ISSN 2278-9723
DOI:10.31838/ijccts/06.01.03

Research Article

Computer Technology Applications and the Data Protection Concept

HRUNYK I.
Faculty of Informatics, Kaunas University of Technology, Kaunas, Lithuania
E-mail: Hrunykl.@gmail.com
Received: 25.10.17, Revised: 27.11.17, Accepted: 15.01.18

ABSTRACT
Personnel record protection serves the purpose of ensuring that the affected individuals' and families fundamental values are promoted, including dignity and worth, respect, individuality, and personal autonomy. Also, personnel record protection has its purpose lie in the avoidance of harm. Hence, personnel records ought to be protected because if they are disclosed to family members, insurers, or employees, they could lead to discrimination, embarrassment, and stigma. For healthcare organizations, an assurance of personnel record protection is important because it prompts personnel to provide complete and candid disclosures of sensitive data to their physicians willingly. Also, personnel record protection is important to healthcare organizations because it promotes more effective communication between personnel and physicians. The objective of this study is to examine computer technology applications, especially concerning their contemporary role in prompting the concept of data protection.
Keywords: physicians willingly, objective of this study examine computer technology data protection.

INTRODUCTION

Terry (2017) contended that the secondary benefit accruing from this assurance of privacy (at the organization level) is that there might be positive outcomes such as the prevention of discrimination, embarrassment, and economic harm, as well as enhanced autonomy and quality care. With Cohen and Mello (2018) observing that the latter beneficial effects of personnel record protection at the organization level translating into personnel satisfaction, the eventuality is that the overall reputation of an organization such as United General, upon ensuring personnel data privacy, could be boosted or remain positive – especially due to minimal complaints associated with inappropriate personnel data disclosures.

To protect personnel health records, legal requirements have been specified in the Privacy Rule, the Health Insurance Portability and Accountability Act (HIPAA). According to this federal privacy law, covered health care providers are permitted to give choices to personnel to determine whether or not their health information could be disclosed for certain key reasons, including health care operations, payment, and treatment (Riley, 2018; Cohen and Mello 2018; Turpin, 2005). Also, written consent needs to be obtained from personnel before disclosing health data to other organizations and people, including the case of disclosures that are meant for further treatment of sensitive health conditions (Terry, 2012; Lyden, 2008). Regarding the type of information that is protected, HIPAA emphasizes protected health information that covered entities and their business associates transmit or hold in media such as oral, paper, or electronic forms (Terry, 2014; Cohen and Mello 2018; Garson, 2010). According to Terry (2017), some of the demographic data that the privacy rule covers include future, present, and past health care payment records and the future, present, and past mental or physical condition or health of an individual. This case study focuses on a data privacy compromise, as well as how computer technological incorporation forms a promising solution.

METHODOLOGY/CASE DESCRIPTION

In this case, Pete compromised the personnel records belonging to Winnie. Therefore, both paper and electronic personnel records face several risks. For instance, there is a likelihood of medical identity theft whereby hackers could use Winnie's data to initiate access to her data. Also, the personnel's record is at risk of falling in the hands of cyber attackers, who could dig into the

data and seek to access crucial information such as her credit card information and security numbers, which could be deemed beneficial to them from the perspective of monetary terms. Overall, paper and electronic personnel records at the institution, due to Pete's compromise of Winnie's data, are prone to threats to security and privacy, including hacking IT incidents, data loss, improper disposal of data, unauthorized access, and data theft. Therefore, this study employed a case analysis approach to determine how computer technology could enhance data privacy, protecting personnel records.

RESULTS, DISCUSSION, AND RECOMMENDATIONS

Table 1. Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)

	2017	2018	2019	2020	2021
Cloud Business Process Services (BPaaS)	42.2	46.6	50.3	54.1	58.1
Cloud Application Infrastructure Services (PaaS)	11.9	15.2	18.8	23.0	27.7
Cloud Application Services (SaaS)	58.8	72.2	85.1	98.9	113.1
Cloud Management and Security Services	8.7	10.7	12.5	14.4	16.3
Cloud System Infrastructure Services (IaaS)	23.6	31.0	39.5	49.9	63.0
Total Market	**145.3**	**175.8**	**206.2**	**240.3**	**278.3**

BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service
Note: Totals may not add up due to rounding.

Source: Gartner (September 2018)

Fig:1

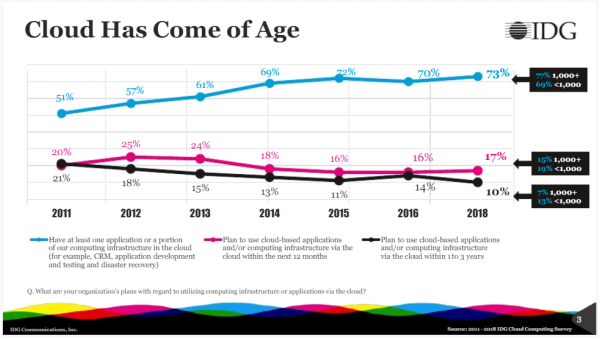
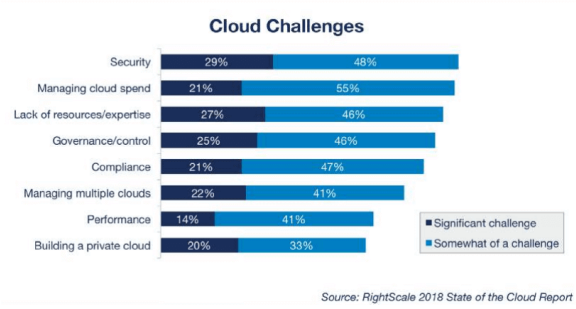


Fig:2



Source: RightScale 2018 State of the Cloud Report

Fig:3

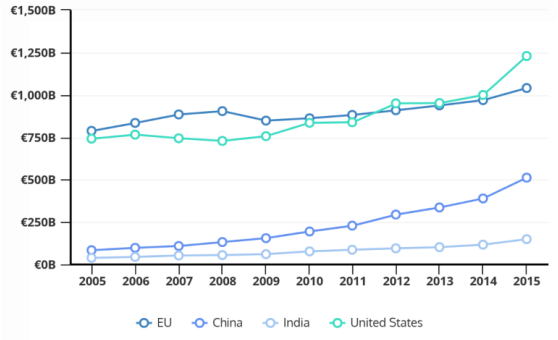


Fig:4

Statistics on Computer Technology Applications and the Data Protection Concept Given the identified threats, several options or countermeasures are at the disposal of United General Hospital. One of the steps involves conducting a risk assessment of the institution's IT systems. According to Cohen and Mello (2018), this step is linked to HIPAA guidelines regarding electronic personnel data transmission. By conducting a risk assessment of the IT systems, United General will ensure that vulnerabilities are uncovered and threats identified within the system, with Riley (2018) observing that an additional benefit of this assessment lies in the provision of room for the review of a firm's security policies. In response to the data compromise, another step that United General could implement involves the continued provision of HIPAA education to workforces. In so doing, Terry (2012) observed that the resultant sensitization of employees regarding implications of data breach reduces future risks of violation significantly. At United General, this education is poised to allow the employees to understand current regulations and rules as stated by HIPAA, as well as state regulations, upon which personnel data privacy (including Winnie's records) might be enhanced.

The third strategy at United General's disposal involves monitoring records and devices. According to Terry (2014), the period following a personnel's health record compromise requires institutions to be watchful of paper records and electronic devices that are left unattended, especially with the aim of avoiding theft. Hence, United Generals' senior leaders and managers have a role to play to ensure that all employees play an active role towards data safety, including locking devices and protecting systems in phones, desktops, and laptops using strong passwords. Whenever possible, United General could also curb the potential compromise of personnel records by enabling a Multi-Factor Authentication. Another major step that the organization needs to adopt and implement involves curbing against possible exposure of private personnel information to the public via networks available to all persons. Particularly, it is recommended that the organization creates sub-networks meant for guest activity. According to Terry (2017), this strategy is effective because of its ability to separate more secure networks meant for medical applications and devices from other guest activities. At United General, this step is poised to ensure that applications that carry and transmit sensitive personnel data do not interact with guest activities on publicly available networks.

Stringent management of access and identity is also recommended for implementation at United General, upon which records might be protected from compromise. Particularly, the organization needs to ensure that at each level, system users only gain access to information that is deemed pertinent to their specialized roles or positions, with easy log off or log on procedures only permitted on shared devices. This strategy is recommended because Pete, an intern at the institution and also a related party to Winnie's family, gained access to the wireless network of United General, as well as the personnel records of Dr. Moore to review Winnie's HIV test results, eventually spreading the same information to Pam (Winnie's daughter).

CONCLUSION

To ensure that the recommended strategies above are achieved, which involve curbing against future personnel record compromise and also HIPAA regulations governing how the organization needs to conduct its personnel record access and disclosure activities, several training topics are important, especially for the firm's employees. One of the recommended topics involves the Federal Trade Commission (FTC) Act and HIPAA. Imperatively, United General collects and shares personnel data. Therefore, this topic is deemed relevant because it might sensitize employees regarding the need to stretch beyond compliance with HIPAA and also ensure that their personnel record access and disclosure statements d not contravene the provisions under the FTC Act. Another topic includes public health. Particularly, there is a need for regular seminars and conferences to train United General's employees on how they could disclose protected health information under the Privacy Rule (for specified public health purposes and without the authorization of the target groups), especially during processes such as outbreak investigations and public health surveillance.

Another training topic involves health research and data privacy. In health-related and medical disciplines, it is important to note that there is a reliance on access to health information sources such as government complications of health data, hospital discharge records, disease registries, and epidemiological databases. From the perspective of the Privacy Rule, the research community needs to disclose, access, and use health information that is deemed individually identifiable, especially while implementing various research projects and protocols. At United General, it becomes important for employees to be trained on the extent to which such information's privacy if held by a covered entity, is protected by the Privacy Rule, as well as how researchers, subject to various conditions, could access and use the data for research purposes. Other recommended topics include HIV and HIPAA, genetic information, and health information technology.

REFERENCES

1. Cohen, G. and Mello, M. M. (2018). HIPAA and Protecting Health Information in the 21st Century. *JAMA*, 320(3), 231-232
2. Garson, A. (2010). *Current Perspective: The US healthcare System 2010, Problems and Potential Solutions.* American Heart Association
3. Riley, M. F. (2018). Big Data, HIPAA, and the Common Rule. In: Cohen IG, Lynch HF, Veyena E, Gasser U, eds. *Big Data, Health Law, and Bioethics*. New York, NY: Cambridge Univ. Press

4. Terry, N. P. (2012). Protecting personnel privacy in the age of big data. *UMKC Law Rev*., 81(2), 385-415
5. Terry, N. P. (2014). Big data proxies and health privacy exceptionalism. *Health Matrix Clevel*., 24(1), 65-108
6. Bansal, S.K., Saxena, V., Kandpal, S.D., Gray, W.K., Walker, R.W., Goel, D.The prevalence of hypertension and hypertension risk factors in a rural Indian community: A prospective door-to-door study(2012)Journal of Cardiovascular Disease Research, 3 (2), pp. 117-123.
DOI: 10.4103/0975-3583.95365