Privacy Management Accountability Framework in a Cancer Registry

Sónia Dória-Nóbrega [1], Rafael Silva[2], Sofia Martins[2], Júlia Amorim[2]

[1] Data Protection Officer of Hospital de Braga, Portugal.
[2] Cancer Registry of Hospital de Braga, Portugal.

Introduction

The importance of cancer registries for planning, management and evaluation of healthcare systems has been shown widely during the last decades.
Since 25th May 2018, the european General Data Protection Regulation (GDPR) aplies to cancer registries´s data, enhancing more individual control of data subjects on their data, more responsabilities for data controllers, data protection by design and by default and the best practices in information security.

Objectives

The aim of this review is to examine what are the implications of GDPR on the privacy management activities of cancer registries.

Methods

We have mapped the GPDR to the Framework to help streamline the compliance, structured on 13 privacy management processes, identifying technical and organisational measures that, if put in place, may produce appropriate evidence to demonstrate GDPR compliance in a hospital cancer registry.

Results

Privacy Management Categories	Aim	Technical and organisational measures	Relevant GDPR Articles
1. Maintain Governance Structure	Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures	**a.** Assign responsibility for data privacy to an individual (representative)	27
		b. Appoint a Data Protection Officer (DPO)	37, 38
		c. Conduct an Enterprise Privacy Risk Assessment	24, 39
2. Maintain Personal Data Inventory and Data Transfer Mechanisms	Maintain an inventory of the location of key personal data storage or personal data flows, including cross-border, with defined classes of personal data	**a.** Maintain na inventory of personal data and/or processing activities	30
		b. Maintain documentation of the transfer mechanism used for cross-border data flows (e.g., model clauses, BCRs, regulator approvals)	45, 46, 49
		c. Use contracts as a data transfer mechanism (e.g. Standard Contractual Clauses)	46
		d. Use regulator approval as a data transfer mechanism	46
		e. Use adequacy or one of the derogations (e.g. consent, performance of a contract, public interest) as a data transfer mechanism	45, 48, 49
		f. Use Privacy Shield as a data transfer mechanism	46
3.Maintain Internal Data Privacy Policy	Maintain a data privacy policy that meets legal requirements and addresses	**a.** Maintain a data privacy policy	5, 24, 91
		b. Document legal basis for processing personal data	6, 9
4.Embed Data Privacy Into Operations	Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives	**a.** Maintain policies/procedures for collection and use of sensitive personal data (including biometric, health, genetic data)	9
		b. Maintain policies/procedures for collection and use of children and minors' personal data	8, 12
		c. Maintain policies/procedures for maintaining data quality	5
		d. Maintain policies/procedures for the de-identification of personal data	89
		e. Maintain policies/procedures to review processing conducted wholly or partially by automated means	6, 13, 14
		f. Maintain policies/procedures for secondary uses of personal data	6, 13, 14
		g. Maintain policies/procedures for obtaining valid consent	6, 7, 8
		h. Integrate data privacy into records retention practice	5
		i. Integrate data privacy into research practices (e.g. scientific and historical research)	21, 89
5. Maintain Training and Awareness Program	Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks	**a.** Conduct privacy training	39
6. Manage Information Security Risk	Maintain an information security program based on legal requirements and ongoing risk assessments	**a.** Integrate data privacy risk into security risk assessments	32
		b. Integrate data privacy into an information security policy	5, 32
		c. Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)	32
		d. Maintain measures to encrypt personal data	32
		e. Maintain procedures to restrict access to personal data (e.g. role-based access, segregation of duties)	32
		f. Conduct regular testing of data security posture	32
7. Manage Third–Party Risk	Maintain contracts and agreements with third-parties and affiliates consistent with the data privacy policy, legal requirements, and operational risk tolerance	**a.** Maintain data privacy requirements for third parties (e.g., clients, vendors, processors, affiliates)	28, 32
		b. Maintain procedures to execute contracts or agreements with all processors	28, 29
		c. Conduct due diligence around the data privacy and security posture of potential vendors/processors	28
8. Maintain Notices	Maintain notices to individuals consistent with the data privacy policy, legal requirements,	**a.** Maintain a data privacy notice	8, 13, 14
		b. Provide data privacy notice at all points where personal data is collected	13, 14, 21
9. Respond to Requests and Complaints from Individuals	Maintain effective procedures for interactions with individuals about their personal data	**a.** Maintain procedures to respond to requests for access to personal data	15
		b. Maintain procedures to respond to requests and/or provide a mechanism for individuals to update or correct their personal data	16, 19
		c. Maintain procedures to respond to requests to opt–out of, restrict or object to processing	7, 18, 21
		d. Maintain procedures to respond to requests for data portability	20
		e. Maintain procedures to respond to requests to be forgotten or for erasure of data	17, 19
10. Monitor for New Operational Practices	Monitor organizational practices to identify new processes or material changes to existing processes and ensure the implementation of Privacy by Design principles	**a.** Integrate Privacy by Design into data processing operations	25
		b. Maintain DPIA guidelines and templates	35
		c. Conduct DPIAs for new programs, systems, processes	5, 6, 25, 35
		d. Conduct DPIAs for changes to existing programs, systems, or processes	5, 6, 25, 35
		e. Engage external stakeholders (e.g., individuals, privacy advocates) as part of the DPIA process	35
		f. Track and address data protection issues identified during DPIAs	35
		g. Report DPIA analysis and results to regulators (where required) and external stakeholders (if appropriate)	36
11. Maintain Data Privacy Breach Management Program	Maintain an effective data privacy incident and breach management program	**a.** Maintain a data privacy incident/breach response plan	33, 34
		b. Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol	12, 33, 34
		c. Maintain a log to track data privacy incidents/breaches	33
12. Monitor Data Handling Practices	Verify operational practices comply with the data privacy policy and operational policies and procedures, and measure and	**a.** Conduct self–assessments of privacy management	24, 39
		b. Maintain documentation as evidence to demonstrate compliance and/or accountability	5, 24
13. Track External Criteria	Track new compliance requirements, expectations, and best practices	**a.** Identify ongoing privacy compliance requirements, e.g., law, case law, codes, etc.	39

Conclusions

The regulation aims at protecting the confidentiality of personal health data whilst preserving the benefits of data processing for research and public health purposes (exceptions in article 9 and 89).
However, it is mandatory to ensure data are protected and all the technical and organizational measures are developed in order to ensure the rights and freedoms of the data subjects.
There are still many doubts about the transposition of GDPR for the national law, in Portugal. Meanwhile, hospitals must comply with the general rules and prepare for the authority control audits.

References

General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 of the European Parliament and of the Council) http://eugdpr.org/the-regulation/;

Evert-Ben van Veen (2018): "Observational health research in Europe: understanding the GDPR and underlying debate", European Journal of Cancer, 104 (2018) 70-80.