Research Article

Portuguese Journal of PUBLIC HEALTH

Port J Public Health 2017;35:52–66
DOI: 10.1159/000477650

Received: January 29, 2016
Accepted: February 17, 2017
Published online: September 28, 2017

Over Troubled Water: E-Health Platforms and the Protection of Personal Data: The Case of Portugal

Maria Eduarda Gonçalves[a] João Raimundo[b]

[a]ISCTE – Lisbon University Institute, DINÂMIA'CET-IUL, Centre for Socioeconomic and Territorial Studies, ISCTE-IUL, Lisbon, Portugal; [b]DINÂMIA'CET-IUL, Centre for Socioeconomic and Territorial Studies, ISCTE-IUL, Lisbon, Portugal

Keywords

Big data · Data protection · E-health · E-health platforms · Health data

Abstract

How healthcare is being administered is nowadays one of the distinctive traits expressing the progress of a given society. The steadfast implementation of e-health services has become an indispensable tool in order to bring the provision of healthcare to the next level. Notwithstanding e-health's actual and promising applications, e-health hinges on highly sensitive information on patients' personal lives and even intimacy, which, in Member States of the European Union (EU), must comply with the pertinent personal data protection legislation. In effect, health data have been classified as a special category of personal data by Directive 95/46/EC, the Data Protection Directive (DPD). The DPD subjects the processing of personal health data to a specific, stronger protection compared to less sensitive personal data in the form of a prohibition, which can only be excepted when the data subjects grant their explicit consent to the processing or if such consent is overridden by a superior interest provided by the law. Aware of the major changes brought about by technological progresses in this field, the EU initiated in January 2012 a revision of the DPD. Eventually, Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) were published in May 2016, to be applicable as of spring 2018. Regulation 2016/679 displays an even greater carefulness with the safeguard of health data than the DPD. Yet, it is unclear whether this legal reform is up to the challenge of current technological developments, particularly, as so-called big data technologies advance. Notwithstanding the impulse that the EU is placing on e-health and cross-border cooperation, e-health systems are developing primarily at the domestic level. In this article, we will seek to review and compare different e-health platforms now operating under the public health system of a EU member state, Portugal, with a specific focus on how the legal protection of personal data is being configured for each of them. Given the growing importance of big data in the field of health, we extend our comparative endeavour to this emerging phenomenon.

KARGER

E-Mail karger@karger.com
www.karger.com/pjp

Maria Eduarda Gonçalves
ISCTE – Instituto Universitário de Lisboa (ISCTE-IUL)
Av. das Forças Armadas
PT–1649-026 Lisbon (Portugal)
E-Mail maria.eduarda.goncalves@iscte.pt

"Over Troubled Water": Plataformas de E-Health e Protecção de Dados Pessoais: O Caso de Portugal

Palavras Chave
Big data · Proteção de dados · e-saúde · Plataformas de e-saúde · Dados de saúde

Resumo
No modo como os cuidados de saúde são ministrados reside um traço distintivo do nível de progresso de uma dada sociedade. A rápida implementação de serviços de e-saúde converteu-se num instrumento indispensável do progresso na prestação de serviços de saúde. Não obstante as promessas que acompanham as atuais e futuras aplicações no domínio da e-saúde, estas implicam a recolha e utilização de informação de elevado grau de sensibilidade sobre a vida pessoal e mesmo a intimidade dos pacientes, a qual, nos Estados-membros da União Europeia (UE), deve respeitar a legislação pertinente sobre a proteção de dados pessoais. Na realidade, a Diretiva 95/46/CE, Diretiva Proteção de Dados (DPD), classifica os dados de saúde como uma categoria especial de dados. A DPD sujeita o processamento de dados de saúde a uma proteção específica mais forte se comparada com a proteção conferida a dados pessoais menos sensíveis sob a forma de uma proibição que apenas pode ser exceptuada em caso de consentimento explícito dos titulares dos dados ou se esse consentimento for superado por um interesse superior contemplado pela lei. Consciente das mudanças decorrentes dos progressos tecnológicos neste domínio, a UE iniciou em 2012 o processo de revisão da DPD. O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 sobre a proteção das pessoas naturais no que respeita ao tratamento de dados pessoais e a livre circulação desses dados (Regulamento Geral de Proteção de Dados) foi publicado em maio de 2016, para entrar em vigor na Primavera de 2018. Este Regulamento revela uma preocupação ainda maior do que a DPD no que se refere à salvaguarda dos dados de saúde. No entanto, não é claro se este regime está à altura dos desafios suscitados pelo desenvolvimento tecnológico, particularmente, em face dos avanços das tecnologias de "big data". Apesar do impulso dado pela UE à cooperação internacional no domínio da e-saúde, os sistemas de saúde vêm sendo desenvolvidos antes de mais no plano nacional. Neste artigo, procuramos examinar e comparar diferentes plataformas de e-saúde que operam hoje em dia no quadro do sistema nacional de saúde de um Estado-membro da UE, Portugal, focando a atenção no modo como é configurada a proteção legal dos dados pessoais no âmbito de cada uma dessas plataformas. Dada a importância crescente das aplicações de "big data" na área da saúde, estendemos a nossa análise comparativa a este fenómeno emergente.

Introduction

Medicine 2.0, Health 2.0, or simply e-health, as the experience of applying Information and Communication Technologies (ICT) to healthcare is commonly known, embraces a wide-ranging and constantly progressing set of tools and services that include electronic health records (EHR), Internet health platforms, and Internet-based health services, dedicated social networks, websites with health content, and now big data in health.

Notwithstanding e-health's actual and promising applications, it must be acknowledged straightaway that e-health hinges on highly sensitive information on patients' personal lives and even intimacy, which, in the European Union (EU), must comply with the EU personal data protection legislation. In effect, health data have been classified as a special category of personal data by Article 8 (1) of the Directive 95/46/EC, the Data Protection Directive (DPD). The DPD subjects the processing of personal health data to a specific and strong protection in the form of a prohibition, which can only be excepted when the data subjects grant their explicit consent to the processing or if such consent is overridden by a superior interest provided by the law.

Aware of the major changes brought about by technological progresses in the ICT domain, the EU initiated in January 2012 a revision of the DPD. Eventually, Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation – GDPR) was published in May 2016, to be applicable as of spring 2018. Noticeably, the GDPR displays an even greater carefulness with the safeguard of health data than the DPD. Yet, it is unclear whether this legal reform is up to the challenge of current technological developments, particularly, as so-called big data technologies advance.

Against this background, it seems opportune to judge how the balance between personal data protection and al-

lowing data uses in the public health interest is being ensured. Notwithstanding the impulse that the EU itself is placing on e-health and cross-border cooperation in this field, e-health systems are developing primarily at the domestic level. Examining member states' e-health platforms, and the rules and procedures under which they operate may, thus, help us grasp this rapidly evolving field. In this article, we will review and compare different e-health platforms now operating under the public health system of a EU Member State, Portugal, with a specific focus on how the legal protection of personal data is being configured for each of them. This will be done against the background of pertinent EU and domestic legislation. Given the growing importance of big data in the field of health, we extend our comparative endeavour to this emerging phenomenon. We will start by introducing the notion of e-health and its overall effects on data protection.

E-Health and the Challenge of Personal Data Protection

E-health is broadly understood as tools and services using ICT, which can improve prevention, diagnosis, treatment, and monitoring of people's health. E-health is also seen as a critical means to deal with today's challenges of the management of the health systems. Admittedly, this objective can be accomplished while enabling patients to play a more active role in the handling of their health through easier access to information and data sharing with health service providers, health professionals, and health information networks [1].

The adoption of EHR represents one of the inescapable features of healthcare computerisation, being pushed forward by governments, namely in the EU and in the USA [2]. The EU Article 29 Data Protection Working Party (Art. 29 DPWP) defined EHR as a "comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form and providing for ready availability of these data for medical treatment and other closely related purposes" [3].

Meant to promote access to healthcare across the EU member states by enhancing cooperation among their healthcare services, Directive 2011/24/EU on the application of patients' rights in cross-border healthcare has had the effect of backing the implementation of e-health systems [4].

Speaking of e-health, Internet health platforms and Internet-based health services also deserve consideration. In fact, going online to look for health information is a common practice these days. According to a Pew Research Centre's Internet and American Life Project report, 72% (1 in 3) of Internet users have gone online to look for health information [5]. Users currently access the Internet not only to search for health information, but also to look for and connect with other patients suffering from the same medical conditions [6]. The increasing influence of social networks is being felt in healthcare and that is also partly due to physicians adhering to these new practices.

E-health also manifests itself in websites that provide various kinds of health content, like Doctissimo (www.doctissimo.fr), allowing users to make a diagnosis of their symptoms, WebMD (www.webmd.com) being probably the most famous of its kind, and platforms like Microsoft's HealthVault enabling patients to create and store individual EHR.

Altogether, this presents itself as an opportunity for health industry stakeholders to seek valuable user-generated content obtained in real time. Likewise, companies that orbit healthcare can reach out to potential clients for marketing their products and services based on profiling, a practice that we know is spreading.

Today, e-health is being furthered by so-called big data technologies as well [7]. Big data refers to the gigantic digital datasets held by large public and private organisations, first of all the main online providers (e.g., Google, Facebook, Amazon) that use automated data analysis algorithms extensively to process large amounts of data for their own commercial purposes and to sell services to third parties. Big data has been defined as "large, diverse, complex, longitudinal, and/or distributed datasets generated from instruments, sensors, Internet transactions, email, video, click streams, and/or all other digital sources available today and in the future" [8]. Under the EU's Digital Agenda for Europe, it is admitted, "Big data has the potential to play an important role in the transformation of medical care. Analysing disparate and highly dynamic data will benefit different fields like epidemiological research or early detection and prevention of diseases. By moving from a reporting approach (what has happened?) to a predictive approach (what will happen?), big data is creating a new knowledge era in the world of medical care" [9]. Even though one might say that the healthcare sector is still starting to implement this technology [10], stakeholders', whether they are companies, governments, or other organisations, are eager to take full advantage of the potential of big data [11]. As a matter of fact, as health records, medical tests, prescribed medica-

tion, or genetic information are aggregated and interconnected, new opportunities unveil themselves to decode the probability of an epidemic propagation, the health patterns of a certain country or region or even a treatment for a yet untreatable disease, bringing key intelligence to medical research [12]. Until recently, Google Flu Trends provided a telling case of the application of big data technologies to health, as Google took the information from its own search engine's queries, allowing it to monitor where (from the 29 countries involved in the project) more searches for influenza-related keywords have been made, thus inferring whether there would be a higher flu activity in a certain location. Google claimed to have tracked the outbreak of seasonal flu before the US Centres for Disease Control and Prevention because people started using the company's search engine to look up symptoms [13]. A recent illustration of the efficacy of this methodology concerned the 2014 Ebola virus outbreak in West Africa. Digital surveillance channels detected reports of the emerging outbreak in advance of official reports [14].

In the medical domain specifically, another emerging development relates to devices to be applied on the individuals' skin so as to collect and measure temperature, blood pressure, and the quality of sleeping, among other information. These breakthroughs have been referred to as Medicine 3.0, telling examples being the watch Oxitone, which evaluates the level of oxygen in the blood and cardiac frequencies and emits alerts in critical situations, and the "intelligent" T-shirts developed by OMsignal, which transmit information relating to the pulse and breathing [15, 16]. Through such devices a continuous monitoring of the physiological condition of the individual could be carried out, leading to a hyperindividualisation of healthcare or "personalised medicine" [12].

Hence the medicine of the 21st century is becoming more and more a science of information, a "médecine des données" [17].

As pointed out already, personal health data feature a particularly sensitive category of personal data, which has deserved specific consideration from personal data protection laws [18]. A European Court of Human Rights' decision, dating back to February 1997 (case of Z v. Finland), addressed health data protection's underlying motivation by saying that "respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties" to the European Convention of Human Rights, "crucial not only to respect the sense of privacy of a patient but also to preserve his/her confidence in the medical profession and in the health services in general." The European Court also affirmed, "domestic law must therefore afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the European Convention of Human Rights," and, mutatis mutandis, Articles 3, No. 2 (c), 5, 6, and 9 of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [19].

The right to privacy, like other fundamental rights, shall not be interfered by a public authority according to the European Convention, "except such as is in accordance with the law" and "necessary in a democratic society in the interests of national security, public safety, or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" (Article 8, No. 2). Restrictions to this right need to be duly justified as being necessary and proportional to the objectives of the public interest pursued.

While ultimately aiming at defending privacy, the EU data protection regime grew as a special set of principles and rights to be observed by data controllers and processors. Indeed, while Article 1 of Directive 95/46/EC makes explicit reference to the right to privacy as an objective of the data protection regime, this reference disappeared in Regulation 2016/679. According to the DPD, basic data protection principles are purpose limitation (i.e., personal data may only be collected for specified, explicit, and legitimate purposes and may not be further processed in a way incompatible with those purposes); data minimisation (i.e., processing of personal data must be restricted to the minimum necessary); proportionality (i.e., personal data must be adequate, relevant, and not excessive in relation to the purposes for which they are collected); and control (i.e., supervision of processing must be ensured by data protection authorities). In addition, the data subjects are assigned a set of procedural rights enabling them to consent, to have access, and to know what information about them is registered in databases, to rectify the data, and to object to data processing in specific situations.

Yet, the DPD, and now the GDPR, include a catalogue of exceptions to the data protection principles largely justified by the legislation's intent not to raise unjustified obstacles to the free movement of the data, a rather ambiguous notion [20], which we can, nonetheless, interpret generally as data uses for the benefit of the economy or of administrations. This is especially clear in the case of the principle of consent. Article 7 (b) to (f) DPD ultimately allowed the processing of personal data on almost any

ground, a door opened by exceptions provided by law to the "legitimate interests pursued by the controller." This criterion is re-proposed by the GDPR. According to Article 6 GDPR, personal data may be processed only if the data subject has given his/her consent to the processing of his/her personal data, or processing is necessary for the performance of a contract to which the data subject is party, for compliance with a legal obligation to which the controller is subject, if processing is necessary in order to protect the vital interests of the data subject or of another natural person, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject. The only criterion offered for assessing the legitimacy of such interests is a balance between them and the "interests and fundamental rights and freedoms" of the data subject, which is quite an evasive criterion [21, 22].

E-Health and Personal Data Protection: An Evolving Regime

It is worth recalling that the DPD was designed having in mind the computer systems of public or private organisations to the extent that they collect, store, and process personal data for the purposes of their own activities. Although drawn up in an age where the Internet was already known among the technology community and was starting to make its way into households, the DPD did not depict a special concern regarding the use of the Web, although some extensive interpretation has been done throughout the years in order to accommodate the special features of the online environment. In 2003, a decision by the European Court of Justice (ECJ) in the Bodil Lindqvist case helped to clarify the applicability of Directive 95/46/EC to the Internet in the specific circumstances in which someone processes and diffuses sensitive personal data, namely health data, of other people on an Internet page. In this instance, the Court considered that the publication of personal data online made the said information available to a countless number of recipients, thus rendering the personal/household exemption prescribed by the article 3 (2) of the DPD not applicable [23, 24].

Thus, it is not hard to deduce that the increasing amount of sophisticated content and services that emerged meanwhile rendered the said inability more obvious these days. In its Communication on a comprehensive approach to the protection of personal data in the EU, the European Commission acknowledged the problems raised by the current easiness with which personal data are shared and publicised in social networks together with the increasing capacities for information retrieval in remote servers in the "cloud" [25]. This recognition led to the proposal for the GDPR, submitted in January 2012.

Strikingly, the atmosphere surrounding the launching of this proposal looked rather optimistic. The European Data Protection Supervisor (EDPS) welcomed the proposal as a huge step forward for data protection in Europe, robust enough to face future information technology-driven challenges [26]. Likewise, for Art. 29 DPWP, the proposed regulation retained and strengthened the core principles of data protection, reinforced the position of the data subjects, enhanced the responsibility of data controllers, and strengthened the position of supervisory authorities [27]. Several commentators also saluted the draft regulation for allegedly providing data subjects with stronger rights and giving more power to customers of online services [28, 29]. Oddly, these stances revealed a somehow perplexing neglect of the challenges arising for personal data protection from the growing availability of e-platforms and large datasets as well as sophisticated tools in data mining and data analytics, and the "totalising surveillance" that accompanies large-scale processes of strategic management relying on big data [30, 31].

As pointed out, health data have been classified by the DPD as a special category of data, ruled by a prohibition, which can only be excepted when the data subjects grant their consent to the processing or if such consent is overridden by a superior interest provided by the law. The DPD's definition of health data is to be perceived as encompassing a strong connection with the health condition of an individual, namely the information on the medication prescribed or consumption habits, as well as any other information (e.g., the patient's social security number) in the medical file of a patient, which are to be assumed as being sensitive [3].

This requirement of the explicitness of consent is related to the sensitivity of the data in question. This, of course, deems any opt-out solutions as unfit for health data processing standards. As far as acquiring consent in the health data context goes, according to Art. 29 DPWP, it must be narrowed to cases where the patient actually has a genuine free choice and is, therefore, able to withdraw his/her consent at any time. Consequently, there will be no need to seek further legitimation in cases when, as a necessary consequence of the patient's clinical condi-

tion, the health professional has to process health data through an EHR platform [3, 32].

Following from Directive 95/46/EC, Regulation 2016/679 safeguards the existence of derogations to the prohibition on processing sensitive categories of data where grounds of public interest so justify, specifically for health purposes, including public health and social protection and the management of healthcare services (Art. 9; Recital 52, GDPR). Noticeably, a comparison between the DPD and the GDPR signals the EU legislator's intent to afford a higher degree of legal protection to health data, hence making the balance between data uses and personal data protection lean to the latter [33].

Actually, in contrast with the DPD, the GDPR includes detailed definitions of "personal data concerning health" (Art. 4, No. 15, and Recital 35), and of "public health" (Recital 54). "Data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his/her health status. A long, even if non-exhaustive list of personal data concerning health is provided under Recital 35 whereby it "should include" all data pertaining to the health status of a data subject which reveal information relating to the past, current, or future physical or mental health status of the data subject; a number, symbol, or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source.

In turn, "public health" is defined as "all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality" (Recital 54).

Article 9, No. 2 (h), GDPR, following up from Article 8, No. 3, DPD, addresses the processing of personal data for purposes such as preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, asserting that processing should be carried out by a health professional or another person under the obligation of professional secrecy. Additional motives of public interest such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, and social protection, and to guarantee the quality and cost-effectiveness of the procedures used for settling claims for benefits and services, may, according to the Regulation, justify data processing provided that the latter is undertaken by a person bound by a confidentiality obligation as well (Article 9, No. 2 [i]).

A few additional novelties in the GDPR may have a bearing on e-health. In particular, Article 35 introduces the obligation of controllers and processors to carry out a data protection impact assessment prior to "risky processing operations," meaning data processing presenting "high risks" such as those involving sensitive information including data concerning health.

Remarkably, whilst the EU is thereby toughening the duties of data controllers and processors, it is concomitantly encouraging the transfer of health data as far as that is needed to provide cross-border healthcare. The aforementioned Directive 2011/24/EU aims to facilitate cooperation and the exchange of information among member states working within a network connecting national authorities responsible for e-health; in so doing the Directive draws a non-exhaustive list of data to be included in patients' summaries to be shared, while encouraging effective methods for enabling the use of medical information for public health and for research (Article 14[2][b][i]). At the end of the day, this Directive follows the trail of the DPD, and now the Regulation too, whose goal is to further the free flow of personal data, while keeping with data protection standards. Eventually, this renders the balance between data protection and data uses even more problematic.

E-Health Platforms in Portugal: Seeking Compliance with Data Protection Laws in an Uncertain Environment

Like in other EU member countries, computerisation of patients' health records has developed in the Portuguese health system since the 1990s alongside a general conviction about the inherent benefits. Decree Law 308/93, 2 September 1993, established the Instituto de Gestão Informática e Financeira da Saúde (Institute for the Computer and Financial Management of Health), which launched the computerisation of the public health sector.

Following the European Commission's initiative on a European E-Health Area, the National Commission for Data Protection (CNPD), in its 2004 inspection report on health information processing in hospitals, recommend-

ed that the Ministry of Health establish EHR as a priority [34, 35]. Numerous advantages were pointed out in that respect, from greater efficiency in health management and preventing healthcare budget deficits to improved services to the patients, based on better-quality information, and from greater administrative control, with EHR offering the required data for enhanced quality control, statistical analysis and planning in the public health care sector, to safer data protection.

Potential risks associated with EHR have been admitted, however, including those entailed by the huge quantity of the data aggregated, the greater pressure for the economic use of the data, specifically by third parties linked to pharmaceutical or insurance companies and law enforcement agencies, the delocalisation of data centres, and the ensuing security issues, all of this boosting any risk scenarios previously equated. Indeed, the simple fact that these records are now available through the Internet, thus being reachable through multiple access points increases the possibilities of health data being intercepted. Art. 29 DPWP is, thus, adamant in considering the challenges brought about by EHR platforms as unprecedented, rendering the processing of sensitive information more intricate, possibly more vulnerable to unauthorised actors and having harmful consequences for the patients' rights [3].

So, in view of the impact of these developments on patients' rights to data protection and to privacy, it is important to consider the rules and practices under which the e-health platforms are operating. The doubt aired by some commentators that health data confidentiality is gradually becoming more of a thing of the past should be taken into account, it being important to stress, following the opinion of Art. 29 DPWP on this matter that all data contained in medical documentation, in EHR, and in EHR systems should be considered to be "sensitive personal data" [3].

In Portugal, Law 67/98, which transposed Directive 95/46/EC to the domestic legal order, and Law 12/2005, which defines the statute and the regime of personal genetic and health information, form the main legal framework of health data today. Law 12/2005 defines personal health information as any kind of information directly or indirectly related to health, present or future, of a person, whether alive or dead, as well as his or her medical and family history (Art. 2). This extensive definition, in line with EU law, is reinforced by the recognition of the data subjects' right to property on their health data (Article 3, No. 1, Law 12/2005), caregivers being relegated to the role of guardians of health data, obliged to use the data for health care or medical research purposes only, a ruling that is in line with the purpose limitation principle prescribed by the DPD and by Law 67/98. The question remains, though, whether a right to property is actually well matched to data uses in the contemporary information age and the loss of effective control by the data subjects of their personal data.

Lastly, a reference should be made to Law 52/2014, transposing the aforementioned Directive 2011/24/EU, establishing rules to facilitate access to cross-border healthcare so as to ensure patient mobility and promote cooperation between EU member states.

Against this background, we will examine the main features and related data protection challenges of e-health platforms now operating under the public health system in Portugal, namely the Health Data Platform and Health 24, before addressing the prospect of related big data applications.

The Health Data Platform

Let us start with the Health Data Platform (Plataforma de Dados de Saúde [PDS]), launched in 2012. The PDS is an online service under the Portuguese Ministry of Health and its shared services (Serviços Partilhados do Ministério da Saúde, EPE [hereafter, SPMS]), which is registered as the data controller [36]. The PDS comprises four interfaces, namely Portal dos Profissionais da Saúde (PDS-PP; Healthcare Professionals' Gateway) [37]; Portal do Utente (PDS-PU; Patient's Gateway) [38]; Portal Institucional (PDS-PI; Institutional Gateway), which allows the extraction of anonymous data for statistical purposes from Portal dos Profissionais de Saúde, for the establishment of a repository of anonymous clinical information; and Portal Internacional (PDS-epSOS; International Gateway) [39]. Overall, the PDS is a tool for interconnecting healthcare providers of the National Health Service (NHS), facilitating their access to patients' health information [40], as well as the sharing of information between health professionals, healthcare services, and the patients themselves. It seeks to improve the quality and the efficiency of healthcare services provided by the NHS entities, while conferring more autonomy to the users in the monitoring and management of their health [41].

As its designation suggests, the Portal dos Profissionais de Saúde (PDS-PP) is meant for healthcare professionals solely, with a wide range of participants in the field being listed, from doctors to administrative personnel, as being allowed to make use of the PDS-PP-featured services. Specifically, health professionals may have access through this portal to the patients' summaries. In turn,

the Portal do Utente (PDS-PU) is designed for the patients, enabling them to have access to a range of online services, to monitor their health data in the platform, and to communicate with healthcare professionals and healthcare facilities. Patients may thus check the information in their patient summaries, contribute to their record with, for example, their eating habits and usual medication, or identify emergency contacts. However, not all the information presented in the Patient Summary is accessible to the patient, as it is up to the healthcare professional to decide which information is made available, so as to prevent that knowing some of the facts may cause harm to the patient who may not be able to deal with his/her condition [42]. The Portal Institucional (PDS-PI) was introduced essentially as a "business intelligence" platform, i.e., a repository of anonymised clinical information meant for the healthcare institutions, the regional health administrations, and the Directorate General of Health, to provide an auditing tool [43]. Lastly, the Portal Internacional, also known as PDS-epSOS, having taken the form of a large-scale pilot project, has reached its conclusion in June 2014 with very satisfactory results, according to its management team [44]. epSOS's main goal was to establish an e-health based infrastructure, which through the wonders of ICT would connect various European healthcare systems, calling also on the cooperation among national data protection authorities [45]. Thus, starting as a project intended to develop and evaluate cross-border e-health services, it has aimed at promoting quality provision of care, namely through carrying out secure services allowing the exchange of patient summary data and electronic prescribing of medicine (ePrescription, not available in Portugal) among European countries. This feature of security was translated into the "two-step-consent" mechanism, recommended by Art. 29 DPWP, in which consent must have been given in two distinct moments, namely when first taking part in the epSOS programme and later on when the patient was actually requiring medical treatment [45].

The commitment to this project goes along Directive 2011/24/EU, rendering the implementation of cross-border e-health services a priority among EU countries [44]. Indeed, through this platform, registered health professionals had access to a patient's health record if he/she was a national of one of the 25 European countries that had joined the epSOS programme. With the conclusion of the programme, a number of subsequent initiatives has been launched, namely the EXPAND project (Expanding Health Data Interoperability Services), which is coordinated in Portugal by the SPMS.

An overview of the terms and conditions of the aforementioned four interfaces of the PDS reveals an overall, explicit concern with data protection. Hence, only registered users may have access to the platforms by the means of a login and a password, while non-registered users can only access general information in the platforms and in the Portal da Saúde (Health Portal) [46]. There are areas in the gateway where users need to offer their personal data or data relating to their entities for the corresponding services to be provided. Some personal data must be provided for the Health Ministry to offer the service. In each case, the gateway's users will be informed on the compulsory nature of the data required through specific instructions for the fulfilment of each field, the Ministry assuming that the data collected have been inserted by the data subject and the insertion has been consented by him/her, and that they are true and exact.

In addition, a number of functionalities are available to patients to limit access by third parties to their personal health data, for instance, to certain health professionals, as well as to check who has consulted information about them in the PDS and when. In turn, health professionals are due to separate patients' identifying information from the rest of his/her health information by the means of a secure encryption system [47]. Moreover, following the consultation of the clinical information of a patient, his/her information is rendered unavailable from the PDS, requiring the health professional to repeat the process in order to have access to it again [47, 48].

Relevant information about compliance of the PDS with data protection legislation comes out from the CNPD's Authorisation, emitted in conformity with Law 67/98 [47]. The CNPD recognised the public interest pursued by the PDS as a legitimate interest, specifically backing good clinical practice, guaranteeing patients' safety, and reducing costs, with a close connection with the management of healthcare services related to provision of healthcare, as prescribed by Art. 7, No. 4, of Law 67/98. Consequently, the CNPD formally authorised the PDS, although under certain conditions. For instance, the CNPD did not consider it admissible that the user's opposition disallowing health professionals from sharing user's personal data, through the PDS, expires in 12 months, as initially projected by the SPMS [47]. Indeed, the CNPD chose not to rely on the legitimate interest exception to authorise the PDS wholly. Accordingly, the processing of the patients' data under the PDS-PU must rely on the patient's explicit, informed, and specific consent, relating to a concrete factual context and precise operation (Art. 7, No. 2, of Law 67/98) [47]. According to

Art. 29 DPWP, for consent to be deemed specific as the processing of health data requires, it has to fully encompass a thoroughly defined situation, prescribed in specific consent clauses and not lost amid other more general terms of any agreement, which may jeopardise a full understanding of the processing in question [48]. Also, the information retrieved should be reduced to the "minimum essential," in line with the data minimisation principle [47].

Meeting another recommendation of the CNPD, the PDS's terms and conditions now render explicit that personal health data may be communicated to third parties only whenever the data subjects have unequivocally given their consent; if it is required by a legal obligation, a deliberation of the CNPD, or a judicial order; or if vital interests of users or another legitimate purpose prescribed by the law are at stake [49, 50]. In all these circumstances, the user of the platform, i.e., the data subject, must be duly informed including on the identity of the receivers of the data and the purpose of the data processing.

Doubts were, however, raised as to how the data protection rules are observed in practice. The CNPD expressed its concern with the supposedly careless routines of health professionals regarding the use of their credentials for access to the platforms, while recommending that healthcare professionals be called upon to adopt a more cautious behaviour, and urging a standardised model for authentication to be adopted [47]. Strikingly, in view of the emergent nature of such procedures, the CNPD stressed the importance of introducing prior impact assessments regarding the processing of health data as well as privacy-by-design initiatives from the PDS platforms' inception, which are also being heavily endorsed by Art. 29 DPWP [3].

Health 24

Health 24 ("Saúde 24") is a clinical service sponsored by the Portuguese Ministry of Health, launched in 2007. Operated by trained nurses, it offers individuals the opportunity to address their health concerns through a 24/7 helpline in both Portuguese and English.

The Health 24 helpline comprises various services including triage, counselling, and forwarding of patients who are in need of medical assistance, therapeutic advising regarding medication, and assistance in public health issues, as well as general information regarding health, namely where the near healthcare facilities or pharmacies can be found [51]. Most often, Health 24's operation consists of a phone call received by a nurse operating the helpline who, according to the information conveyed by the patient, selects the symptoms it relates to in the software provided. These pre-selected symptoms available in the software, along with any notes they may find suitable, help the nurses describe the patient's clinical condition as accurately as possible. If the situation does require going to the emergency room, this information is then converted into an algorithm sent to the nearest hospital by fax machine. The hospital will benefit from a head start to put the appropriate protocols in motion so as to be ready to receive the patient by the time he/she arrives to the healthcare facilities.

Though widely acclaimed, the implementation of this service raised concerns regarding the ways in which the users'/patients' data are collected and handled. In an Authorisation emitted in 2007, while highlighting these concerns and issuing guidelines concerning the data processing by Health 24, the CNPD permitted the private company in charge of the personal data processing to operate the service [52]. The Authorisation specified that identification should not be required whenever the patient seeks only general information [52].

In 2015, a new Authorisation was issued due to the transfer of Health 24's management to a different entity, a consortium of three companies: LCS – Linha de Cuidados de Saúde, S.A., Optimus, S.A., and Teleperformance, S.A. [53]. According to this Authorisation, the data may be collected from both the users of Health 24 and the National Registration of NHS users (Registo Nacional do Utente do SNS). But, as acknowledged by the CNPD, none of the information gathered by Health 24 is added to the patient's EHR [53].

Yet, in the end, Health 24's service was not recognised by the CNPD as involving the execution of medical deeds, since it does not involve a feat related to the purposes of "preventive medicine, medical diagnosis or the provision of care," which could justify a legitimate interest replacing the data subject's consent, pursuant to Law 67/98 (Art. 7, No. 4). The CNPD noted that, even though Health 24 may feature the "management of healthcare services," this would need to be closely connected with medical purposes, which did not occur in the CNPD's view. Therefore, the Commission concluded that no legitimate interest for the data to be processed by Health 24 could be invoked, entailing the requirement that the patient must give a free, unequivocal, express, and informed consent for the data processing to take place. The CNPD's refusal to recognise the legitimate interest exception to Health 24 may then be due to its intent to strengthen the requisite of consent, which otherwise would not need to be explicit for the processing of health data.

Likewise, Art. 29 DPWP has taken a cautious approach as to the scope of Article 8 (3) of the DPD on the exemption from the general prohibition to process sensitive data based on the legitimate interest of the processor. According to the Working Party, this exemption must be interpreted in a restrictive way. Specifically, the Working Party considers that Article 8 (3) could only pertain to the processing of medical data for strictly those medical and healthcare purposes mentioned therein, and under the conditions that processing is "required" and done by a health professional or by another person subject to an obligation of professional or equivalent secrecy. Where the processing of personal data in an EHR goes in any way beyond these purposes or does not meet the said conditions (as is indeed the case for Health 24), then Article 8 (3) cannot serve as the sole legal basis for the processing of that personal data [3].

Eventually, Health 24 may be regarded as essentially an information service involving the processing of health data collected by phone, and what is more, in presumably more vulnerable conditions than similar data revealed by patients at hospitals or other healthcare facilities. This may ultimately elucidate the reinforced protection granted to this platform as far as consent goes.

Furthermore, while Authorisation 631/2007 foresaw a distinction between the handling of health data and of other categories of less sensitive personal data relating to a patient, Authorisation 2/2015 does not refer to this distinction. Indeed, following the initial Authorisation, only healthcare professionals (the nurses) could have access to the health data whereas non-clinical staff could only access the patients' contacts. Authorisation 2/2015 does not clarify whether this differentiation remains. As a matter of fact, according to Law 67/98, the processing of health data may be carried out either by health professionals, or "by another person also subject to an equivalent obligation of secrecy." So, even though all Health 24 staff must sign a non-disclosure agreement, there seems to be the need to clarify what kinds of personal data the Health 24's staff other than the nurses may effectively handle. Art. 29 DPWP endorsed this extra layer of caution regarding the access of non-clinical staff to health data, stressing the need for non-medical personnel to be subject to the same binding rules of healthcare professionals, ensuring an equal level of confidentiality, and ensuring that the data will be used strictly for the purposes of healthcare. Even so, the Working Party fears that EHR may still remain exposed, despite the obligation of secrecy, calling for "additional and possibly new safeguards." Hence, there is a call for the development of a secure identification and authentication system, which also reveals the role in which the healthcare professional is using the platform, for instance as a general practitioner or as a nurse [3].

E-Health and Big Data

As pointed out, e-health is entering the big data age. In the context of the present analysis, a pertinent issue is whether public health institutions are by now resorting to big data products or services or whether they plan to do it, and, if so, under what consideration for the data protection legal framework.

Big data depends on the aggregation of multiple data drawn from different sources, from search engines and social networks to smart phones and geo-location devices. Characteristically, big data products and services rely on a secondary use of data, including personal data collected initially for other purposes, possibly colliding with the data protection purpose limitation principle.

A telling example is Google Trends, one of the many services developed by Google Inc. based on the monitoring of Google users' searches so as to establish patterns. In Google's words, "Google Trends analyses a percentage of Google web searches to determine how many searches have been done for the terms you've entered compared to the total number of Google searches done during that time" [54]. In order to accomplish this, Google relies on the 4 million search queries it receives and processes every minute coming from every part of the world and in several different languages [55].

An application of this service in the field of health was, until recently, Google Flu Trends, offering regularly updated estimates on the flu activity around the world. So, if one sought for flu, one was able to see when this keyword was more often searched for, in what region of the world, country or city and even what were the most common searches related to flu [56].

All of this, of course, is carried out with the indispensable contribution of the users who, often unknowingly, are enriching Google's databases, so this information can afterwards be made publicly available and integrated into the Google Trends platform. Despite the usefulness they may bring, these practices raise doubts about the intrusiveness of the methods used by Google to collect and analyse the data. Thus, in order to obtain some clarification regarding Google's practices and their compliance with the data protection laws, it is important to go through the company's privacy policy.

First and foremost, it should be noted that Google adopts a privacy policy for all of its more than 150 different services, so Google Trends is guided by its controver-

sial "universal" privacy policy [57, 58]. If, on the one hand, it is no secret that the very operability of Google Trends relies on the collection of data from users, on the other hand, this should not serve as an excuse for an unlimited collection of data, namely as far as methodology, purpose, and retention period go. In reality, these data can be, and indeed are, crossed with all of the other data collected from the various Google services even though Google denies ever doing that when it comes to the information collected for Google Trends [59].

Google uses most of the data that it collects to proceed to target advertising practices more accurately to users and its privacy policy is actually clear about that goal [60]. Thus, besides the information users provide in order to create a "Google Account" (such as name, gender, date of birth, country of residence, and, optionally, address, phone number and credit card information), Google collects other information from the use made of their services such as device information; log information (details of how individuals use their services, including search queries, phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information, and types of calls); IP address, crashes that users' device may experience, system activity, hardware settings, browser type, browser language, as well as the date and time of the activity; location information; operating system identifying information, information collected from users' own computers, as well as information stored there by Google itself (such as application data cache and information stored in a web browser for future easier access), and, last but not least, the infamous cookies stored in users' devices whenever they use a company's service or the service of a third party associated with Google and which are often almost "mandatory" to allow if we want to use a certain service. Google makes use of all this information so as to "provide, maintain, protect and improve them, to develop new ones and to protect Google and our (their) users" [60]. Google also states that this information is collected in order to offer "tailored content" to users, namely granting them with search results and ads that may have better appeal individually.

Google does provide a right of access to users, who can proceed to any corrections or even eliminate their Google Accounts, in cases where the information is incorrect. Yet, Google alerts for the possibility of being able to refuse any request that may involve "disproportionate technical effort" or be "extremely impractical" [60].

Moreover, Google foresees in its privacy policy the possibility of sharing personal information collected from users with companies, organisations, or individuals external to Google, unless they are not able to obtain users' consent, which, in the end, is often implied in the use of the services, rendering it a moot requirement.

Focusing on Google Trends' operability in the health domain, its first public appraisal came from an article sponsored by Google itself entitled "Detecting Influenza Epidemics Using Search Engine Query Data," in which it is explained that an early method of detecting disease activity is through analysing search queries showing health seeking behaviour [59]. This article clarifies that none of the queries in Google's database can be associated with a particular user, as it does not keep any information regarding identity, IP address, or location.

While operating in EU territory, Google must, of course, follow the EU data protection laws, namely Directive 95/46/EC. However, in a report prepared following a thorough investigation by the French data protection authority (Commission Nationale de l'Informatique et des Libertés – CNIL), which was mandated by Art. 29 DPWP, CNIL's experts denounced that Google did not respect key data protection principles, specifically the principle of purpose limitation, data minimisation, and the right to object. Indeed, the experts stressed that Google's "inaccuracies" throughout the terms of its privacy policy do not allow for a user to discern which type of personal information is being collected for a given service or the purpose that collection serves. This meant that the privacy policy makes no distinction between innocuous content such as search queries used to fuel Google Trends and the telephone information, for instance, being that, under this policy, all of them can be used in the same way for every purpose displayed in the text [61]. This issue deepens when we consider the fact that Google, as stated in its privacy policy, does combine information gathered through its various services, resulting in a very broad combination, including the activity of every user not only on Google services but also on associated third parties [11].

Even though Google has performed a few changes in its privacy policy (the last one dating 19 August 2015), it still has not responded to the majority of the questions raised by the EU data protection authorities. Were these web search logs not supposed to be anonymous from the start as Google also claims in the article it sponsored? It is a question yet to be answered, one that Google dodges in its privacy policy.

Another shortcoming, which may be worth underlining in Google's privacy policy, is the absence of a more thorough explanation regarding Google Trends operabil-

ity. Indeed, it seems rather bewildering that the only place we are able to find some dedicated information about this platform is on the aforementioned Google-sponsored article (which, by now, may not even be up to date), since the company's policy, being "universal", has clearly decided not to individualise any of its services. Nevertheless, we believe a direct mention would be worth the exception, especially if we consider that many of the search queries on which the platform relies may, in fact, entail an indication of sensitive information, namely a clinical condition that a user may be experiencing, rendering it all the more relevant to know the specific circumstances comprising the storage period and the actual anonymisation of this information.

Addressing big data applications generally, Art. 29 DPWP described the immediate risks surrounding their implementation focusing on the vast amount of data collected from multiple sources, enabling tracking and profiling of users on a whole new level; the security issues raised by this intensive gathering of data, which are being stored and used without adequate protection; the lack of transparency due to the insufficient information conveyed to the subjects rendering them no awareness or control over what is being done to their information; and the dangers of reaching inaccurate results or profiles and that the information is used with discriminatory intent [62]. All these problems need to be duly taken into account once public health entities and services start considering the reuse of personal data either from large big data operators such as Google or from their own e-health platforms and databases.

In Portugal, the SPMS, as the central manager and controller of the shared information system of the Ministry of Health, is presently anticipating the potential utilities of the secondary uses of the SPMS's databases, with emphasis being placed on research and epidemiological ends [63]. But the current lack of a clear legal framework for personal health data to be transmitted to third parties interested in exploring the data is regarded as a strong drawback, hindering potentially valuable uses of the huge repository of health data collected and stored under the SPMS and other e-health platforms and databases [63]. A clarification of the status of health data in that context then appears to be required, including on whether it should still be regarded as the property of the data subject following Law 12/2005, once converted into "reusable," even if anonymous, data, and what the implications should be. By the same token, reassessing the position of the data subjects vis-à-vis the reuse of their personal data for public health purposes exclusively, provided that appropriate safeguards are ensured, may be well timed [64]. Most likely, these are topics for the CNPD and even for the Portuguese legislator to tackle in due time.

Conclusion

No doubt, e-health platforms, as part of the continuously developing computerisation of health systems, represent a progressive move towards greater efficiency and quality of healthcare. Following the general trend, in Portugal, the Health Data Platform (PDS) has been instituted as a tool for easier and broader intercommunication and information sharing by healthcare professionals of the NHS, as well as among professionals and patients. In turn, Health 24 also brings about aids to both patients and healthcare providers as it puts health information at the patients' disposal, while dismissing unnecessary flooding of emergency rooms whenever a patient may not require emergency treatment.

As underlined, since they all deal with sensitive data, the e-health platforms must comply with the data protection regime in force. Our overview of current e-health platforms in Portugal denotes that, notwithstanding the platforms' different scopes and aims, an overall concern with the protection of the personal health data is manifest, as the supervisory role by the CNDP itself indicates. Consent by the data subjects, together with their autonomy in the access and management of personal information, surfaces as key grounds for the platforms' legitimacy. Nonetheless, the variation in the range and objectives of the platforms analysed may explain the changing ways in which the balance between the requirement of consent and consideration of the legitimate interest of the operator is worked out. Noticeably, the closer the platform's function is to medical practice and to the management of healthcare, the easier the recognition of its legitimacy to collect and process the data. Accordingly, the acknowledgment by the CNPD of the PDS's legitimate interest to collect and process personal data (with respect to the Professionals' Health's Gateway) allows for forms of implicit consent, in contrast with the stricter consent requirements of the PDS's Patient's Gateway, and, even more, of Health 24. In the case of Health 24, its configuration as essentially an information service may account for the CNPD's stringency in the application of the principle of consent.

Besides, the firmer confidentiality duties imposed on the health professionals working for the NHS, hence for the PDS, may also justify the relative suppleness of the

PDS's data protection regime when compared with Health 24. As acknowledged by the CNPD, it is important to ensure that clinical and non-clinical members of staff do not have the same level of clearance, as health data are in principle reserved for access to health professionals. In this regard, Art. 29 DPWP has actually gone as far as proposing a "modular access rights" system comprehending different categories of healthcare professionals and institutions, which would have limited access to some sets of health data, depending on their role in the patient's treatment [3]. Nevertheless, from our analysis of Health 24's terms of reference, no evidence has emerged on the basis of which Health 24's staff may have access to patients' health data, from technicians to nurses and administrative personnel. This should be fully clarified so as to ensure that patients' data are stored safely and solely at the disposal of those who should have access to them. Even though Authorisation 2/2015 rendered this issue hazier by not even addressing it, considering the principle of transparency, users should be enlightened about the processing their data undergo. Knowing who handles the health data is an absolute requisite for transparency and the right to information to be guaranteed, even assuming that every member of the staff has signed a non-disclosure agreement.

Against this background, the PDS can actually work as a model as the data controller has been careful enough to explain to users how the data processing works, which categories of data are collected, who can access them and for what purposes, having in mind privacy and data protection norms.

Compared to these e-health platforms, all confined to a single state's jurisdiction, big data's current and prospective applications are considerably more challenging as far as safeguarding the data protection principles and rights is concerned. Based on the example of Google Trends, we infer that this platform offers a useful tool to perform constant monitoring of users' Google Search-enabled queries, in order to discover what the most popular topics of a given period of time are and to establish patterns. This, of course, can be applied to monitoring the activity of a given clinical condition, which may help healthcare authorities and providers identify and handle any occurrence, promoting a more rapid and efficient response.

Yet, the operation of Google Trends and of similar platforms raise concerns regarding the intrusiveness of the methods used and the conformity of the respective "privacy policies" with the EU data protection legislation. Although Google claims that users' information is collected so as to give them "tailored content," the company persistently fails to uphold the rules of the DPD regarding consent, purpose limitation, data minimisation and data retention, and even admits the possibility of sharing users' personal information with other companies, organisations, and external individuals. As noted, Art. 29 DPWP has been pressing Google to revise its policy so as to comply with the EU data protection law.

This recognition becomes especially acute as NHS, in Portugal and elsewhere, envisage relying on information collected from big data operators as part of their e-health strategies. Considering the Portuguese NHS as an illustration, it may look inconsistent that, while seeking compliance with data protection rules and procedures for e-health platforms, data starting to be increasingly gathered and reused from Google or other big data operators do not guarantee an equivalent protection. Indeed, whereas in the case of Health 24, we may be talking about mild carelessness in displaying information regarding the processing of patients' health data required to aid pursuance of the goals underlying the platform, which is to improve the quality and efficiency of the healthcare system, today, the most prominent big data services are ultimately related to the essentially commercial purposes of the operators, serving the public interest only indirectly. Still, one may wonder whether the opportunities opened up by big data for the improvement of healthcare might not justify the elaboration of a specific regime for health data reuses, one that could, likewise, encompass reuses of health data available through e-health platforms such as those addressed in this paper.

References

1 Moen A, Hackl WO, Hofdijk J, Van Gemert-Pijnen L, Ammenwerth E, Nykänen P, et al: eHealth in Europe: status and challenges. Eur J Biomed Inform 2012;8:2–7.
2 Dumortier J, Verhenneman G: Legal regulation of electronic health records: a comparative analysis of Europe and the US; in Carlisle G, Whitehouse D, Duquenoy P (eds): eHealth: Legal, Ethical and Governance Challenges. Berlin, Springer, 2013, pp 25–26.
3 Article 29 Data Protection Working Party: Working document on the processing of personal data relating to health in electronic health records (EHR) adopted on 15 February 2007. Brussels, Directorate General Justice, Freedom and Security, European Commission, 2007.
4 Directive 2011/24/EU of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare, 9 March 2011. OJEU 2011;L88:45–65.

5 Pew Research Center's Internet and American Life Project: Health Online 2013. Washington, Pew Research Centre, 2013.
6 Strauss S, Nentwich M: Social network sites, privacy and the blurring boundary between public and private spaces. Sci Public Policy 2013;40:724–732.
7 Allemand L: Les promesses du big data. La Recherche 2013;482:26–42.
8 National Science Foundation: Solicitation 12-499: Core Techniques and Technologies for Advancing Big Data Science & Engineering (BIGDATA). Arlington, National Science Foundation, 2012.
9 European Commission: Discussion Big Data and Healthcare: A New Knowledge Era in the World of Healthcare. Brussels, European Commission, 2014.
10 Shah ND, Pathak J: Why health care may finally be ready for big data. Harvard Business Review, December 3, 2014.
11 Chong R: Big predictions for big data impact on public health. Techwire's Insider, November 7, 2013.
12 Louca S: Personalized medicine: a tailored health care system: challenges and opportunities. Croat Med J 2012;53:211–213.
13 Article 29 Data Protection Working Party: Google privacy policy: main findings and recommendations. Brussels, Directorate General Justice, Freedom and Security, European Commission, 2012.
14 Anema A, Kluberg S, Wilson K, Hogg RS, Khan K, Hay SI, et al: Digital surveillance for enhanced detection and response to outbreaks. Lancet Infect Dis 2014;14:1035–1037.
15 MarkMonitor: Domain Big Data: Oxytone.com. Englewood Cliffs, MarkMonitor.com, 1999.
16 MarkMonitor: Domain Big Data: Omsignal.com. Montreal, MarkMonitor.com, 2011.
17 Sadin E: La vie algorithmique: critique de la raison numérique. Paris, Éditions L'Échappée, 2015.
18 Vayena E, Salathé M, Madoff LC, Brownstein JS: Ethical challenges of big data in public health. PLoS Comput Biol 2005;11:e1003904.
19 European Court of Human Rights: Case of Z v. Finland: Application No. 22009/93 ECHR 10. Strasbourg, European Court of Human Rights, 1997.
20 Fuster GG: The emergence of personal data protection as a fundamental right of the EU. Cham, Springer International Publishing, 2014.
21 Article 29 Data Protection Working Party: Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Brussels, Directorate General Justice, Freedom and Security, European Commission, 2007.
22 Zanfir G: Forgetting about consent: why the focus should be on "suitable safeguards"; in Gurwitch S, Leenes R, de Hert P (eds): Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges. Dordrecht, Springer, 2014, pp 237–257.
23 European Court of Justice: Case C-101/01: Bodil Lindqvist. Strasbourg, European Court of Justice, 2003.
24 Warso Z: There's more to it than data protection: fundamental rights, privacy and the personal/household exemption in the digital age. Comput Law Security Rev 2013;29:493–496.
25 European Commission: Communication of the Commission to the European Parliament, The Council, The Economics and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union. Brussels, European Commission, 2010.
26 European Data Protection Supervisor: Annual Report 2012: Smart, Sustainable, Inclusive Europe: Only with Stronger and More Effective Data Protection. Luxembourg, Publications Office of the European Union, 2013.
27 Article 29 Data Protection Working Party: Opinion 01/2012 on the Data Protection Reform Proposals. Brussels, Directorate General Justice, Freedom and Security, European Commission, 2012.
28 Hert PD, Papakonstantinou V: The proposed data protection Regulation replacing Dir 95/46/EC: a sound system for the protection of individuals. Comput Law Security Rev 2012;28:135.
29 Tene O, J Polonetsky J: Privacy in the age of big data: a time for big decisions. SRL Online 2012;64:63–69.
30 Couldry N, Powell A: Big data from the bottom up. Big Data Soc 2014;3:1–5.
31 Mantelero A, Vaciago G: The "dark side" of big data: private and public interaction in social surveillance: how data collections by private entities affect governmental social control and how the EU reform on data protection responds. CRI 2013;14:161–162.
32 Article 29 Data Protection Working Party: Opinion 15/2011 on the definition of consent. Brussels, Directorate General Justice, Freedom and Security, European Commission, 2011.
33 Iorio CTD, Carinci F: Privacy and health care information systems: where is the balance?; in Carlisle G, Whitehouse D, Duquenoy P (eds): eHealth: Legal, Ethical and Governance Challenges. Berlin, Springer, 2013, pp 85–87.
34 European Commission: Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: e-Health: making healthcare better for European citizens: an action plan for a European e-Health area. Brussels, European Commission, 2004.
35 Comissão Nacional de Protecção de Dados: Relatório de auditoria ao tratamento de informação de saúde nos hospitais. Lisbon, Comissão Nacional de Protecção de Dados, 2004.
36 Portugal: Ministério da Saúde. Plataforma de dados de saúde. Lisbon, Ministério da Saúde, 2013.
37 Portugal: Ministério da Saúde. Portal dos Profissionais de Saúde. Lisbon, Ministério da Saúde, 2016. https://www.sns.gov.pt/profissional/ (accessed January 12, 2017).
38 Portugal: Ministério da Saúde. Portal do Utente. Lisbon, Ministério da Saúde, 2016.
39 European Commission: epSOS: International Portal. Brussels, European Commission, 2016. http://www.epsos.eu/home/about-epsos.html (accessed January 12, 2017).
40 Portugal: Ministério da Saúde. Resumo clínico único do utente. Lisbon, Ministério da Saúde, 2016.
41 Anes E, Dias J, Oliveira M, Silva MG, Vasconcelos P, Rodrigues P, et al: Protecção de dados pessoais em saúde. Rev Sinais Vitais 2004; 55:15.
42 Comissão Nacional de Protecção de Dados: Autorização 3742/2012. Lisbon, Comissão Nacional de Protecção de Dados, 2012.
43 Sá PJR: Plataforma de dados de saúde: portal institucional. Dissertação de Mestrado. Porto, Instituto Superior de Engenharia, 2013. http://recipp.ipp.pt/bitstream/10400.22/6270/1/DM_PauloSa_2013_MEI.pdf (accessed January 12, 2017).
44 European Commission: EPSOS: Letter to epSOS Contributors. Brussels, European Commission, 2014.
45 Article 29 Data Protection Working Party: Working Document 01/2012 on epSOS, 25 January 2012. Brussels, Directorate General Justice, European Commission, 2012.
46 Portugal: Ministério da Saúde. Portal da Saúde. Lisbon, Ministério da Saúde, 2016.
47 Comissão Nacional de Protecção de Dados: Authorisation 3742/2012. Lisbon, Comissão Nacional de Protecção de Dados, 2012.
48 Portugal: Ministério da Saúde. Medidas de segurança do tratamento. Lisbon, Ministério da Saúde, 2016.
49 Article 29 Data Protection Working Party: Opinion 15/2011 on the Definition of Consent, 13 July 2011. Brussels, European Commission, 2011.
50 Portugal: Ministério da Saúde. Autorização de consulta de dados. Lisbon, Ministério da Saúde, 2016.
51 Portugal: Ministério da Saúde. Health 24 helpline: Health 24: "Quem Somos." Lisbon, Ministério da Saúde, 2007.
52 Comissão Nacional de Protecção de Dados: Authorisation 631/2007. Lisbon, Comissão Nacional de Protecção de Dados, 2007.
53 Comissão Nacional de Protecção de Dados: Authorisation 2/2015. Lisbon, Comissão Nacional de Protecção de Dados, 2015.
54 Google: Trends Help. Mountain View, Google, Inc., 2016.
55 Gunelius S: The data explosion in 2014 minute by minute: infographic. ACI, July 12, 2014.
56 Google: Google Flu Trends: how does this work? Mountain View, Google, Inc., 2014.
57 Google: Privacy Policy. Mountain View, Google, Inc., 2016.

58 Article 29 Data Protection Working Party: Letter Sent to Larry Page, Google Inc. CEO, 23 September 2014. Brussels, European Commission, 2014.
59 Ginsberg J, Mohebbi MH, Patel RS, Brammer L, Smolinski MS, Brilliant L: Detecting influenza epidemics using search engine query data. Nature 2009;457:1012–1014.
60 Google: Privacy Policy. Mountain View, Google, Inc., 2015.
61 Commission Nationale de l'Informatique et des Libertés: Google's New Privacy Policy: Incomplete Information and Uncontrolled Combination of Data across Services: Press Release 16 October 2012. Brussels, Commission Nationale de l'Informatique et des Libertés, 2012.
62 Article 29 Data Protection Working Party: Opinion 03/2013 on Purpose Limitation, Adopted on the 2nd April 2013. Brussels, European Commission, 2013.
63 Martins H, Soares J: Sistemas de Informação de Saúde: potencialidades do uso secundário de dados, desafios e oportunidades; in CNECV 25 anos: Conferência Comemorativa, Lisboa, 5 de Outubro de 2015. Lisbon, Conselho Nacional de Ética das Ciências da Vida (CNECV), 2015.
64 Taylor MJ: Legal bases for disclosing confidential patient information for public health: distinguishing between health protection and health improvement. Med Law Rev 2015; 23:348–374.