CSCI 2390 GDPR Case Study: Doctors without Encryption

Aaron Jeyaraj
Brown University

Chris Sarli
Brown University

Abstract

CNIL, the French data protection agency levied fines against two doctors for taking insufficient measures to protect patient data under and for failing to notify the CNIL of a data breach under Articles 32 and 33 of the GDPR. The breach of data occurred as the ports on the doctors' Internet servers were not closed, allowing external agents to connect to the servers and access data stored on them. In addition, neither doctor had taken steps to encrypt the data on their hard drives as suggested by the CNIL's guidelines. Furthermore, neither doctor had fulfilled their obligation to notify the CNIL of the breach. The CNIL also highlighted that as the breach had involved sensitive medical information as defined by Article 9, that it was paramount the doctors be especially vigilant in protecting the data.

1 Introduction

On December 7, 2020, the Commission nationale de l'informatique et des libertés (CNIL), the Data Protection Authority (DPA) for France decided two independent cases relating to the responsibility of French doctors in securing patient information under GDPR. Out of protection for the privacy for the doctors, their practices, and the patients they serve, information that would identify the doctors or their practices were redacted from relevant publicly-available documents. Therefore, the cases can best be identified by their case numbers, `SAN-2020-014` and `SAN-2020-015`.

In both cases, doctors maintained Internet-connected servers which stored patient information. The servers did not have any ports closed, and lacked security measures sufficient to prevent unrestricted, unauthenticated access to the information stored on the servers, meaning patient data was effectively publicly available. In both cases, it was found that the stored data was not encrypted. Additionally, these breaches were both brought to the attention of the doctors by CNIL, and the breaches were not reported to patients in a timely manner. [2, 3]

Although the cases were similar and apparently decided concurrently, there were situational differences between the two. In `SAN-2020-014`, one of the primary technical issues appears to have been caused directly by a doctor, [3] whereas in `SAN-2020-015`, the doctor claimed that the primary infraction was caused by an IT service provider to which they designated certain responsibilities. [2] Taken together, these cases therefore provided a test of the definitions and responsibilities defined in GDPR.

Although it is not possible to determine all details surrounding the prominence and position of the doctors or the number of patients affected (given the aforementioned redactions), we believe it is reasonable to assume that the doctors run small, independent firms. Filings list the doctors themselves (not companies or larger entities) as defendants, and in the case of `SAN-2020-014`, suggest that a doctor personally and directly adjusted the configuration of a server to allow for remote access, [3] which is a task of sufficient technical knowledge and skill that we believe this would occur at a larger practice or in a hospital environment. Additionally, given that there is little press coverage of this case (and effectively none outside of articles covering the case for its wider GDPR implications, and not the actual case-specific penalties and damages), we believe that this violation affected a relatively small number of individuals.

2 GDPR violation

2.1 What happened?

The technical issues primarily focus on the network settings of the routers used by the doctors. Both doctors had a home router which they used to facilitate connection with a physical storage device located in their homes which contained medical information on their patients. In order to access this data remotely, the doctors had all the ports on their routers opened. This, however, allowed the information stored on the hard drives to be freely accessible from the Internet. The issue was thus the fact that the doctors did not take sufficient steps to

safeguard the security of the health information that they were processing.

Furthermore, both doctors did not encrypt some of the information stored on these hard drive, even when this encryption was made available to them by the operating system, either by encrypting a container of files or each individual file. This unencrypted data included medical images, patients' full legal names and dates of birth, dates of medication examinations, names of the physicians who carried out medical examinations, names of referring physicians, and locations where medical examinations occurred.

In the case of SAN-2020-014, these oversights resulted in the patient data being exposed for 4 months. For SAN-2020-015, the data was exposed for 5 years. Both cases were reported to CNIL by third-parties: the reporter's identity for case SAN-2020-014 is not clear [3], while the reporter for case SAN-2020-015 was disclosed to be a "computing security company." [2]

2.2 Who/What is Responsible?

In both cases, the CNIL found that the doctors were the ones who were ultimately responsible for the breach, as both of them were data controllers. Thus, they were obligated under Article 32 of the GDPR to adopt sufficient technical measures to minimize the risk of data breaches.

The defendant in SAN-2020-015 claimed that an IT service provider, and not the doctor themself, had been the entity which modified the configuration of the system, implying that responsibility should lie partially or fully with that contractor rather than with the doctor. The CNIL concluded that these circumstances were not taken into account when assessing whether the doctor was compliant with Article 32. The CNIL judgement noted that this fell under the clause of adopting adequate organizational measures—such as the distribution of the responsibilities between controller and processor (the IT service company in SAN-2020-015 was considered to be a data processor), and sufficient training for those handling the data (in this case, both of the doctors).

The CNIL also ruled that the doctors were not in compliance with Article 33 of the GDPR as neither of them had reported the breach to the CNIL. In both cases, however, CNIL was the one who notified the doctors of the breach. In spite of this, the CNIL concluded that this did not relieve the doctors of their obligations to notify the CNIL of the breach.

2.3 What Could Have Prevented This?

Prior to the outcome of these cases, the CNIL and the French Medical Council (CNOM: Conseil national de l'Ordre des médecins) had published an instructional guide in June 2018 specifically to help physicians in private practice ensure compliance with GDPR [4]. This guide included relevant technical measures that the physicians in these cases could have taken to better ensure compliance with GDPR. It also included samples of the required security clauses for subcontracting data processing responsibilities to other parties.

Furthermore, the CNIL/CNOM guide also referenced a separate guide specifically focused on security, which included information on guaranteeing the security of the data infrastructure. [1] However, this guide varies widely in the technicality of its content. For example, under a section titled "Securing Servers", one of the "elementary precautions" they suggest physicians take is "limiting access to administrative tools to authorized persons," but another is "implementing the TLS protocol and taking measures to prevent SQL injection attacks." [1, 17]

It appears as if the governing agencies involved in this case, CNIL and CNOM, made a not insignificant effort to educate physicians on the requisite measures they would have to take to ensure GDPR compliance. In spite of this, however, there does seem to be an inherent knowledge gap that exists within the medical field, as in these cases, it appears as if the doctors lacked a sufficient technical understanding of the systems which they were operating (although GDPR requires them to undertake the necessary training to appreciate some of these technical nuances). Potential economic inequalities might also factor into some of these cases, as doctors who serve underserved communities in rural and urban France might be less equipped financially to handle some of the more onerous requirements of the GDPR.

3 Discussion

3.1 Outcome of the Case

In light of the breaches under Articles 32 and 33 of the GDPR, the doctor in SAN-2020-014 was fined €3,000 and the doctor in SAN-2020-015 was fined €6,000 on December 17, 2020.

We feel that this is a reasonable outcome. While not meaningless, we do not believe that the fines would ruin either doctor or their practices. Given that it appears that both doctors were well-intentioned, and not particularly negligent given their lack of background technical and legal knowledge, we would have objected if the penalty imposed was more severe in nature.

However, as we discuss in the next subsection, if CNIL's intention in pursuing these cases is to "make an example" or "fire a warning shot" for other private doctors who could inadvertently make similar infractions, we believe that additional regulation aimed at helping small and independent firms with the burden of GDPR compliance should be explored.

3.2 Regulatory Remedies for Gaps in Regulation

We believe that these cases, taken together, demonstrate a "gap" in GDPR that might best be solved by additional gov-

ernment regulation and action. SAN-2020-014 offers a cautionary tale: even if a doctor possesses the technical know-how and enthusiasm to administer a server and VPC, they do not necessarily have the knowledge and experience needed to correctly set up a VPN (or other security measures) to protect the information they store. On the other hand, SAN-2020-015 offers indications that delegating such tasks to professional IT service providers, which *should* be expected to establish a system in compliance with GDPR is not a shield for a doctor and their practice from related liability.

Acknowledging that doctors should not be expected to understand the complexities and requirements of privacy law themselves is reasonable, but also raises problems when a doctor can be held liable for the infractions of supposed experts in the field. Having established that a doctor should not be expected to administer their own computing infrastructure given a lack of expertise on their part, it is hardly reasonable to expect them to fully assess the compliance offered by a contracted service provider.

We propose a solution whereby CNIL (with other DPAs) designate certifications for certain industries, and contractors such as IT service providers can earn accreditations from these authorities. Such accreditations would be designed for contractors aimed at servicing small firms in specific industries (for example, there may be a certification for contractors servicing independent medical practices) which are too small to retain in-house expertise on data processing and privacy, to maintain their own infrastructure.

Such certifications may designate specific legal responsibilities and protections. Specifically, we believe that should a small firm (like one of the doctors' practices) choose to contract with an accredited service provider, the contractor should be treated as a *proxy* data controller, rather than a data processor under GDPR. As a proxy data controller, the contractor may function as a data processor, but is responsible for ensuring that any services they provide to the actual data controller (the doctor, in this example) are compliant with GDPR. Should an issue be found with the infrastructure they provide, even if they are functioning as data processors, the contractor would be partially or fully liable as the data controller (including being vulnerable to the loss of their certification), and the firm (the doctor's practice) would be partially or fully shielded from responsibility.

We don't believe that small firms in specific industries should be *required* to contract with a firm with a given accreditation, but we do believe that the legal protections offered to them by doing so would be a powerful incentive that ultimately benefits individual privacy. There may be increases in overhead to account for such requirements, but we believe the individual privacy benefits and relative predictability of this scheme are worth the costs. Much in the way we expect our physicians to be board certified and held to a consistent level of care, we believe that doctors should be able to expect that IT service providers they contract with the be similarly certified.

References

[1] title = Commission nationale de l'informatique et des libertés.

[2] GDPRhub. Cnil - san-2020-015 — gdprhub,, 2020. [Online; accessed 23-September-2021].

[3] GDPRhub. Cnil - san-2020-014 — gdprhub,, 2021. [Online; accessed 23-September-2021].

[4] Conseil national de l'Ordre des médecins. Guide pratique sur la protection des donnÉes personnelles, 2018. [Online; accessed 23-September-2021].