



Research Article

Milioris K & Papageorgiou K J Hosp Health Care Admin 4: 149.

DOI: 10.29011/2688-6472.000149

A Study on Healthcare ICT Systems and their Usefulness During CoVid-19 Focused in the European Environment

Konstantinos Milioris¹, Konstantinos Papageorgiou^{2*}¹Department of Tourism Management, University of West Attica, Egaleo, Attiki, Greece²Department of Business Administration, University of West Attica, Egaleo, Attiki, Greece***Corresponding author:** Konstantinos Papageorgiou, Department of Business Administration, University of West Attica, Egaleo, Attiki, Greece.**Citation:** Milioris K, Papageorgiou K (2021) A Study of Healthcare ICT Systems and their Usefulness During CoVid-19 Focused in the European Environment. J Hosp Health Care Admin 4: 149. DOI: 10.29011/2688-6472.000149**Received Date:** 25 August, 2021; **Accepted Date:** 03 September, 2021; **Published Date:** 08 September, 2021

Abstract

Recent rapid technological developments in the global environment are forcing countries to adapt their healthcare systems to current needs. Especially after the outbreak of Covid-19 pandemic multiple countries are updating and employing their ICT healthcare systems to facilitate the prevention and containment of the pandemic. Below literature review examines the efforts of multiple countries in Europe which employed Information Technology to monitor patients and control the spread of the pandemic. Additionally, security and privacy of sensitive medical data and tools for infection surveillance is also a crucial concern which is examined below.

Keywords: Information and Communications Technology; Healthcare Information Systems; Health Informatics

Introduction

Information and Communication Technologies (ICT) for healthcare unveil a plethora of new possibilities during current days. They provide a technical base for easy testing; they improve significantly the quality of service by allowing immediate access to medical data, test results and treatment history. At the same time they facilitate correct diagnosis by employing easier analytics, data correlation and easier monitoring of patients' health parameters. They facilitate setting up appointments with appropriate doctors at a convenient time. Some medical treatments can be even conducted online. Digitisation supports the promotion of a healthy life style and can prevent diseases. Electronic healthcare solutions can be offered across borders, giving citizens the feeling of security in this respect [1]. Digital technologies and data play a crucial role to contain the COVID-19 crisis. Information and Communication Technologies and data can offer an important tool for informing the public and helping relevant public authorities in their efforts to contain the spread of the virus or allowing healthcare organisations to exchange health data [2].

However, in order for all stakeholders to fully benefit from and trust electronic services and products, they must be properly designed, implemented in cost-effective way and provide an acceptable level of security and privacy. Specific Healthcare Information Technology systems and network-connected medical devices ("Internet of Medical Things") can be considered as two main components of the healthcare environment, where certification schemes could be visualized. Accordingly they include various sub-categories-starting from the hardware components used in the devices, to IT systems and services (cloud, portals). They all have their particularities, which need to be taken into account when discussing possible certifications. Health Information Technology is in fact the way of application of IT to the healthcare sector. It has a purpose of managing information exchange among all its stakeholders – government healthcare agencies, doctors, patients, administrators of data, insurance companies and others. Digital healthcare refers to tools and services that use Information and Communication Technologies (ICTs) to improve prevention, diagnosis, treatment, monitoring and management of health-related issues and to monitor and manage lifestyle-habits that impact health. Digital healthcare is innovative and can improve access to care and the quality of that care, as well as to increase the overall efficiency of the health sector [1]. Multiple innovative solutions that make use of digital technologies can provide the means to

support a reform in health and long-term care systems. eHealth, telemedicine and other digital technologies such as 4G/5G mobile communications, artificial intelligence and supercomputing offer new opportunities to transform healthcare systems. They allow the capture, management and processing of large volumes of diverse data generated from multiple sources to create new knowledge. They enable new approaches to personalised medicine, accelerating scientific progress, early diagnosis and prevention of diseases and more effective treatments. Furthermore, digital tools can assist in addressing shortages in healthcare staff in rural areas and certain specialties. They can also connect the various factors across the health and social care sectors, thus ensuring effective sharing of data and collaboration, in more effective care models. In addition, digital technologies can enable citizens to access information about health risk factors and well-being measures, and help them engage in healthy lifestyle behaviour and disease prevention. Finally, the analysis of digital health data and patient-reported data can lead to improved procedures, reduce inefficiencies, support outcome-oriented healthcare, promote the evidence-based assessment of innovative health technologies, as well as improve emergency preparedness and response to epidemics. EU policies have consistently emphasised the importance of digital solutions in healthcare [3]. Recent outbreak of CoVid-19 pandemic forced many countries to re-design their healthcare ICT systems to adapt to current needs.

Digitalising public health management

Against this wider public health background, the COVID-19 crisis is providing several examples of the use of digital technologies for health protection. First, telework and alternatives to face-to-face meetings like video conferencing are now being widely considered as a public health measure to be used at the outbreak peak and, at the same time, as a contribution to the green agenda against climate change. Telemedicine, the healthcare version of telework, is now being used in more and more from many countries as an appropriate mean to deliver care in the middle of the coronavirus outbreak [4]. The COVID-19 pandemic has also highlighted the pressing need for improved data collection and exchange to better monitor and manage public health issues and health systems. Data fragmentation and the limited degree of interoperability of health information systems are inadequate to provide the right information to the right people at the right time. In 2017 OECD Council Recommendation on Health Data Governance unveiled the framework to encourage greater availability of timely health data within countries and across borders, while ensuring that risks to privacy and security are reduced and appropriately managed. To improve co-ordination between authorities across the EU, and as part of its effort to create a European Health Data Space, the European Commission is currently developing a governance framework to promote a better use of health data, as well as a digital

health infrastructure supporting such access. Once operational, it will allow better use of data for health care, research, innovation and more evidence-based health policy-making. Two decades into the 21st century, health systems need to harness more fully the potential of new information and communication systems [5].

A report from OECD suggests that digital data can be amplified far beyond the original user. It provides the basis for doing science at new levels and in fields outside the original intent. For example, if weather, climate and public health data is designed for interoperability (the ability of two or more systems or components to exchange information) it can be integrated to predict the outbreak of an epidemic. Open access to data can lead to research being conducted all over the world for different purposes and in different contexts. Interoperability and commitment to open access to databases is, therefore, crucial for international and interdisciplinary access and understanding of data for the development of convergence technologies [6]. The EU recovery plan that was adopted by the European Council in July 2020 is designed to support the economic recovery from the COVID-19 pandemic and investments in the green and digital transitions of EU economies [7].

As already noted, alternatives to traditional face-to-face consultations are growing rapidly in many countries through the use of digital technologies, providing new opportunities to facilitate patient and doctor interactions in various ways. In 2019, primary care physicians in Sweden and the United Kingdom were more likely to offer to patients web-based communication options such as prescription refill and test results [8]. The COVID-19 pandemic has exposed the insufficient preparation of countries to cope with major public health emergencies. The costs of having more resilient health systems pale in comparison with the huge economic consequences of failing to do so. The new coronavirus is neither the first pandemic nor the last one, and many other more or less predictable events may have a huge impact on public health. It has thus become apparent that both the global and EU health security framework need significant strengthening. Fragmentation makes us all vulnerable and it is only through multilateral cooperation that we can face up to public health threats of the magnitude of COVID-19 [5].

Containment strategies, citizen's mobility and geo-location data usefulness during CoVid 19 pandemic

Google Community Mobility data show how visits to categorised places changed compared to an average reference. This reference was defined as the median value from a specific period. In order to estimate the overall strictness of the containment and mitigation measures taken by countries, an average reduction in mobility was calculated over March to May 2020 (i.e. from when most European countries enforced general social distancing measures), as compared with the reference period. Analysis

focused on leisure activities (restaurants, cafes, shopping centres, theme parks, museums, etc.) and public transport [5].

Thanks to this public-private cooperation, a systematic analysis of the relationship between human mobility and virus spread was conducted for the first time by scientists, together with a comparative cross-country analysis of the efficiency of containment measures. The data has provided clear evidence on the impact of mobility on the spread of the virus. It shows that mobility alone can explain the initial spread of the virus in Italy, France and Spain. The results also show that the containment measures taken by governments and regions, including physical distancing and mobility restrictions, were efficient in limiting the spread of the virus. Furthermore, the mobility data helped identify mobility patterns and areas, which cross regional or provincial borders. For instance, to reach the closest grocery store or the closest city offering employment possibilities, some Europeans have to cross a regional border. The findings therefore suggest that mobility restrictions should take into account such geographical mobility patterns, rather than be based on administrative areas such as regions or provinces. It also emerged that when physical distancing measures were put in place, the mobility factor became less important in defining the spread of the virus. These findings show that in the future, mobility data may support policymakers in formulating the best data-driven approaches for coming out of confinement, mapping the socio-economic effects of the lockdown measures and building future scenarios in case of new outbreaks [9].

Many successful health ICT applications were further developed during CoVid pandemic. SORESA and the Campania Region of Italy have cooperated to digitalise healthcare in Campania. Then the COVID emergency struck. As a result, the system was enriched with an Information Technology (IT) platform specialised in monitoring the emergency. The new platform brought together citizens, doctors, epidemiologists, prevention services, and laboratories. The new development enables citizens to access the results in real time and to send reports to their personal doctor. Integrated with the COVID patients' surveillance platform, the system facilitates a structured monitoring of suspected COVID and COVID-positive patients [10].

Mobile and location-based technologies help track, trace and isolate infections

Contact tracing is an investigative process through which the recent contacts of confirmed infections are traced backwards, so that they can in turn be tested and isolated as a means to break the chain of contagion. Especially when the prevalence of infection is still relatively low and geographically limited, contact tracing can thus be an important component of an effective containment strategy. However, it is a very labour-intensive activity, which requires trained investigators to manually track down people

who have been exposed to infected individuals. As the number of professional contact tracers was insufficient in most countries, and the speed at which contacts are traced is a crucial variable for the success of this strategy, several countries have looked into the possibility of automating at least part of this process using digital instruments such as smartphone apps and related technologies. Across Europe, digital contact-tracing apps have either been developed or launched in at least 23 European countries. Based on a self-report system by users who have been diagnosed as infected, these apps use data on proximity (Bluetooth) and location (cell towers and global positioning system, i.e. GPS) to identify individuals who may have been exposed to confirmed cases. Alerts are then sent to those individuals, recommending that they should be tested or even self-isolate. Some apps send broad alerts to people who were located in a certain area, and other apps send targeted alerts at specific individuals who may have been in contact with a confirmed case. Some apps are used by traditional face-to-face contact-tracers to assist them in interviewing potential contacts, while other apps are fully automated. The data generated by these apps can be communicated to, and stored in, a central server or it can be decentralised, saved only in the mobile devices of users. Some digital tools – like the Google COVID-19 Mobility Report – use collective data from many individuals to monitor changes in mobility in response to lockdowns, social distancing and quarantine policies. Other digital applications take advantage of data on specific individuals to enforce policies to contain the spread of the virus. In Poland, an app uses facial recognition and location data to monitor and enforce quarantine by imposing fines, and can be used by the police. In France, cities are using artificial intelligence and CCTV to monitor the use of masks in public spaces. Lichtenstein is the first European country to use electronic bracelets to collect biometric data in real time, and the United Kingdom is using an app to collect self-reported symptoms from users. Over 50 million Europeans downloaded digital contact tracing apps in the first nine months of 2020. Close to 40% of the Icelandic population has downloaded a similar app and between 20-30% of populations in Finland, Germany, Ireland, Norway, Switzerland and the United Kingdom have downloaded national apps. Most apps target 50-60% penetration to reduce the reproduction number of infected population. While lower adoption rates may still have some benefits, low rates will inevitably fail in their objective of facilitating traditional contact tracing efforts. There are also questions regarding the reliability and accuracy of the underlying data, and the potential for false positives and false negatives infections. Furthermore, in 2019, around 27% of individuals did not use mobile devices to access the internet in the EU. In this case, a fully automated digital contact-tracing strategy is unlikely to be successful, although it can complement traditional contact-tracing efforts (ECDC, 2020). There are also significant concerns regarding the potential for misapplication and privacy abuses. A recent assessment of 17 contact-tracing apps

(including apps from Europe) found them to be insecure and easy to hack. There is also a fear that once new tools of surveillance are introduced, they are difficult to reverse, even when the crisis has passed [5].

Contribution of regularly collected data from electronic health records

Beyond innovative uses of mobile technology, there are rich opportunities to take advantage of the massive amount of data that are collected every day in health systems across Europe. Countries with standardised national Electronic Health Records (EHRs) can extract high quality routine data from those systems for real-time surveillance, but only six European countries (Austria, Denmark, Estonia, Finland, Slovak Republic and the United Kingdom), have high technical and operational readiness to generate information from EHRs [11]. Finland and Iceland both have national EHR systems with patient portals and, as a result, were able to quickly develop the capability to track COVID-19 patients' longitudinal progress, offer integrated tools for people to report their symptoms, and triage people to appropriate services as their symptoms progressed. OECD data from 2019/2020 indicate that ten EU countries are prepared to undertake national dataset linkages in support of COVID-19 research because they routinely link at least hospital and mortality data (Austria, Czech Republic, Denmark, Finland, France, Latvia, Netherlands, Norway, Slovenia and Sweden). However, very few of these countries had data timely enough to be useful for decision-making. Only 3 out of 16 surveyed European countries had hospital and emergency care data that were updated either daily or weekly, and only two had mortality data in real time. Further, only six countries (Austria, Denmark, Estonia, Finland, Slovak Republic and the United Kingdom) made a range of health care data readily and securely available to the research community through real-time remote access services or a research data centre. These services increase the probability of having a strong unit of researchers familiar with the data who could respond quickly to generate new information to address the crisis [5].

Determining Europe's digital future

The European Commission is working to provide citizens with access to safe and top quality digital services in healthcare. The communication on the digital transformation of healthcare identifies 3 priorities:

- Citizens' secure access to their health data, including across borders, enabling citizens to access their health data across the EU.
- Personalised medicine through shared European data infrastructure, allowing researchers and other professionals to pool resources (data, expertise, computing processing and storage capacities) across the EU.

- Citizen empowerment with digital tools for user feedback and person-centred care using digital tools to empower people to look after their health, stimulate prevention and enable feedback and interaction between users and healthcare providers.

A public consultation on the transformation of healthcare was held in 2017. It gathered input on the scope of policy actions to be pursued in order to improve people's healthcare. This consultation received nearly 1,500 replies of which over 90% of respondents agreed that citizens should be able to manage their own data. More than 80% of the respondents agreed that sharing health data can be beneficial and around 60% of respondents said that they do not have access to digital health services. Transformation of healthcare for a digital Europe will benefit people, healthcare systems and the economy. Digital technologies such as 5G mobile communication, artificial intelligence and supercomputing offer new opportunities to transform the way we receive and provide healthcare services. They enable innovative approaches to independent living and integrated health and social care. Health data and advanced data analytics can help accelerate scientific research, personalise medicine, and provide early diagnosis of diseases [1].

Building upon precedent initiatives enhancing the creation of a Europe fit for the digital age, the digital transition should be something that benefits everyone, putting people first and opening new opportunities for business. Through initiatives for health sector and health information system reform, European Member States are now actively building upon their national foundations for eHealth to deliver public health and health services in a more strategic and integrated manner. They acknowledge and understand the role of eHealth in contributing to the achievement of universal health coverage and have a clear recognition of the need for national policies, strategies and governance to ensure the progress and long-term sustainability of investments. However, leveraging eHealth as a national strategic asset demands a more coordinated approach to planning, implementation and evaluation. Evidence of the importance of this approach is observed through a majority of European Member States developing national strategies or policies for eHealth, universal health coverage or national health information systems, and ensuring sustainable funding for their implementation [12].

Factors and process for digital transformation in healthcare

More important, however, is the recognition that successful investment in eHealth requires far more than just the acquisition of technology. A view of the complete spectrum of the impact and changes required to organizational processes, structures, roles, standards and legislation is needed. As well as consideration of the specifics of human resources, education, reimbursement and the culture of those who will be utilizing the eHealth services

any of which can serve to derail initiatives if neglected. Perhaps the most revealing message is the need for stronger political commitment for eHealth, backed by sustainable funding, and for effective implementation of policy that is protected from frequent changes in the national political landscape. Recommendations for ICT healthcare transformation are a call to action for all Member States in the WHO European Region to take appropriate steps to strengthen their existing national eHealth foundations and to accelerate activities for future development and adoption of eHealth. Explicit political commitment by governments in the European Region to adopting eHealth is required. This commitment needs to be backed by sustainable funding for the implementation of eHealth programmes and actions for capacity-building and evaluation that are aligned with a national strategy for eHealth. An inclusive and intersectoral approach to the development of national eHealth strategies is recommended to ensure their relevance to all stakeholders and to promote shared action in achieving health objectives. Member States are further recommended to use the methodology described in the WHO and International Telecommunication Union National eHealth strategy toolkit as a basis for developing their national vision, action plan and monitoring and evaluation frameworks for eHealth. Having a national eHealth strategy that embodies the elements of achieving Health 2020 policy is a key enabler for strengthening people-centred health systems and public health capacity [12].

Patient care, including patient quality, patient safety and patient satisfaction, is a clear focus of healthcare organisations both in Europe and in the wider EMEA region at this time. Most of the organisations represented in this sample are stepping up to this challenge by implementing ICT solutions that focus on the clinical areas of their hospital. They are also taking the time to address underlying infrastructure issues, such as implementing wireless systems, an intranet and identity management solutions to ensure easy and secure access to clinical (and other) data. As they move forward, healthcare organisations need to keep in mind that ICT is a tool to support the overall business objectives of the healthcare organisation. As such, it is critical that the ICT strategic plan directly supports the healthcare organisation's broader strategic initiatives. Senior ICT executives must also participate, providing them with a voice for ensuring that ICT can fully support organisational objectives. In addition, as organisations move forward with implementing clinical technologies on a wide variety of levels, they need to ensure that clinicians are involved at every stage of the process. This means that clinicians should be involved in making the decision on the technology, involved in implementing the technology, and be accountable for realising the value of the ICT investment through lower costs, better patient outcomes, smoother processes and better patient and employee satisfaction. Only then will the organisation be able to get the buy-in needed from clinicians to make the implementations successful

[13]. In addition, we must harness the lessons of this pandemic crisis and plan for a thorough assessment of health system resilience, drawing on the best practices from countries within and outside Europe and the support that the European Commission can provide. This process should involve all stakeholders and lead to better readiness for pandemics and other public health emergencies in the future [5].

Security and privacy

Consent of medical data access from multiple healthcare parties, could decrease privacy by leading patients to make decisions to share data where they do not understand the consequences that may be clear to persons with professional knowledge of the risks and benefits. In short, medical privacy and consent are deeply connected, but they are not equivalent [14]. Security threats in health care are an evolving concern. While in the financial sector the motives of an attacker are often clear, this is often not the case in health care. For instance, a phishing attacker wants to get types of private information that can be monetized in the online black markets, information like bank account passwords and credit card numbers. Accordingly, healthcare organizations store, maintain and transmit huge amounts of data to support the delivery of efficient and proper care. The downsides are the lack of technical support and minimal security. Complicating matters, the healthcare industry continues to be one of the most vulnerable to openly disclosed data breaches. Whereas implementing security measures remains a complex process, the stakes are continually raised as the ways to defeat security controls become more sophisticated [15].

Three factors need to be taken into account in predicting attacker motives and assessing security risks. First, health data often has associated administrative and financial data. For example, medical demographics may well include enough information to associate the patient name with a credit card. Moreover, personal information can be used to file fraudulent claims. Large-scale insurance fraud in the form of false billings is another common incentive.

Second, health data may become collateral damage in an attack. This threat is worsened by the regulatory review process for hospital equipment, which may slow the updating of software, hence preventing the rapid application of security patches. Detection of an intrusion in a hospital would result in the system being taken out of service until recovery is carried out.

Third, even if health data may motivate fewer attackers than in other sectors of the economy, it is often exceptionally critical to the safety of an individual and its corruption can be life-threatening. It may seem unthinkable that someone could deliberately consider corrupting health data, until it is done.

On the bright side, unlike rooms full of paper records, it is possible to trace, through electronic logs, which users look at which records so an auditor can use this information to detect abuses. There have been many examples of abuses that were caught in this way. Some involve access to the records of celebrities like athletes and actors: others involve incidents where, for instance, an employee of a provider accesses the record of a former spouse. These and other types of abuses are often addressed by investigations carried out after a complaint [6].

The invasion of patient privacy is considered as a growing concern in the domain of big data analytics due to the emergence of advanced persistent threats and targeted attacks against information systems. As a result, organizations are in challenge to address these different complementary and critical issues [15].

As medical data continuously transform, security and patient privacy is dominant in milestone in such technologies. Since healthcare clouds with big data become noticeable with their presence, data maintaining organizations will be more reluctant to share massive healthcare data for centralized processing. Hence, distributed processing across disparate clouds and leveraging on collective intelligence could be implemented instead. Secure patient data management is foreseeable in healthcare clouds. Where data will be collected and linked in large amounts from multiple networks. Furthermore, by ensuring secure and privacy issues real-time analytics will drive proactive healthcare and wellness [16].

Conclusion

The foremost lesson learnt from the COVID-19 pandemic is that there is no trade-off between lives and livelihoods. Public health and the global economy are inextricably linked. We cannot have one without the other. Healthy global economic systems depend on healthy citizens. Strengthening the preparedness and resilience of health systems will require additional resources. With the right investment – from better global public health governance, to stronger health information systems and support for a digital transformation of health systems – the return on the well-being of people and the functioning of economies and societies will be high and long-lasting [5]. Further collaboration at EU level could strengthen mutual learning, knowledge sharing and transfer among care authorities and help those who wish to ease their path to large scale adoption of digital health innovations. Joint action can also boost the possibilities for economies of scale for technology and service suppliers and reduce the risk of fragmentation in care delivery for citizens [3].

References

1. eHealth (2021) Shaping Europe's digital future - European Union.
2. JoinUp European Union (2021) Rolling plan for ICT standardisation.
3. Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions on enabling the digital transformation of health and care in the Digital Single Market empowering citizens and building a healthier society. COM (2018) 233 final.
4. EHTEL (2020) Public health emergencies and digital health.
5. OECD/European Union (2020) Health at a Glance: Europe 2020: State of Health in the EU Cycle, OECD Publishing, Paris.
6. OECD (2013) ICTs and the Health Sector: Towards Smarter Health and Wellness Models, OECD Publishing.
7. European Council (2020) Special meeting of the European Council (17, 18, 19, 20 and 21 July 2020) - Conclusions.
8. Michelle M, Tikkanen R, Shah A, Schneider EC (2019) Primary Care Physicians' Role in Coordinating Medical and Health-Related Social Needs in Eleven Countries. *Health Affairs* 39: 1.
9. European Commission (2020) Coronavirus: Mobility data provides insights into virus spread and containment to help inform future responses-Digibyte.
10. EHTEL (2021) SINFONIA faces the COVID-19 emergency.
11. Colombo F, Oderkirk J, Slawomirski L (2020) Health Information Systems, Electronic Medical Records, and Big Data in Global Healthcare: Progress and Challenges in OECD Countries, in *Handbook of Global Health*, Springer International Publishing.
12. WHO - From Innovation To Implementation - eHealth in the WHO European Region (2016) WHO Regional Office for Europe, Denmark.
13. Garets DE, Horowitz JK (2008) Healthcare ICT in Europe: Understanding trends in adoption and governance. *Journal of Management & Marketing in Healthcare*. 1: 286-296.
14. Asghar MR, Lee T, Baig MM, Ullah E, Russello G, et al. (2017). A review of privacy and consent management in healthcare: A focus on emerging data sources. 2017 IEEE 13th International Conference on e-Science (e-Science) (pp. 518-522). IEEE.
15. Abouelmehdi K, Beni-Hessane A, Khaloufi H (2018) Big healthcare data: preserving security and privacy. *Journal of Big Data*. 5: 1-18.
16. Patil KH, Seshadri R (2014) Big Data Security and Privacy Issues in Healthcare. 2014 IEEE International Congress on Big Data.