Cybercrime and Private Health Data:
Review, Current Developments, and Future Trends

Stavros Pitoglou
https://orcid.org/0000-0002-5309-4683
National Technical University of Athens, Greece & Computer Solutions SA, Greece

Dimitra Giannouli
Computer Solutions SA, Greece & University of Leeds, UK

Vassilia Costarides
Institute of Communication and Computer Systems (ICCS), Greece

Thelma Androutsou
National Technical University of Athens, Greece

Athanasios Anastasiou
National Technical University of Athens, Greece

INTRODUCTION

One significant benefit of the development of information technology is its positive impact on the health sector. Over the last years, the use of electronic patient records has illustrated rapid expansion. The advancements in health information technology, the limited potential of the traditional processes and the need for flexible access to health information, have promoted new paradigms and as a result, personal health record (PHR) systems, empowering both patients and healthcare providers, present a constantly evolving area for research, development, and implementation (Genitsaridi, Kondylakis, Koumakis, Marias, & Tsiknakis, 2015). The technological challenges intertwined with the increasing adoption of such tools and platforms are optimally addressed with the rise of Cloud Computing (Martens & Teuteberg, 2012) which is formally defined as *"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction"* (Mell & Grance, 2011). Promising coherence and economies of scale through the ability of robust sharing of computational resources, Cloud Computing has been a continuously evolving sector over the last decades (Guzek, Bouvry, & Talbi, 2015).

Furthermore, the availability of large medical datasets for secondary purposes such as research has become a powerful tool for producing knowledge and information, leading the medical and health care sector to a new, more personalized level. Large-scale biomedical databases are created and continuously enriched for research purposes while providing the right tools for handling and analyzing their content (Dankar & Al Ali, 2015). Researchers using personalized patient medical data have the ability to present valid and reliable data, to reuse existing data, and to compare the results of their study with similar ones based on the same database (Emam, 2013).

DOI: 10.4018/978-1-5225-9715-5.ch052

As the type of data shifts toward electronic records and large datasets are made accessible via distributed networks and the world wide web, hospitals, and other health providers increasingly suffer from data breaches whose nature likewise shifts toward electronic means, such as hacking (Spitzer, 2018). A data breach is *"an impermissible use or disclosure that compromises the security or privacy of the protected health information and is commonly caused by a malicious or criminal attack, system glitch, or human error"* (Bai, Jiang, & Flasher, 2017). Breaches can be conducted by a variety of ways, including credential-stealing malware, an insider who either purposefully or accidentally discloses patient data, or lost laptops and smart devices (Center for Internet Security, 2018).

Healthcare industry is highly targeted by cybercriminal organizations and individual hackers, as, according to research, an individual's medical data, are 20 to 50 times more valuable to cybercriminals and black market than other types of targeted information, e.g., personal financial data, credit card details, social security numbers, etc. (Center for Internet Security, 2018). Therefore, cybercriminals have higher incentives to target databases with medical content in order to sell or exploit the sensitive information for their own personal gain (Center for Internet Security, 2018). In this context, it is not a coincidence that the biggest recent data breaches have seized health care records as the prize.

Access to highly sensitive medical information which is exposed through data breaches, gives cybercriminals the opportunity to commit identity theft, medical fraud, extortion, and the ability to illegally obtain controlled substances (Kruse, Frederick, Jacobson, & Kyle, 2017). More specifically, patient records can be used for various types of financial gain, including (Boden, 2018):

- sale on the Dark Web
- fraud commitment (tax, insurance frauds)
- extortion of people whose disclosure of illness could provoke public relationships problems and difficulties in their working environment
- targeted phishing campaigns against individuals whose records were leaked

In the recent years there is an uptick in attacks against health care systems due to a variety of factors, including low organizational vigilance, inadequate and poorly trained staffing, insufficient technology investment and funding for information technology security, all these combined with the potential value of healthcare data as compared with other industries (Gordon, Fairhall, & Landman, 2017).

CURRENT TRENDS

In the past years, the growth of healthcare data breaches in both size and frequency was remarkable, with the largest breaches having an impact on millions of people (Chideya, 2015). In the years 2016-2017, approximately 90 percent of healthcare providers were faced with data breaches and cyber-attacks were up 125 percent since 2010 (Kruse et al., 2017). Currently, in the U.S., the number of individuals affected is estimated to be more than half of the total population.

A data breach outside of the USA that is worth mentioning is the Singapore Health cyberattack. The personal particulars of almost 1.5 million patients, including that of the country's Prime Minister, were stolen from the database. The data include both demographic and medication records (Singhealth et al., 2019). On the other hand, National Health Service (NHS) was on the top of the list for serious data breaches in 2014. The percent of severe data breaches that were reported to the Information Commis-