GDPR Case Study: Centro Hospitalar Barreiro Montijo

Ankita Sharma, Privacy-Conscious Computer Systems

1. Abstract:

A public hospital establishment in Portugal, Centro Hospitalar Barreiro Montijo (CHBM), was fined 400,000 € for General Data Protection Regulation (GDPR) violations by Comissão Nacional de Protecção de Dado (CNPD) in October 2018. This was the first GDPR fine in Portugal. The fines that were issued against the hospital were related to insufficient hospital account management practices which enabled unauthorized and unrestricted access to sensitive personal data. The hospital contested these violations by indicating their use of an external data processing service, but the CNPD has concluded that it is the hospital's responsibility to ensure that the systems they use comply with the GDPR. The hospital will not have to pay the fine with Portugal's recent law passed in June 2019 implementing GDPR which exempts public entities from fines imposed on them in the short run.

2. Background:

CHBM operates in an area with a direct influence of 75,000 to 500,000 inhabitants [5]. CHBM utilizes an IT system that is provided to public hospitals by the Portuguese Health Ministry called SClinico [6]. All patient medical data is inserted using this software and once inserted, the patient medical data is exposed to any hospital employee, regardless of their role at the hospital [13]. Essentially, any technical profile within the framework is created with unlimited access [3]. While the current situation raises several concerns, what is more alarming is that if an employee's credentials i.e. username and password provided by the hospital are compromised, now *anyone* can have unlimited access to personal and private patient data [6].

The CHBM GDPR violations were fined by the CNPD. The CNPD is an independent body that has the power to supervise and monitor compliance with laws and regulations with regards to personal data protection in accordance with the current Portuguese Data Protection Law [1]. The CNPD is the Portuguese Data Protection Authority [8].

The GDPR left to each member state of the EU the decision on "whether and to what extent administrative fines should be imposed on public authorities and bodies [11]." In June 2019, Portugal finally approved a law implementing GDPR which made the decision to exempt public entities for a "maximum period of three years [11]." It has been noted in the media that the CNPD was not actively involved in the drafting of this law [11].

3. GDPR Violations:

The following articles of the GDPR [9] were violated by CHBM:

(1) Article 5(1)(c): Data minimization
(2) Article 5(1)(f): Appropriate security of personal data
(3) Article 32(1)(b): Ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services

These violations are in direct relation to CHBM's non-compliant access to and protection of patient data.

3.1 Details

The CNPD acted on a newspaper article before investigating CHBM GDPR infringement. A medical workers union comprising of Portuguese doctors reported that non-clinical staff had access to CHBM's computer system [7] in a newspaper article. A few months later, CPND conducted an audit on the hospital and confirmed the violations that were known through the media.

The audit revealed that 985 users were registered on the system as "physician" despite there only being 296 physicians in the hospital as per the official hospital human resources charts [8]. The audit also revealed that only 18 user accounts were inactive; the last account deactivated in November 2016 [8]. Furthermore, a test profile was set up for technical personnel which the CPND found to have unrestricted access to patient information [7] that *should* only be accessible to physicians.

3.2 Responsibility

Any profile created in the CHBM's IT framework has unrestricted access to confidential patient information.

CHBM argued that it was not responsible for the deficiencies in their account management system since they used an external system, provided to public hospitals by the Portuguese Health Ministry [12]. However, CNPD holds the hospital responsible for ensuring that the systems they use comply with GDPR.

The GDPR violations stem from a lack of attention and care by the hospital administration. Before beginning to improve the organizational and technical infrastructure, the hospital needs to think about procedures for the creation and definition of access [2]. Some considerations that should be made are (1) Allowing access to patient data based on divisions of specialty (2) Restricting non clinical staff from accessing clinical data (3) Allowing account types to only access what they need (4) Deactivating user accounts when a user is no longer employed [10].

3.3 Prevention

CHBM should have prioritized implementing the principle of least privilege i.e. minimizing account privilege based on the requirements of a task or job [4]. This would have avoided the unregulated and unrestricted access to private patient information among all staff employed at CHBM. While this principle is helpful in building a strong foundation for compliant access to secure data, it also requires periodic checks in the form of access reviews to ensure that this principle is being adhered to over time and that the system is up to date.

Automated data classification [4] is another helpful technique that can aid in an organization determining what sensitive data exists and who has access to it.

Implementing protocols or procedures to obtain consent from patients to process their data and levels of data access would have also aided in CHBM avoiding a significant portion of the penalty [2].

Keeping security controls up to date aids in providing evidence that the processing of personal data in an organization is happening securely. CHBM has been unable to document this which is a violation of the GDPR [9].

4. Conclusion:

There is a lot to learn from the GDBR violations of CHBM. For instance, if policies and procedures are not put in place from the ground up, it becomes difficult to control a situation properly and promptly. Sources have noted that the CHBM administration was aware of the flaws within their system long before CNPD conducted their investigation. The CHBM administration chose to ignore the situation probably because of the enormous effort that would be required to correct the situation.

It is impressive how quickly CNPD acted on the GDPR violations that were made public to the media. The quick response goes to show the powerful impact GDPR is having in shifting where the priority of protecting user data falls in the eyes of both public and private institutions.

The CHBM case is a really convincing argument for GDPR and why we need it. Without it, organizations can make reckless decisions and not be held accountable for it.

The penalty imposed on CHBM is warranted by the CNPD. Although CHBM is excused from the fine with recent laws passed in Portugal that provide public institutions up to 3 years to become compliant with GDPR, the media buzz and audit are enough to give CHBM a wakeup call to ameliorate the situation.

5. References:

[1] *CNPD English Page*, www.cnpd.pt/english/index_en.html

[2] Fernández, Alba. "First Substantial GDPR Fine Issued against a Hospital in Portugal • AuraPortal." *AuraPortal*, 10 Jan. 2019, www.auraportal.com/first-substantial-gdpr-fine-issued-against-a-hospital-in-portugal/.

[3] "GDPR Fine of EUR 400,000 to Portuguese Hospital." *GDPR as The New License to Operate*, www.omada.net/en-us/more/news-events/news/gdpr-fine-portuguese-hospital.

[4] "GDPR Fines Issued So Far: Key Takeaways." *Netwrix Blog GDPR Fines Issued So Far Key Takeaways Comments*, 18 June 2019, blog.netwrix.com/2019/06/18/gdpr-fines-issued-so-far-key-takeaways/.

[5] "Healthcare in Portugal." *Wikipedia*, Wikimedia Foundation, 12 July 2019, en.wikipedia.org/wiki/Healthcare_in_Portugal#Public_hospitals.

[6] "Hospital Center Barreiro-Montijo Leaves Patient Data Unprotected ." *GetComplied Blog*, 31 Oct. 2018, blog.getcomplied.com/en/hospital-center-barreiro-montijo-leaves-patient-data-unprotected/.

[7] Irwin, Luke. "Portuguese Hospital Appeals GDPR Fine." *IT Governance Blog*, 15 Jan. 2019, www.itgovernance.eu/blog/en/portuguese-hospital-appeals-gdpr-fine.

[8] Monteiro, Ana Menezes. “First GDPR Fine in Portugal Issued against Hospital for Three Violations.” *First GDPR Fine in Portugal Issued against Hospital for Three Violations*, International Association of Privacy Professionals, 4 Jan. 2019, iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/.
[9] “Official Journal of the European Union.” *L_2016119EN.01000101.Xml*, eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32016R0679.
[10] “Portuguese Hospital Fined For GDPR Violations.” *Eagle Consulting Partners Inc.*, 10 May 2019, eagleconsultingpartners.com/general-news/portuguese-hospital-fined-for-gdpr-violations/.
[11] “Portuguese Law Implementing GDPR Finally Approved.” *Cloud Privacy Check (CPC)*, cloudprivacycheck.eu/latest-news/article/portuguese-law-implementing-gdpr-finally-approved/.
[12] Stevovic, Jovan. “GDPR Fines – 7 Key Lessons for Healthcare.” *The Chino.io Blog*, The Chino.io Blog, 12 Feb. 2019, www.chino.io/blog/gdpr-fines-in-helthcare-7-lessons/.
[13] “Top 5 GDPR Fines.” *Data Privacy Manager*, 10 Sept. 2019, dataprivacymanager.net/top-5-gdpr-fines/.