the data they access to provide safe care. For access to data in the context of educational activities, data subjects must provide consent for "*the processing of personal data for one or more specific purposes*"[2(p.6)], balancing the right to privacy, secrecy, and confidentiality and the necessity for clinical records access by students, as this is a necessary condition for their training.

Pre- and post-graduate training mainly takes place in clinical practice, which is relevant because the code of ethics does not bind pre-graduate students, but, as citizens, they must comply with legal requirements. Additionally, students are supervised by healthcare professionals, specifically nurses, who have the duty to safeguard the interests of the individuals they care for, ensuring the privacy and confidentiality of their data.

Research and auditing are also important activities in care provision. They require adherence to confidentiality obligations, as stipulated by the Clinical Research Law, Law No. 21/2014, of April 16[9], which allows various subjects, such as researchers or auditors, to access health data. Research is essential for advancing knowledge in the profession and often requires access to clinical data, highlighting the need for obtaining informed consent prior to accessing health data.

Therefore, it is crucial to emphasize the importance of structured policies within organizations on this matter. Nurses should only consult, disseminate, and transmit personal data within the framework of their code of ethics, competencies, and responsibilities. It is essential to adopt technical and organizational measures that ensure personal data is processed lawfully and transparently concerning the data subject, limited to the purpose for which it was collected. It is equally important to ensure data security, maintain its integrity and confidentiality, and protect it against unauthorized or unlawful processing, as well as accidental loss, destruction, or damage.

The application of timely and appropriate measures aims to prevent the loss of control over personal data, the limitation of individual rights, discrimination, and the breach of confidentiality for personal data protected by professional secrecy.

Regulation in Nursing

The code of ethics is a fundamental pillar of nursing practice in Portugal. It outlines the professional duties grounded in the rights of the citizens and communities to whom nursing care is provided, and in the responsibilities the profession has assumed.[10,11,12,13] This framework emphasizes that personal data and its processing require special attention, a focus that GDPR has reinforced. According to the regulation, the processing of personal data is only permissible when the data subject has given explicit consent or in other exceptional situations provided for in Article 9 of the GDPR.[2] One of these exceptional

DOI: 10.56732/pensarenf.v28i1.322

situations relates to the necessity of processing personal data to provide healthcare services.

The legislative framework reflects the importance of the information provided in the healthcare context, which is an essential element of the right to health protection and is integral to providing care. In this regard, the Health Information Law (Law No. 26/2016, of August 22) recognizes that clinical information is health information intended exclusively for use in care delivery and stresses the need to reinforce the duty of confidentiality and ethical education for all professionals.

This recognition of the right to information, along with the necessity of accessing and processing personal data in healthcare, implies the assignment of responsibility, with the corresponding imposition of confidentiality and professional secrecy. These are necessary conditions for the nurse-patient relationship, which must be built on truth and mutual trust in care delivery.

It is, therefore, natural that this responsibility and duty hold a prominent place in the key documents governing the profession, such as the nursing code of ethics.[10,11,12] The code sets forth the values and principles that support professional ethical duties, notably in Article 99,[12] which emphasizes significant descriptors for care provision, including: "*the right to care*" (Article 104), "*the duty to inform*" (Article 105), "*the duty of confidentiality*" (Article 106), "*respect for privacy*" (Article 107), and "*excellence in practice*" (Article 109).[12] The code of ethics itself serves as the foundation of professional practice. However, for this article, we will focus primarily on the "*duty to inform*," the "*duty of confidentiality*," and "*respect for privacy*," without diminishing the importance of the other duties outlined in the code.

The duty to inform is grounded in the principles of autonomy, dignity, and personal freedom, as it is intrinsically linked to individual freedom and respect for the decisions each person makes about themselves, representing a legitimate expression of autonomy, if it is free and informed. In other words, information must be clarified within the context of nursing care and provided to the appropriate person, whether the patient or their family. In this context, informing means "transmitting data about anything" that potentially reduces or eliminates uncertainty and contributes to decision-making in care provision. Thus, "*information consists of data with meaning and relevance to a useful context*".[13(p.110)]

Nurses have the duty to respect, defend, and promote the individual's right to informed consent (Article 105(b) of the code of ethics).[12] Respect for autonomy presupposes the person's consent. The General Directorate of Health highlights that "*informed consent in the healthcare context stems from the ethical principle of respect for autonomy, recognizing the person's ability to freely make decisions about their health and the proposed care. It involves integrating the person into the decision-making process regarding the health interventions proposed to them through sharing knowledge and skills that empower them to make the decision to accept or refuse these interventions. (...) It should be an effective moment of communication, aiming to empower the person by providing them with the necessary tools for decision-making*".[14(p.9)]

The Convention on Human Rights and Biomedicine also establishes that "*any intervention in the health domain may only be carried out after the person concerned has given free and informed consent. This person must first be given adequate information regarding the purpose and nature of the intervention, as well as its consequences and risks. The person may freely revoke their consent at any time*".[15(p.27)]

Therefore, it is essential to ensure that the information is complete, unbiased, and clearly understood by the person receiving care to respect their autonomy, empowering them and raising their awareness of the importance of their decision-making.

In a therapeutic relationship, the partnership between the nurse and the person receiving care is based on mutual respect for capabilities and recognizing each party's role. Information is a key element in this relationship, generating learning and new skills and promoting decision-making capacity. Thus, "*nurses must possess the knowledge and skills to adjust and direct information; serve as resources for clients in accessing and using information*,"[16(p.8)] thereby contributing to more meaningful nursing care for individuals.

The contexts in which nurses operate are demanding and complex, which can sometimes be discouraging. Nurses face various daily challenges, such as: What are the legal limits regarding the information provided? What information should or should not be shared with the patient and their family? When should this information be given?

It is crucial to ensure that clinical settings and the professionals working within them integrate the profession's key frameworks into their clinical practice, particularly the code of ethics, which serves as a guiding tool for clinical practice. In this regard, nurses hold a privileged position within the multidisciplinary team due to the time spent with and proximity to the patient. They are responsible for conveying essential information about the patient's health plan. Providing information is a duty, and it must be proactive, especially considering that patients are often in a vulnerable position, preventing them from asking all necessary questions. Therefore, nurses are responsible for providing the necessary information regarding care within the therapeutic plan, enabling patients to make informed and autonomous decisions.[14,16] The act of sharing information with the patient should be viewed as a therapeutic action[16] rather than merely an administrative task.

The nurse's duty of confidentiality is addressed in various documents, such as the Patient Rights Act (Law No. 15/2014, of March 21, Article 6), which states, "*Health service users have the right to confidentiality regarding their personal data*".[17(p.2)] This right is grounded in the Universal Declaration of Human Rights (Article 12), which states, "*No one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence, nor to attacks upon their honor and reputation*".[14(p.2)]

Additionally, the nursing code of ethics (Article 106, Clause A) emphasizes that "*nurses must consider confidential all information related to the care recipient and their family, regardless of the source*".[18(p.8)]

The nurse must collect data to identify nursing care needs and establish an intervention plan. Despite the potential benefits, the nurse should remain aware that this data collection constitutes an intrusion into the patient's life and privacy. It is essential to highlight that nurses access personal data in their role as healthcare professionals. Thus, they must ensure the confidentiality of all information, regardless of the source (whether from the patient, the family, the medical record, or direct observation, among others).

Nurses should only collect information relevant and useful to the provision of care, meaning only the information strictly necessary for that moment's care process should be gathered. In this context, sharing pertinent information should only occur "*with those involved in the therapeutic plan*" (Article 106, Clause B).[12(p.8)] As the Jurisdictional Council of the Order of Nurses notes in its stance on patient safety, "*all information is confidential, and only the relevant information should be shared with those involved in the therapeutic plan*".[19(p.6)] *Sharing information requires the patient's authorization for that purpose.*[13(p.118)] It is important to emphasize that "*all information regarding health status, clinical condition, diagnosis, prognosis, and treatment, as well as other information, must remain confidential even after death*".[15(p.120)]

The information entrusted to nurses represents a professional responsibility, which must consider its relevance and the intended purpose. It is essential to clearly identify the professionals involved in the therapeutic process and ensure that only those individuals have access to relevant and useful information, thereby preventing unauthorized access and privacy violations. According to CJ 041/2020 of the Order of Nurses, "*only nurses involved in the therapeutic process with the patient are permitted to consult the clinical record, provided there is a clinically and functionally appropriate reason*".[20(p.3)]

The right to confidentiality reinforces the principle that the individual should, whenever possible, decide what information can be shared. This personal right aligns with the professional duty of confidentiality.

The physical layout of clinical settings often poses challenges to maintaining confidentiality. There are frequently no specific rooms designated for providing sensitive information to patients or their families, leading to the use of improvised spaces, which can violate the right to confidentiality.

Finally, the ethical duty of nurses to respect privacy is emphasized in Article 107, Clause A, which states, "*Respect the person's privacy and protect them from intrusions into their private and family life*".[12(p.12)] Protecting individuals from invasions of privacy extends far beyond physical protection. It also involves safeguarding their personal data and most intimate information, such as personal, emotional, sexual, political, or religious beliefs, illnesses, treatments, and more.

Therefore, nurses must exercise extreme caution when accessing or sharing patient information without a therapeutic purpose. This includes refraining from orally sharing sensitive information or leaving information systems open and accessible to others, which in itself constitutes a crime. Such scenarios fail to ensure the data subject's privacy, potentially allowing unauthorized individuals access to privileged and confidential information, which should only be accessible to the healthcare professionals involved in providing care.

Final Considerations

The importance of data protection is universally recognized across different domains, particularly in healthcare, where it plays a crucial role in care delivery, education, research, and auditing. The concerns in this area are well-known, not only because they involve citizens' rights but also because they pertain to the duties of healthcare professionals. Accordingly, extensive legislation has been developed to ensure "*all precautions are taken to respect the privacy of individuals and minimize potential harm to their rights*".[2(p.1)]

The GDPR[2] offers a legal framework sensitive to the importance of health data and its appropriate use, which is essential for providing excellent care. The need to access a patient's clinical information is essential for improving the planning, safety, and efficacy of care. This need is rooted in the trust between the professional and the patient or family. It is safeguarded by the duties of confidentiality and respect for privacy, as outlined in the nursing code of ethics.

The complementary relationship between the duty to inform, the duty of confidentiality, and respect for privacy enumerated in the various updates of the code of ethics[10,11,12] and the existing legislation on citizen data security and protection naturally emerges from a context that seeks balance between the necessity of accessing information and the right of every individual to have their information protected.

When the patient is involved in decisions about the consultation, treatment, and access to data, their right to self-determination, privacy, and intimacy is ensured. Empowering the patient is fundamental to achieving better health outcomes while maintaining their dignity.[16]

Given the complexity of this subject and the challenges associated with the changing data protection paradigm, it becomes clear that progress must be made incrementally. Leadership plays a critical role in facilitating this process and encouraging behavioral changes that prioritize citizens and the defense of all their rights.

Authors' Contributions

H.C.F.C: Conception, Drafting of the manuscript; Critical revision of the manuscript;
C.D.D: Drafting the manuscript; Critical revision of the manuscript;
M.A.M.P: Drafting the manuscript; Critical revision of the manuscript.

Conflicts of interest and Funding

No conflicts of interest were declared by the authors.

Acknowledgments

The authors thank the Professor Paulino Artur Ferreira Sousa for his availability.

Sources of support / Financing
The study was not funded.

References

1. Lei n.º 27/2021. Carta portuguesa de direitos humanos na era digital. Diário da República n.º 95, Série I de 2021-05-17, [Internet]. [cited 2023 dezembro 15]; p. 5-10. Available from: **https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2021-164870244**

2. Regulamento (UE) 2016/679 de 27 de abril. Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia (UE). Jornal Oficial da União Europeia [Internet]. 2016 maio 4 [cited 2023 dezembro 15]; 59(L119): 1-88. Available from: **https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679**

3. Lei n.º 65/93. Lei de acesso aos documentos da administração (LADA). Diário da República n.º 200, Série I-A de 1993-08-26 [Internet]. [cited 2024 fevereiro 28]; p. 4524 – 4527. Available from: **https://dre.pt/dre/detalhe/lei/65-1993-632408**

4. Lei n. º 58/2019. Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Diário da República n.º 151, Série I de 2019-08-08 [Internet]. [cited 2024 fevereiro 16]; p. 3-40. Available from: **https://dre.pt/dre/detalhe/lei/58-2019-123815982**

5. Lei 59/2019. Aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais. Diário da República n.º 151, Série I de 2019-08-08 [Internet]. [cited 2024 fevereiro 16]; p. 41-68. Available from: **https://dre.pt/dre/detalhe/lei/59-2019-123815983**

6. Ordem dos Enfermeiros. Competências do enfermeiro de cuidados gerais. Lisboa: Ordem dos Enfermeiros; 2003.

7. Regulamento n.º 190/2015. Regulamento do perfil de competências do enfermeiro de cuidados gerais. Diário da República n.º 79, Série II de 2015-04-23 [Internet]. [cited 2024 março 1]; p. 10087–10090. Available from: **https://diariodarepublica.pt/dr/detalhe/regulamento/190-2015-67058782**

8. Regulamento n. º 101/2015. Regulamento do perfil de competências do enfermeiro gestor. Diário da República, n.º 48, Série II de 2015-03-10 [Internet]. [cited 2024 março 8]; p. 5948–5952. Available from: **https://diariodarepublica.pt/dr/detalhe/regulamento/101-2015-66699805**

9. Lei n. º21/2014. Lei da investigação clínica. Diário da República n.º 75, Série I de 2014-04-16 [Internet]. [cited 2024 fevereiro 28]; p.2450–2465. Available from: **https://dre.pt/dre/detalhe/lei/21-2014-25344024**

10. Decreto-Lei n.º 104/98. Cria a Ordem dos Enfermeiros e aprova o respectivo Estatuto. Diário da República n.º 93, Série I-A de 1998-04-21. [Internet]. [cited 2024 março 8]; p. 1739-1757. Available from: **https://diariodarepublica.pt/dr/detalhe/decreto-lei/104-1998-175784**

11. Lei n.º 111/2009. Procede à primeira alteração ao Estatuto da Ordem dos Enfermeiros. Diário da República n.º 180, Série I de 2009-09-16. [Internet]. [cited 2024 março 8]; p.6528-6550. Available from: **https://diariodarepublica.pt/dr/detalhe/lei/111-2009-490239**

12 Lei n. º 156/2015. Segunda alteração ao Estatuto da Ordem dos Enfermeiros, conformando-o com a Lei n.º 2/2013, de 10 de janeiro, que estabelece o regime jurídico de criação, organização e funcionamento das associações públicas profissionais. Diário da República n.º 181, Série I de 2015-09-16 [Internet]. [cited 2024 março 11]; p 8059-8105. Available from: **https://diariodarepublica.pt/dr/detalhe/lei/156-2015-70309896**

13. Nunes L, Amaral M, Gonçalves R. Código deontológico do enfermeiro: Dos comentários à análise de casos. Lisboa: Ordem dos Enfermeiros; 2005.

14. Direção-Geral da Saúde. Consentimento informado, esclarecido e livre dado por escrito: Norma 015/2013 de 03/10/2013 atualizada a 04/11/2015 [Internet]. Lisboa: Direção-Geral da Saúde; c2024 [cited 2024 fevereiro 7]. Available from: **https://www.dgs.pt/normas-orientacoes-e-informacoes/normas-e-circulares-normativas/norma-n-0152013-de-03102013.aspx**

15.Resolução da Assembleia da República n.º 1/2001, de 3 de janeiro. Convenção para a protecção dos direitos do homem e da dignidade do ser humano face às aplicações da biologia e da medicina: convenção sobre os direitos do homem e a biomedicina. Diário da República n.º 2, Série I-A de 2001-01-03, [Internet]. [cited 2024 janeiro 18]; p. 14 – 36. Available from: **https://diariodarepublica.pt/dr/detalhe/resolucao-assembleia-republica/1-2001-235128**

16. Ordem dos Enfermeiros. Consentimento informado. Enunciado de Posição EP02/07. Lisboa: OE; 2007

17. Lei n.º 15/2014. Direitos e deveres do utente dos serviços de saúde. Diário da República n.º 57, Série I de 2014-03-21 [Internet]. [cited 2024 março 1]; p.2127-2131. **https://dre.pt/dre/legislacao-consolidada/lei/2014-106901319**

18. World Health Organization. A declaration on the promotion of patients' rights in Europe. Principles of the rights of patients in Europe: a common framework. Copenhagen: WHO Regional Office for Europe, 1994. 30p.

19. Ordem dos Enfermeiros. Tomada de posição sobre a segurança do cliente. Parecer do Conselho Jurisdicional. 2 maio 2006. Lisboa: OE; 2006

20. Ordem dos Enfermeiros. Acesso a Informação de Saúde. Parecer do Conselho Jurisdicional 041/2020. Lisboa: OE; 2020.