Technical Viewpoint of Challenges, Opportunities, and Future Directions of Policy Change and Information-Flow in Digital Healthcare Systems

Areeg Samir
Computer Science Department
UiT The Arctic University of Norway
Tromsø, Norway
email: areeg.s.elgazazz@uit.no

Håvard D. Johansen
Computer Science Department
UiT The Arctic University of Norway
Tromsø, Norway
email: havard.johansen@uit.no

***Abstract*—Digital healthcare systems often run on heterogeneous devices in a distributed multi-cluster environment, and maintain their healthcare policies for managing data, securing information flow, and controlling interactions among systems components. As healthcare systems become more digitally distributed, lack of integration and safe interpretation between heterogeneous systems clusters become problematic and might lead to healthcare policy violations. Communication overhead and high computation consumption might impact the system at different levels and affect the flow of information among system clusters. This paper provides a technical viewpoint of the challenges, opportunities, and future work in digital healthcare systems, focusing on the mechanisms of monitoring, detecting, and recovering healthcare policy change/update and its imprint on information flow.**

Keywords*—*Digital Health; Healthcare; Distributed Environment; Policy; Multi-Cluster; Monitor; Detection; Performance; Workload; Recovery.

I. Introduction

Digital healthcare systems deliver services to consumers and patients and help them manage their health by providing a real-time communication environment. Each system is commonly organized into many clusters with different capacities, configurations, resources, and policies. A cluster has a set of components that include several services. For instance, a healthcare component might include services, such as primary and hospital care services. Each service consists of workflows, information pathways, and processes. A service could be integrated within the same organization to create a single unit. Different systems are also used for various purposes; for example, the municipality uses one electronic medical record system for documentation, while the hospital and primary healthcare services use another type. Moreover, various resources are shared among multiple organizations and healthcare individuals. Here, it is difficult to predetermine a fixed set of system individuals in such a dynamic environment as their roles and access control could be changed with system policy change. The system is expected to scale to respond to load variations, leading to unexpected overhead due to data movement and high resource consumption impacting system services, processes, and information flow.

Different distributed management information system policies of healthcare are applied to manage the system's information flow, such as data security, data management, health information dissemination, healthcare system resources, and data analysis. In such a system, communications, dependency, precedence, information shared between the system's clusters, different data standards, and multiple processes might be impacted by changing/updating policies associated with data flow in the system.

The lack of integration between the system's clusters and services complicates sharing, accessing, and flowing of information in the system. Coordination is more of a challenge due to the increasing complexity of services and the increasing complexity of their political environment.

The paper aims to explore challenges, opportunities, and future research directions in the digital healthcare system focusing on the impact of policy change/updates on the flow of information and its propagation at different system levels. We provide high-level information about the paper topic while being low-level enough to represent several key research areas that mainly focus on the challenges and opportunities within digital healthcare systems. We mainly concentrated our investigation on the perspectives of sharing, monitoring, detecting, and recovering the policy change and information flow within healthcare system processes.

The paper is organized as follows. Section II explains the method of research. Section III explores the information flow of the digital healthcare system. Section IV discusses the challenges of information flow within a digital healthcare system. Section V introduces opportunities. Section VI provides a set of future research directions followed by conclusions section.

II. Research Method

The paper's objective is addressed by answering a research question: what are the challenges and opportunities that the digital healthcare system might face when healthcare policies change in a distributed environment?

A. Search and Review Strategy

We conducted a systematic review according to PRISMA guidelines [1] to identify documents that reported on the policy change and information flow in healthcare and digital healthcare systems. We reviewed the state-of-the-art focusing on the policy's change/update and its impact on the information flow in the digital healthcare domain. We are interested in investigating various mechanisms that monitor, detect, and recover the change and its impact on the flow.

Moreover, the research paper focused on reports issued from pioneer healthcare organizations World Health Organization (WHO), Joint Commission International, and the Organization for Economic Co-operation and Development (OECD) for the period from 1999 to 2022 for several reasons:

- Detailed quantitative data on the use of digital health appeared during that period.
- WHO released its first Guidelines [2] on digital health.
- A significant development in digital health became active during that time [3].
- Significant relevant research was conducted during that period [4]–[10].
- Diversity of digital health strategies [11].

According to the previously mentioned organizations, we selected reports and documents issued by the healthcare associations focusing on healthcare in general and digital healthcare in specific, and we classified them into regions according to the published classification by WHO as shown in Table I. After that, we selected around 19 countries from all regions[1], and we investigated the healthcare system use-cases of these countries. The selection is made according to the common features, the characteristics of their healthcare, and digital healthcare systems within and across regions in which we are interested, such as:

- Digital healthcare technology: the ways that health individuals communicate, access/store/process medical and health records, research health information, and engage in a person-to-person exchange of text, audio, video, and other data.
- Digital healthcare processes: the workflows and information pathways within and across the organization.
- Multiplicity of policies: methods followed in handling various policies with their versions in the organization.
- Resources variations: various resources in varying amounts and configurations are dispatched towards the system's activities depending on the dynamic requirements. The scale of resources is the basis of the diversity of the actions taken.
- Dynamic adaptation: adaptation to hazards and adequately environment conditions and to the emerging needs and requirements of the situation.
- Collaboration across and within an organization: the activities are performed by organizations from different sectors, including interactions, operations, and relationships of system components within and across the organization.
- Consistency of information sharing across the whole process of the system.

[1]Europe: Nordic countries, Netherlands, Czech Republic, Serbia. Asia: Japan, China, Vietnam, Taiwan, Kurdistan. Africa: South Africa, Tunisia, Egypt, Nigeria, Zambia, America: the USA

TABLE I
HEALTHCARE ASSOCIATIONS ACCORDING TO REGIONS

Region	Associations
Europe	Public Health Association - European commission
	Council of Europe and Health
America	Pan American Health Organization (PAHO)
	American Public Health Association
	Joint Commission on Accreditation of Healthcare Organizations (JCAHO)
	National Institutes of Health (NIH)
Asia	The Association of Asian Pacific Community Health Organizations (AAPCHO)
Africa	Africa Health Organisation (AHO)
	West African Health Organisation (WAHO)
	Amref Health Africa
	African Union

B. Search Criteria

Moreover, papers are selected from major journals and conferences[2] in health, healthcare, digital healthcare, and medical care. Based on that, we searched Web of Science, PubMed, Scopus, Medline, Scielo, IEEE Xplore Library, ACM Digital, Science Direct, Springer Link, and Google Scholar using criteria: years = $1996 - 2022$, and keywords = "Healthcare System Information Flow" OR "Information Flow Control Multi-Cluster System" OR "Policy Change and Update Management" OR "Monitor Policy Change" OR "Detect Policy Change" OR "Recover Healthcare System" OR "Health Care Management" OR "Healthcare Service Quality" OR "Information Share" OR "Hierarchical Policy Management" OR "IoT in Healthcare" OR "Cost Reduction" OR "Healthcare Resource Allocation" OR "Hospital Workflow Processes" OR "Uncertainty in Healthcare Management" OR "Digital Healthcare Security Cloud".

C. Search Outcome and Analysis

We ended up with more than 2000 papers distributed unevenly among the journals and conferences.

We created a map analysis of the "Digital Healthcare" definition based on bibliographic analysis utilizing VOSviewer version 1.6.18 to concentrate on the works in digital healthcare during the period mentioned above. We determined whether each paper: (1) had some form of qualitative/quantitative analysis, technical viewpoints, method development, or review of methods in the keywords mentioned above, and (2) considered a multi-cluster approach. We conducted a systematic literature review of potential barriers to policy change and information flow in digital healthcare systems. That left us with 241 papers for a full review. We evaluated the papers according

[2]healthcare, health policy management, health services research and policy, transactions on software engineering, computing transactions, Internet of Things, International Journal of Trend in Research and Development, Journal of Business & Economic Policy, International Journal of Advanced Computer Science and Applications, International Conference on Pervasive Computing Technologies for Healthcare

to different criteria: information flow control modeling, dynamic monitoring, continuous detection, data sharing, policy consent, security concern, information flow recovery, and cost reduction. Papers that did not focus on those criteria were excluded. We ended up with 22 papers that are relevant for our survey.

D. Search Boundaries

We analyzed the healthcare, digital health, and medical systems in cloud computing, edge computing, statistical and dynamic analyses, machine learning, telemedicine, e-Health, security (blockchain platforms), and IoT. Due to the enormous scope of digital health technologies and literature studies, the paper could not discuss all aspects of these fields. The paper aims to discuss the recent challenges and advances in healthcare and digital healthcare.

III. Information Flow in Healthcare System

According to the research method conducted previously, the infrastructure of a healthcare system consists of various electronic medical/health records, databases, networking technologies, and other specific biomedical, administrative and financial technologies that generate, transmit and store healthcare information [4][6][7][12]–[16]. The information flow from healthcare providers (Health Individuals) is entered into an Electronic Health Record (EHR) [17] and then networked to regional and national databases through EHR [12][15][18], as shown in Figure 1.

Based on that, a healthcare provider might generate various complex processes that affect the flow of information within a system [8][12][15][19][20]. The number of possible processes increases with the number of interacted participants. Thus, the complexity of processes varies among the interacted healthcare participants. For example, four healthcare participants in a hospital care team might create eight separate processes or more, as shown in Figure 2. The main flow of information among the healthcare participants is within two units: inpatient care (patient and admission to medical department) and primary care (doctor, medical department, general practitioner). Both units share information, and only authorized participants such as medical staff could access the collected data. The patient needs a general practitioner referral (A) for specialist treatment coverage, communication with laboratories and radiology services, and sick leave. The patient uses the referral (B) to the general practitioner's acute-care services and makes co-payments directly to care providers during their visits. The general practitioner admitted the patient to the medical department (C) to be examined and treated by a specialized doctor (D:H). At the same time, the general practitioner transmits prescriptions electronically to pharmacies and uses electronic health records to store, access, and retrieve patient data. Such flow of information is shared between the system's participants, and it might constitute one or more processes that might include other sub-processes. For example, a nurse directs a patient to a medical doctor who takes information from the patient and records it, see Figure 2.

When referring the patient, a doctor sends a referral message to the Health Registry Server. The message is stored in a Repository (e.g., health, clinical, national, and statutory). The doctor sends a referral message to a requested hospital, which sends the patient's information to the Registry Server for future use. The flow of information could be direct flow, such as the interaction between patients and physicians (e.g., doctor and nurse), as shown in Figure 2. It could be an indirect flow through central units such as funds and insurance companies, as shown in Figure 1. In such a case, the hospital is responsible for refunding and defining its policy.

The flow could be more divergent such as a patient needs unavailable service in a hospital. In such a case, the hospital would buy the service from another specialized hospital, which generates a net of interacting hospitals with various processes and sub-processes, including their dependency and precedence. A massive amount of data from multiple components might be generated and gathered to be stored and analyzed locally or remotely (i.e., cloud servers) to manage the flow of information.

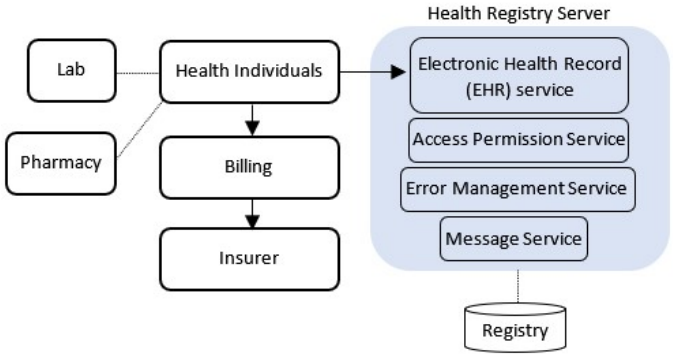

Figure. 1. Healthcare Information Flow

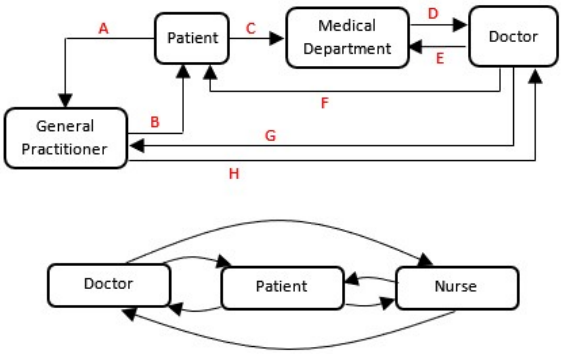

Figure. 2. Possible Processes Between The Communicated Individuals

In such a system, the information shared between participants might be subjective to several perspectives, such as:

- Organizational and managerial perspective: organizational boundaries, system participants' experience, variety of resources, trust between participants within and across organizations.

- Technological perspective: heterogeneous resources, multiple software, various security techniques.
- Policy perspective: the attempts to review policy processes in system workflow are challenging in resource constraint settings with less accessibility of policy, variety of policies, different policy versions, multiple policy path dependencies, and fragmentation of health sectors.
- Political perspective: routine, legislation, and information authority could limit health services offered by some providers.

The poor share of information could have consequences at different system levels. For example, at the computational level, the system's components resources (node's CPU, memory, network) could be saturated for several reasons such as security breaches, lack of resources, or process delay. Information exchange delays might happen in a healthcare system at the administrative level due to policy updates or lack of information. A healthcare system could be bounded by having many different policies that shape its system performance at the communication level. For example, a policy might prohibit general practitioners from obtaining a medical record directly from the records of a department without the permission of a hospital clinician. Electronic health records make it possible for healthcare individuals to share essential information at the security level. The share and open nature of interconnected health records across various organizational structures might allow access to sensitive medical data. For instance, medical staff could override restrictions to access sensitive data that were restricted in normal conditions when critical situations occur.

IV. The Challenges of Healthcare Policy Change and Information Flow Management

Due to the distributed nature and dependencies between components of healthcare system clusters, safe interpretation of the information exchanged between such heterogeneous organizations, and healthcare systems might face several challenges such as changes in regulation, lack of functional integration, lack of support for delivery of information across system components, leak of sensitive information, and lack of interoperability among healthcare system components. In such a case, policy violations might happen and lead to performance degradation.

The Followings represent the challenges of healthcare and digital healthcare systems related to policy management, policy propagation, information flow, policy change, healthcare data storage, and information sharing focusing on monitoring, detecting, and recovering information flow.

A. Policy Change and Information Flow

A healthcare policy defines the way information moves throughout a system. The policy is designed to preserve the confidentiality of data or integrity of data to prevent information from flowing to nonauthorized healthcare participants. However, healthcare applications involve dynamic requirements, which motivates the development of various kinds of dynamic policies as follows.

1) Domestic Regulations: Healthcare policy involves the creation and implementation of laws, rules, and regulations for managing nation's healthcare system. Some factors could condition information flow when a policy change propagated to the system, such as domestic politics, including political constraints, ideological preferences of politicians, policy participants, and policy entrepreneurs. One way to improve healthcare is through change policy, which involves decision-makers and stakeholders from different institutions; however, it is difficult to change policies because of dependency paths between different institutions. Healthcare agencies might be slow, bureaucratic, and inefficient. Once a country or a region has started a policy change, the cost of a reversal is very high. Moreover, in some areas of regulation, the division of authority is not clearly outlined, a drawback that has sometimes led to chaotic results. Any regulation that affects the healthcare system also affects the quality of healthcare. Thus, monitoring transparency in regulation is required to ensure quality-assured, safe, and effective healthcare services. A simple approach could be to provide interval forecasts of the policy change/update impacts of legislation considering cost and time.

2) Multiplicity of Policies: A healthcare system has several policies composed of different rules with their constraints, resources, parameters, and strategies. A change within policies could influence the internal and external system processes. Every process in a system might be executed in a given run, making correlations among them nontrivial. For different policies, the system might be re-analyzed in case of a policy change to track dependencies between the system's processes at run-time and at the same time to use the collected set of dependencies to check its processes against possible correlations for potential indirect information flow. Healthcare organizations find it difficult to effectively manage information flows within and across healthcare systems as it flows within and across diverse organizations. Thus, the change of policy results in many problems such as inappropriate decision making, less care management, poor quality assessment, ineffective planning, increase in medical errors, high cost, and a decline in the quality of patients' care.

3) Resource Utilization: When a policy change occurs, a system should cooperate correctly with the existing infrastructure to cope with the new applied rules and constraints and avoid rewriting all existing code to account for information flow constraints. Here, information flow congestion could mainly happen due to the intensive use of resources. Even though the policy rules are pre-specified, certain policy alterations could sometimes cause intensive resource use. Several static [21] and dynamic [22] analysis techniques are used to track the change in information flow and policy change; however, the literature studies neither provided run-time dependency tracking nor addressed indirect flows [23]–[26]. Moreover, current systems are not designed with an automated mechanism to dynamically adapt to the change in

information flow policies [19][27].

The system should be able to predict future health services, healthcare needs, and rates of utilization of services and resources based on a foreknowledge acquired through a systematic process. The main idea is to monitor the current state of system resources and deal with a workload based on the current availability of the system cluster's capacity to satisfy their optimal performance parameters without causing performance degradation. A good understanding of the healthcare system requires analyzing the current and historical data to predict future needs accurately. Thus, reliable health forecasting could create alerts for the management of information flow and scientifically allocate resources to reduce the costs of supplies and resource redundancy.

4) Leak of Information: Another challenge for changing policy is that it might allow information to flow from personal data to public observers. Electronic IDs and tokens are used to prevent leaks and theft of information. However, current works [28] are not practical enough to handle the runtime policy change, or their method was inconsistent with the decentralization nature. Some works [29]–[31] rely on computationally heavy modular exponential operations or elliptic curve point multiplication operations. However, those works are very complex as the number of involved calculations is enormous, the structure of the data stored in the blockchain is difficult to query within a blockchain, limiting data usage, and the problem of efficiency remains to be solved. Noninterference is utilized to keep the flow of information within the authorized parties; however, many applications permit such downward flows according to their defined security policy, and some valid programs are rejected as insecure. Thus, specifying the kind of policies that includes downgrading, determining the nature of a downgrading mechanism, and the kinds of security guarantee are challenging because current approaches are too restrictive and challenging to enforce [32].

5) Lack of Interaction: Healthcare participants faced interaction difficulties due to situational and organizational factors. Lack of interaction leads to miscommunication and duplicate work. The cost of upgrading the system with the changed policy could be very high, which makes justifying the return of investment a challenging task. The use of cloud-based communication platforms like Unified Communications as a Service (UCaaS) is highly effective in breaking down communication barriers. However, the quality and availability of UCaaS services are tied to an organization's unique use case and specific set of business demands. When degradations in the quality of services occur, it is difficult to pinpoint the source of the problems in such a complex environment, making it challenging to ensure the quality of the healthcare system participants experience. A key to successful information flow while policy change is the seamless interaction between healthcare participants across and within the system. It is required to understand and control the overall effect of governing policies on the system behavior. The system should be self adaptable to the changes in policy and adjust its flow accordingly so the system's participants could receive the information smoothly. The correctness of the adaptation process should consider system stability, service availability, and resource capacity. Strategies should also be in place to help build the empathetic, relationship-building skills required to understand the patient's perspective.

B. Poor Sharing of Health Information

The Healthcare system requires collaborative efforts from diverse healthcare providers and institutions to provide care for patients; however, since a patient is no more a passive recipient of care, the provision of high-quality services becomes indispensable due to:

1) Tangled System Structure: Patients' information is stored in diverse registries and repositories across different healthcare organizations to simplify authorized access to healthcare participants within the same institution. In such a system, many participants are involved in delivering care services, each having their interests, concerns, rules, and constraints. Some works [33] only handled hierarchical system structures without dealing with complex interrelationships between system variables. Network analysis techniques such as the Bayesian network [34] enable the estimation of the probabilities of system states and their covariates. Graph pruning is utilized to remove weak dependencies in the system structure [35]. However, it is challenging to choose prior probabilities and their appropriate probability distributions in such a dynamic system, especially in the presence of missing data.

Here, the conceptual framework must be set up clearly to identify the hierarchical structure. However, it is difficult to establish a relationship among all care entities as the system has a hierarchical dependent nature. Failure to account for the hierarchical structure could result in models that lead to unclear and misleading interpretations of the relationships under investigation, which results in additional costs in terms of resources, protocol complexity, and performance.

Thus, fragmentation and duplication of patients' information might happen, which impedes the ability of diverse healthcare practitioners to share data and gain access to patients' vital information. Accessing sensitive patients' information is complex and time-consuming for health care participants as it results in high transaction latency and low transaction throughput. Also, due to the dynamic nature of information flow and the change within policy rules, the quality of information is variable and unreliable. Hence, authorization and privacy should be dynamically adapted to the new policy rules to share patient data among different institutions within the system and give patients access to their records.

2) Information Inconsistency and Incomplete: Healthcare providers are usually presented with incomplete and inconsistent information during care. In such a case, information storage and retrieval problems might happen due to an information gap between medical participants and patients. The incomplete exchange of healthcare information during care transitions might cause ineffective care and additional healthcare spending [36]. Here, rollback of process or correction is one of the biggest challenges as it may lead to the waste of

many months or years of research. Detection mechanisms, as the work in [37], could be utilized to identify inconsistency in information. However, some mechanisms are not flexible to be used in large-scale distributed systems, and they lack the support for handling dynamic policy change.

3) Big Data Analytics in Healthcare: Another challenge is utilizing different data formats. Medical data is not uniform. Imaging data comes in all different formats, for example, X-Rays will store differently from MRIs. Moreover, general hospital images are different from specialist hospitals that leverage more complex technology to ascertain more intricate images. Here, it is not easy to ensure data captured is clean, complete, accurate, and formatted correctly for use in multiple systems. Thus, EHRs are less interoperable and not easily deployable as there is no standard data format in the healthcare industry. EHRs require efficient automated or manual updates because medical data change minute-by-minute — this poses challenges in determining how to update quickly without end-user downtime and without slowing the system processes. A series of templates should be developed and included in the system's architecture to create an EHR standard to support an interoperable system. Thus, healthcare systems need integration of healthcare standards data models, such as Health Level Seven (HL7), Fast Healthcare Interoperability Resources (FHIR), or open EHR archetype along with terminologies like SNOMED-CT, to provide timely access to healthcare information, reduce the administrative burden from providers, offer one common integrated system across all care settings, and to seamlessly share data across multiple settings (e.g., OpenHIE and IHE).

Different studies [13][20][38] explore approaches to solving interoperability problems. However, there are difficulties in adopting health standards and tools for adequate data representation (ontologies, databases, clinical models) that ensure healthcare professionals efficiently manage the data, such as:

- Unstructured text fields are not readable to the machines,
- The combination of text fields with health standards was almost unanimous due to a low variety of semantic healthcare web technology,
- The storage solution is related to the type of adopted healthcare standard,
- The usage of use of ontologies impacts the choice of storage solution since querying the ontological structure is language-dependent,
- Data are sometimes not compatible for exchanging information,
- Health and medical concepts and terms used across the organization do not preserve their meaning when externally shared,
- Healthcare applications that use common EHR standards for data sharing might not ensure confidentiality and privacy of patient's sensitive health records that are shared in closed and open networks.

Until information sharing is addressed adequately, poor communication often causes cancellation of procedures, loss of revenue, and inefficient resource utilization. Thus, healthcare organizations need comprehensive auditing and tracking features to guarantee compliance. Organizations need the ability to perform patient record matching, where error and duplicate rates are monitored, and any access to patients' records is detected. Hence, health participants and providers could share sensitive patient data securely within and across systems with the proper information protection strategies. Sharing healthcare information requires different levels of integration within and across organizations. The need for securing EHR differs within the same organization's participants. A dynamic and robust technique should be designed to permit the secured sharing of sensitive health data in the disparate interoperable healthcare domain. According to HealthIT [39], healthcare participants should be provided with self-adaptable services that allow them: to search for and access electronic health information within their workflow, seamlessly integrate electronic data from inside and outside the healthcare system, and set preferences and control how they can share the electronic records, with whom, and for what purposes.

C. Healthcare Registry Management

One of the main information flow between system components is information pathways between hospital care services and specialist consultation. Along the path, different healthcare providers are involved and use different electronic systems, which are also used for different purposes within a single organization. For instance, the municipality uses one electronic medical record system for documentation, while hospitals and primary healthcare services use another. In such cases, various data types are used with no common format for holding it commonly. The information flow among healthcare participants, other organizations, and institutions needs to be organized and visualized so that information can be accessed at any time and in any place.

Due to the lack of integration between various system components, health participants and patients might have limited access and control over the collected data within a registry network. In case registries have been developed and data are collected, it might be challenging to modify the established data collection procedures. A patient's informed consent should allow data to be shared within a registry network. However, if there are established registries at a country or region level, network models might be more efficient in terms of costs and time. These registries are time-consuming and resource-intensive to establish, particularly if large numbers of patients or long-term follow-up data are needed. Moreover, registries using network models might face some additional challenges related to governance, data harmonization, data sharing, and change management. Some registries incorporate information from other data sources, such as electronic health record data.

For multinational registries, linkage and access to other data sources might be challenging due to varying requirements and availability for accessing such sources [14]. Data records that are available in certain countries might be restricted to

particular regions or localities and might be difficult to link with individual patients.

D. Management of Policy Propagation in Multi-Cluster System

Healthcare policy poses rules and complex legal to protect the health of individuals.

Policy rules are associated with policies to data flow steps. Some rules and descriptions are needed to propagate policy, such as a description of policies attached to data sources, a description of data flow (the actions performed on the data), and policy propagation rules (which actions do propagate a given policy). This activity results in many numbers of rules to be stored and managed.

As policies are associated with licenses, a suitable mechanism is required to check the compatibility of licenses and to validate constraints attached to components in a multi-cluster system. Data Hubs are used to collect a large variety of data sources and process them to implement the workflow that connects data in their sources to applications that might exploit these data. These systems create new challenges in terms of the volume of data to be stored and require novel processing techniques such as stream-based analysis to govern data. Assessing what policies propagate from the licenses associated with the data sources to the output of a given data-intensive process is a significant problem. Policy rules could be compressed using an ontology of the possible relations between data entities [22].

However, the ontology matching problem could arise due to finding the semantic mappings between entities of two given ontologies. The coherency check algorithm allows effective reasoning with a compressed rule base but assessing policy rules' coherence demands a partnership between participants of different healthcare sectors and requires cache coherency awareness.

A generic graph matching algorithm is used to match and convert schema into directed labeled graphs and then uses fixpoint computation to determine correspondent entities (nodes) in the graphs. However, the algorithm does not function accurately:

- If there is no label for the graph arcs,
- In case the labels are almost identical, or
- If there are a few levels and most of the relations are associated with the concepts at the top of the graph.

Besides that, several methods [26] are used to enforce information flow policy propagation. Run-time mechanisms that tag data with information flow labels have been employed at operating system and programming language levels. Static analyses have also been developed to ensure that information flow within the system complies with policy rules. The problem of false positives and negatives is less in the case of dynamic analysis because they analyze by running the test cases. However, dynamic analyses are inaccurate as they cannot observe all execution paths. They require a large number of test cases to ensure a certain confidence level in detecting violations and to cover all information pathways. Thus, to guarantee noninterference, the techniques either terminate executions that might release sensitive information or ignore updates that might leak information.

Another method to enforce information flow policy propagation is through a security type system, which enforces security properties within a system application. Hence, the system allows the flow of information for the changed policy if it is type-checked and contains no improper information flow.

Nevertheless, such methods are too strict for use in most real-world applications, such as non-interference policy. Thus, several approaches are proposed to control various policy releases, such as information declassification and formal modeling, so an active attacker might not manipulate the system to learn more secrets than what passive attackers already know. However, the performance of evaluating those approaches is complex in the case of analytical methods or discrete event simulation. Regardless of their dependability on specific commercial-off-the-shelf simulation packages, more invasive revisions of their model are needed, especially with policy changes. Controlling policy change and its versions should contemplate its relations with system configurations and tangled clusters, considering the maximum capacity of the cluster and cost.

E. Information Flow and Policy Change - Monitor

Monitoring information flow and policy change is a way to consider the system state and the execution paths. Here, we should consider the system's current state and the executed paths and non-executed paths to monitor the policy change and ensure that sensitive data will not be revealed to unauthorized parties.

Data label tags and semantic rules could be used to monitor information flow for sequential processes and observe the application's inputs and current values in variables. Each application input receives a tag, which reflects its security level and the current value of the variable. Here, an evaluation of rules is applied to return a value, and a tag is created to reflect both all the previous information flow and the generated one by the evaluation [23].

However, monitoring the information flow of changed policy and its prorogation is challenging in a multi-cluster environment because of the diversity of data structures, various data type formats, dependencies among system components, and the precedence between system components. Here, a directional graph could be used to represent each subject as a node, and the flow of information is represented as a directed edge. The graph could be further refined by using an information flow vector to divide the complex directional graph into sub-layers and quantifying the flow of information [25][26]. An authentication mechanism could be used to compare authenticated credentials to a set of known credentials to determine the access of authorized applications. Nevertheless, massive amounts of data and rules might be generated, aggregated, processed, and stored. Collecting a large variety of data sources, and processing them to implement a workflow that connects data, creates new challenges in terms of the volume

of data to be streamed, analyzed, managed, and stored. Such data could be associated with new rules and constraints that require policy rules to be adaptable to reflect and propagate the new modifications to the system. Hence, it is challenging to develop a monitoring technique that coordinates various monitor instances running locally on the edge gateways and optimizes the communication cost when processing the data while minimizing the overhead of CPU, memory, and network.

Thus, coherency check algorithms, properties matching, static analysis or tag checking algorithms allow practical reasoning about the change of policy rules. However, several challenges have arisen [21][22], such as identifying policy properties to be monitored at different system levels. Changing or updating a piece of data or a policy rule might alter the hierarchical dependency between system components and might affect the flow of information within the system. The situation becomes complicated when hundreds of global regulations, federals, states, and region-specific mandates with too many updates and versions of policies. Every time a policy is impacted by a change in regulation, it goes through a cycle of updates, reviews, approvals, communication, and attestations.

Hence, when changes happen in a policy, the modifications affect the system's participants. Unless new policies become established, organizational performance might be negatively affected as participants become accustomed to new ways of performing tasks or different expectations for personal behavior. An overhead might happen to a system components due to strangulation of the information flow in processes. In such a case, the performance of services, applications, nodes, and communication networks vary significantly depending on runtime variations in running conditions such as availability of resources and the network connection quality between different application components distributed over the Internet. Thus, several factors should be considered during policy change/update, such as hierarchical dependency between system components, the flow of information in processes, the impact of policy changes on the system's properties, and the necessity of the change/update and its relevance.

Monitoring policy at every system's stage helps identify and address problems in information flow pathways. Hence, a systematic and consistent solution is needed to integrate policy change management to be forwarded faster and mitigate compliance risks.

F. Information Flow and Policy Change - Detection

Dynamic detection is a technique that leverages metadata tags to track the information flow and policy change among different entities.

Information flow policies define the authorized paths throughout a system. These policies are designed to preserve confidentiality and integrity of data by associating labels and rules to represent a security class with information and entities containing that information and enforce some rules about the conditions under which data could flow throughout the system.

Several techniques of information flow are proposed to detect policy changes and to analyze them for signs of possible incidents such as violations of security policies or non-acceptable use of policies [21][24][40]. Static and dynamic analysis techniques are used for verifying a program's compliance with information flow policy. However, static analyses are less precise than dynamic analyses, as they consider only the executable flow paths, generate many false positives, and provide no runtime dependency tracking mechanism. Static and dynamic analyses are combined to reduce the false positives and minimize uncertainty within both information flow and policy propagation that could arise due to lack of information, growing scale, and complexity of the data. Thus, machine learning techniques are used to build detection models that characterize the activity of the system's components at runtime [41][42]; however, they require high computational power, and they need to be trained from the beginning if new data arrive.

Hence, examining logs, identifying new rules and labels, and checking tags during runtime are used to simplify detecting illegal information flow and determine policy violations. However, applying those mechanisms to data flow might be a complex process as they often require merging data from disparate sources. Such data merging might cause potential disclosure of sensitive information, data redundancy, lack of interoperability, shortfall of data sharing, workflow interruption, and barriers of interdependency between system's processes. Thus, to tackle those challenges, some factors should be considered, such as: identifying properties that effectively could be used to detect the policy change/update. Here, it is difficult to detect the change in policies because of the dependency between the system's clusters and its components and their impact on the system's constraints and resources. Moreover, the eligibility of policy's change/update during runtime should be checked to prevent illegal information flow to the system's components, as illegal flow might occur even if every access request is authorized.

Because of the complexity of policy's rules change/update, and the varying degrees of security levels between clusters, it is challenging to make these systems secure as security is a crosscutting requirement scattered over distributed clusters. A mismatch or local vulnerability between security mechanisms adopted at different clusters might impact the flow of information between clusters and cause an overall system's performance degradation. Thus, detecting policy change in a distributed system requires keeping track of all processes, rules, and resources and applying an authentication mechanism to each cluster's components.

Here, changing policy rules might allow unauthorized access. Users acquire their necessary permissions by being assigned membership to suitable roles; this might significantly reduce the system's overhead since users with similar access requirements are grouped into the same set of roles, and the requisite permissions are included in those roles. However, in such a system, policy's rules might be restricted to the share of resources, the hierarchical directed or in-directed relationship, and the precedence between multiple distributed clusters. Hence, tags are used to indicate different security policies with different instruction types; however, utilizing tags

might cause a waste of tag storage as

- Tags' size grows with the incremental flow of data,
- Not all data are involved in computing, and
- Many tags might not be used at runtime.

Moreover, different tag propagation and tag check rules might be customized according to corresponding instruction types [24][43]. Here, performance overheads might occur, and the complexity of tag storage might be increased due to the utilization of extra detecting operations. That, in turn, introduced high hardware overhead, high false positives/negatives values, and a lack of flexibility for specific types of policy reconfiguration for different program contexts (e.g., security policy).

Other works, such as in [44], utilized prespecified heuristic rules, which require experts to be defined based on the historical knowledge of system behavior.

Thus, a dynamic approach for managing information flow could be applied to cope with policy changes and eliminate repeated and inefficient flows.

G. Information Flow and Policy Change - Recovery

Healthcare systems recovery is defined as *"the rebuilding, restoration and improvement of the healthcare system's components and its core functions, in alignment with the principles of building sustainable development"* [12].

Healthcare system processes are performed sequentially or simultaneously by various participants within and across the system, and they are organized through several tasks in a workflow. The workflow might be subject to vulnerabilities such as malicious attacks. A malicious attacker might create an illegal task or corrupt a task in the workflow. Such malicious tasks would possibly corrupt data items accessed by some benevolent tasks, or it might trigger other workflow tasks due to dependencies and precedence between them. Moreover, tasks that depend upon malicious tasks might be corrupted and might affect the flow of information within the system.

Some literature studies investigated the recovery from malicious attacks [45]. In such systems, a transaction executed by a malicious attacker might corrupt other transactions in the workflow. Techniques and algorithms are used for assessing and recovering that damage, such as parsing a database log to check which transactions are affected by malicious transactions and undoing/redoing the affected transactions. Store the dependent transactions in separate structures is also applied to preserve a log from being traversed for damage assessment and to be used later for repair. A backup service is utilized as a way of recovery to allow restoring the system's state after a severe attack.

However, such techniques for recovering damage are not adequate for workflows as transactions in a database are independent entities. Hence, a workflow classification is utilized to classify workflow into documents, processes, and system workflows to identify potential types of attacks and to restore the most recent consistent process state after a failure or rollback of inconsistent execution of interrupted tasks [40]. Another recovery way is to resume the execution of the process from the closest consistent point where the attack occurred [46].

A recovery action could be taken on a particular occurrence with an immediate response at the desired state or a set of states to apply a recovery mechanism. Here, the system should calculate its current state and capabilities depending on a set of actions to transition from the current state to the desired one. A resource controller could help assign spare resources to the requesting cluster's components. Once the resources are reserved, the cluster regulates the allocation and reallocation of the assigned resources considering their utility optimization and cost reduction.

Alternatively, a recovery could be made by removing a compromised task from the process, restoring the process to a normal state, cleaning up corrupted data in data memory, and releasing the resources taken by the compromised task.

Hence, for deciding which recovery action to take when a policy change is detected, a mechanism should automatically determine one or more recovery plans based on the type of detected change, considering the control and information flow among tasks across the impacted components in the system. Here, constraints might be applied to choose an alternative recovery action if the immediate previous action failed. In contrast to ranked actions, the execution order is computed dynamically at runtime; however, there are some challenges, such as defining a domain-specific language to describe the capabilities of each component in the system in terms of actions, roles, responsibilities, and information pathways. In such a case, high overhead during runtime might happen due to various constraints on the flow of information across distributed clusters.

Moreover, a deep understanding of the underlying infrastructure is required to develop a recovery-based strategy for determining an optimal recovery plan and recommending a set of successful recovery actions for a given violation. The strategy should consider the system's available resources, allowable information pathways, and regulatory and business constraints (e.g., computational budget). An executable model of a recovery plan could be designed to carry out the recovery in a distributed and coordinated way across various components in the system. Here, the system's resources, status, capabilities, and dependency between components should be considered to check the extent of damage after a failure.

Furthermore, suppose all system policy parties' response ends, and the recovery phase begins. In that case, the consensus of the system's parties might take some time before the recovery transition mechanism and structures are formalized, even if all parties agree that the transition phase has begun.

Ensuring resilient and responsive healthcare systems are vital to achieving the objective of Universal Health Coverage (UHC) Vision 2023, and for advancing progress on the Sustainable Development Goals (SDGs). Hence, creating effective health systems requires well planned and well-implemented recovery strategy.

V. Healthcare Opportunities and Future Research Directions

The Healthcare system is a dynamic environment with significant opportunities such as cost concerns, service quality, uncertainty in new technology, and complexity due to diversity of tasks, diversity of care pathways, lack of sharing, the vulnerability of patients, dependency, and relationships between system's components. The healthcare system aims to improve, secure, and accelerate care services to participants. The following explains the potential opportunities and future research directions in healthcare systems, mainly focusing on information flow and policy change share, security, monitoring, detection, and recovery.

A. Cost Reduction

Several factors could aid in reducing healthcare costs, such as utilizing information technology investments in the healthcare industry to increase profitability, quality of products, and services.

Providing online healthcare services decreases the processing costs of many activities compared with manual handling operations. Such a way might reduce the number of inefficient processes by allowing data sharing across multiple healthcare sectors, pooling the skills and capacities of healthcare participants for problem-solving, contributing to the elimination of mistakes from manual procedures, and reducing the required time for transactions.

Moreover, the cost of components, which are needed to support capabilities such as sensing, tracking, and controlling mechanisms, needs to be relatively inexpensive through utilizing cost reduction strategies (e.g., service standardization, performance tuning). Such strategies could prioritize patients' health while examining opportunities to lower overall costs and increase patient satisfaction.

However, the adaptability of the healthcare system might complicate attaining the goal of reducing the overall cost, as it is prone to inefficiencies such as unnecessary care, waste in healthcare, unwarranted clinical practice variation, administrative burden, and fraud. Thus, cost-containment policies might be applied to target all aspects of the healthcare system, such as prices, volumes, supply, demand, and market processes. An effective financing system should estimate a potential expenditure based on the volume of data and costs and might use the estimation to change the number of funding sources to meet budget constraints across different hospitals.

One of the cost reduction methods in the healthcare system is reassessing the organization's healthcare planning processes to improve accountability and agility of the overall healthcare participants and system's processes. Another way is to use an advanced cost accounting tool (e.g., Activity-based cost analyses, marginal cost analysis, minimum pricing analysis) to drive a deeper understanding of the system's targets and achieve them. Hence, an organization should invest in the healthcare processes to educate healthcare leaders on the usage of advanced cost accounting tools and understand the data.

The healthcare delivery system needs to automate both the connection of healthcare devices and the data centralization to reduce the cost of system management and patient care and to optimize the healthcare system's processes. An autonomous healthcare system could drastically reduce the system's cost management, decrease patient care costs, and improve the system's performance through reallocating resources according to the organization's needs.

B. Healthcare System Services Quality

The quality of healthcare system service affects the satisfaction of healthcare individuals and could increase the likelihood of desired health outcomes. It consists of technical (type of delivered service to a patient) and functional components (service delivery process). These components contribute to healthcare quality and affect the success of its services through (1) providing direct and remote access to health and medical records. (2) Enable automatic data sorting to enhance the generation of information. (3) Reduce medical errors in healthcare services. (4) Analyze causes of a system failure. (5) Effectively communicate and collaborate with other health professionals or institutions. (6) Regular monitoring of the services based on importance and priority. (7) Avoid the suspension of healthcare services. (8) Support standardized treatment policies and protocols that minimize errors. (9) Develop a financing mechanism that supports continuous quality improvement. (10) Enable prevention, detection, and response to health security threats.

To increase the outcomes of healthcare and to minimize resource waste, the quality of healthcare system services should include characteristics such as availability, compatibility, performance, interoperability, accessibility, privacy, confidentiality, accuracy, reliability, and comprehensiveness [15]. The system should allow continuous, convenient, timely access to care services, compliance with clinical practice guidelines, and support continuous monitoring of patient conditions. These lead to accurate and comprehensive patient medical records, which increase the efficiency of diagnosis and treatment services.

Moreover, the ability to exchange and share records across different departments and organizations leads to cost efficiency, effective patient treatment, elimination of redundancy, enhancement of doctor-patient relationships, and enables authorized centralized care coordination to provide access to high-quality people-centered health services.

The quality of healthcare services mainly depends on participants' knowledge and technical skills. Some barriers impact the quality of the healthcare system, such as centralization, bureaucracy, and hierarchical dependency among organization and institution sectors. Such barriers might cause delays in the provision of healthcare services and might lead to a negative perception of the provided service quality in case it is unnecessary by participants.

Thus, the healthcare system should focus on: the design of participants-oriented-service processes, tracking whether the system's policies and processes are being met, and creating

collaborations within and beyond the system. In such case, relational analysis (e.g., grey relational analysis, analytic hierarchy process) [47] could be utilized to improve the quality of healthcare system service delivery and to analyze the relations between system's services.

Furthermore, the quality of healthcare system services could be impacted by a service failure such as a service breach that might affect the service's availability and reliability. The severity of service failure and the occurrence or frequency of failure should be measured to manage and recover the failure according to the health quality and standards (e.g., CAHPS 6.P[48], Six Sigma Healthcare [49]).

Moreover, because of the heterogeneity inherent in services, different participants within the same organization might experience various instances of service failure and its recovery. However, if the service failure is detected early, the system's reliability and participants' satisfaction would be increased. Improving quality of health services requires good communication and collaboration among healthcare providers to provide effective and efficient services and promote shared responsibility to deliver the highest-quality care.

C. Uncertainty in Internet of Healthcare Things (IoHTs)

IoT devices offer opportunities for healthcare provider organizations through providing remote tracking and monitoring to reduce healthcare costs, optimize resources, and provide accurate data collection.

As the number of connected IoT devices grows, the amount of generated data increases and becomes more complex, which requires a mechanism to analyze data and utilize repositories that hold all volumes of information. Thus, healthcare organizations find it challenging to adopt IoT because of:

- The lack of standards and security practices,
- The challenges of integrating data from IoT applications into legacy systems,
- Inadequate privacy regulations,
- The use of expired infrastructure,
- Lack of consensus regarding IoT protocols,
- The high cost of implementing IoT technologies,
- Diversity in devices calculation and communication capabilities, and
- resources constraints.

Several factors might influence the occurrence of uncertainty in IoT, such as:

1) Security and Privacy: Confidentiality and privacy are important concerns in healthcare. Low security and misconfigured device and network settings could affect patients' privacy and their data. The use of various providers mandated to submit confidential data to law enforcement agencies, this could affect the adoption and use of the technology. The networks that transmit data are often highly heterogeneous and are frequently managed by third parties, which makes the protection of security and privacy and governance of this data even more challenging. Moreover, an organization could identify risks associated with IoT devices and should preauthorize the security team to help remove vulnerable devices from the network during attacks. It could be aware of all assets that can impact the security of the healthcare IoT network such as limit access to the IoT network, separate network segment for IoT devices, encrypt the network, protect the data, ensure and manage the communication of authorized devices.

2) Hardware and Software Failures: Hardware and software failures might put healthcare tasks at risk, as a delay might occur to one or more processes, which might propagate to the entire workflow. As a result, multiple devices might not work well together, or the functionality of devices produced by different manufacturers might have varying characteristics. In such a case, a security breach in IoT might occur and leak personal information to unauthorized participants or a device malfunction. Furthermore, with different hardware solutions, the software has to be timely updated to a safely stay at its latest version and allows the aggregation of data from various devices. Such constant updates require lots of effort and might spawn many technical issues. Hence, policy should strengthen current requirements for data exchange among electronic health records, the emerging IoT devices, and solutions. It might maintain an inventory of all healthcare systems connected to the network so that organization could quickly identify, and address risks associated with IoT devices.

3) Devices Resources Constrains: In healthcare, many devices are connected, producing a massive amount of data and information, which might affect the computational and processing capabilities of devices. Offloading could be utilized to partition and execute tasks between devices and edge nodes to minimize energy consumption [50]. A mathematical programming-based framework is utilized to allocate tasks while satisfying operational constraints optimally [51]. However, those ways focus on optimizing limited system parameters (e.g., processing capacity and network bandwidth, and couldn't handle the dynamic nature of policy change.

4) Interoperability and Devices Heterogeneity: Many devices now have sensors to collect data and often communicate with a server in their language. Each manufacturer has its proprietary protocol, which means sensors made by different manufacturers cannot necessarily communicate with each other. Device management requires directories of devices' functionality, protocols, terminologies, and standards compliance. Interoperability is a significant challenge in creating medical devices that easily connect with other devices and sensors to health providers' electronic medical record systems. However, it takes time to corroborate such a massive amount of data with the different terminologies and standards on every system and might even yield inaccurate results. Moreover, current health standards are challenging to use due to the lack of adequate code for electronic medical records and because they describe fixed timing of examination results, not being a sequence of patient episodes. Thus, migrating to more interoperable technical solutions should ensure continuous and uninterrupted services and provide universal guidelines on the consistency and agreement of data in a format, queries, and synchronization. The solution should support workflow consistency in how technology helps decision support, clinical

guidelines, rules, and user interfaces. It should provide an approach that deals with different device calculation and communication capabilities to share, understand, interpret and use data without ambiguity. The solution should use low-cost interfaces [52] and open APIs (such as HL7 and FHIR) to solve the usability and cost issues as they distinctly define security mandates and transmission protocols which lower the risk of errors and have real-time ability to share and access data.

D. Enhance Healthcare Services Security - Blockchain

The healthcare system involves many processes such as emergency department operations, managing finances, and patient transfers to different facilities. Such processes constitute one or more workflows, which might involve repetitive tasks related to one or more aspects (e.g., patient transfers can be plotted out as a series of conditional tasks). To provide better internal controls that minimize risks, eliminate workflow cycles, and reduce overhead, the healthcare system focuses on protecting its processes and services against unauthorized access, hardware theft, data manipulation, and common threats and exposures. Thus, rules and principles are enforced to regulate the access and transmission of data to healthcare participants and providers. Here, blockchain techniques (e.g., public, private, hybrid, and consortium) appeared to provide a secure, authentic, and transparent distributed technology that could integrate the healthcare system's services from multiple nodes in the blockchain network to enhance their computation, storage, and transactions processing. Furthermore, it provides:

- Better healthcare data-sharing,
- Assists in the diverse use cases of healthcare,
- Trace data shared within and across a business network to provide well-controlled privileges to healthcare participants.

To safely exchange healthcare information between authorized participants, blockchain-oriented platforms [53], and blockchain models [54] could be used to evaluate healthcare data sharing requirements in different sources, validate data accuracy and patient engagement, and improve the dissemination of accumulated information in a secure, interoperable environment. Other models [55][56] are used to evaluate the performance of new patient block components and system configurations, improve data accessibility between healthcare providers, and provide a secure runtime monitoring system. Such a system enables healthcare participants to track the healthcare status of their patients remotely while safely maintaining the latest history of patients. Here, authorized participants only could view patients' identities within the authorized network. A hyperledger platform [55] is one of the techniques that could be used to provide patient-controlled healthcare data management.

To protect patients' sensitive data from being tampered with and to eliminate the cascading of malicious behavior to the overall system, digital signature introduces another level of authenticity. It uses a cryptographic operation that binds the signature and the signed data by adopting the idea of the Public Key Infrastructure (PKI) feature. A unique digital signature is issued to lock the data and prevent any additional signatures, annotations, or data fill-ins.

Another way is to use smart-contract-enabled blockchains [56] like Ethereum to create digital currencies (tokens), which could remotely monitor the healthcare system, and securely identify, authenticate, and authorize system participants. Here, smart-contract might be utilized to create representations of existing health and medical records that are stored within individual system components. The contract might contain records of metadata ownership, permissions, data integrity, relationships, and state transition functions to carry out policies and enforce a set of rules regulating specific records access.

Hence, blockchain allows the distribution of EHRs among different health care sectors to manage patient-sensitive information through several nodes of an interconnected network. However, correctly arranging the gathered data and defining their dependency and precedence in a blockchain network are problems due to the existence of private transactions and the concept of cryptographic protocols that allow private calculation of encrypted transactions to be accessible into the blockchain. Thus, blockchain healthcare technologies could optimize system performance while retaining small processing and computation capabilities for data representation. Moreover, the most promising applications of blockchain in healthcare are for dynamic patient consent and identity management. However, to enhance the healthcare sector, the healthcare applications need to support big data scalability to deal with the massive amount of health data, cross-border health data, and their policies. As the volume of data and transactions increases, a mechanism is needed to minimize the delay of storing and processing massive data access transactions considering the incomplete and missing data provided.

E. Improve Healthcare System Recovery

The ultimate goal of healthcare system recovery is to design a system that can respond to the dynamic demands, perform its functions effectively and sustainably, increase health systems resilience, and mitigate the risk of future healthcare policy change. Health system recovery is determined or influenced by the typology of emergency care. Hence, to understand the system's processes and its tasks, it is mandatory to understand the need for recovery and the emergency of recovery to develop a recovery plan. The recovery might be based on restoring the system to a specific point while investing in risk reduction and strengthening preparedness for future hazards.

To enhance the healthcare system, some critical elements for enhancing the system's recovery could include:

1) Recovery Duration: Some criteria could be used to assess the phase of recovery, such as urgency, sustainability, and cost-effectiveness of the tasks being carried out. Recovery duration is another criterion that could impact the recovery phase. Once the initial recovery has been carried out, other residual or outstanding activities could be integrated into subsequent standard planning mechanisms. The duration of the recovery phase could be a short-term or long-term recovery.

However, differences in the types and evolution of emergencies might increase due to an overlap between the two phases and emergency response and recovery. Thus, dividing the recovery process into phases is essential to facilitate standardization and harmonization.

2) Recovery Conflicts: Conflicts are typically protracted, and there might be an assortment of health participants with different degrees of legitimacy from different organizations. When multiple participants are involved, recovery might be delayed, and efforts could be duplicated as recovery from conflicts passes through a long process of restoring the capacity of the health system's components and core public health functions. The process includes restoring the government and communities' capacity to rebuild and recover from crises and preventing relapses. Moreover, a system with various resources, capacities, and capabilities of its participants' should be supported by a government throughout each recovery phase to avoid recovery conflict within and across the healthcare organizations. Although it is critical to have a concerted health sector recovery mechanism led by a government to focus on funding and resources, a complete understanding of the process is necessary to distinguish between conflict and non-conflict-related emergencies.

3) Up-To-Date Recovery Mechanism: Hence, self-healing systems could be adopted to take corrective recovery actions and trigger an alert if a system does not satisfy constraints while identifying lessons learned from healthcare members to support future recovery. Thus, to meet recovery objectives, developing a recovery plan should support dynamic monitoring tools and evaluation mechanisms to measure the progress of the recovery process and its outcomes. The plan might identify funding sources for an early recovery plan and provide a recovery strategy with contingency plans for different scenarios. The development of a recovery strategy and plan should be based on the results of the recovery assessments. Thus, a recovery mechanism should adapt to the new integration principles to ensure that the recovery is aligned with national priorities across healthcare sectors to manage unavoidable trade-offs between short and long-term recovery priorities and economic and environmental policy goals. The recovery mechanism should ensure that the recovery responsibilities, including financial requirements and policy arrangements, are transferred to support the recovery phase. In conjunction with the recovery process, an assessment of post-recovery is needed to determine the overall recovery funding needs. Thus, adapting public financial management systems could support the government and provide international best recovery practices. The recovery mechanism should adapt to the new health sector recovery roles, responsibilities, and priorities, including those of the municipality, the district private health sector, and partners. The recovery action should consider the coordinated entities within and across the organizations, even with prior regulations, strategies, mechanisms, and platforms.

4) Recovery Consistency: A consistent recovery between healthcare system organizations and their participants helps meet their perspective needs. The coordination and definition of roles and responsibilities during recovery should be supported by national legislation or a memorandum of understanding before a recovery mechanism formalizes the roles or before the failure spreads to the whole system. The recovery mechanism should be confirmed with health sector partners to be used for consulting stakeholders on the draft recovery plan. The mechanism should provide a recovery guide for the use of stakeholders to identify priority health sector repairs with partners. The mechanism should allocate the cost and time of immediate recovers required for the system. During this period, a cost indemnity agreement should be designed and agreed upon within and across healthcare organizations to guarantee immediate recovery action.

5) Seamless Communication and Collaboration: As healthcare is a tangled system with multiple participants and protocols, data-sharing protocols and agreements should be developed by organizations that have access to and stewardship of required data. The recovery mechanism should consider the variety of data-sharing protocols and agreements to facilitate communications and collaboration and support real-time information flows between and among health organizations. The mechanism should ensure consistent and up-to-date repair to reduce duplication [16]. A gap evaluation analysis is required to assess system capacity and capability to meet recovery objectives and identify the differences between the current state of the system and the desired one. The mechanism should re-assess the initial needs and the recovery plan (inputs, outputs, results), modify the process as required by results, and disaggregate the indicators under observations. A recovery index of health organizations (e.g., WHO and PAHO recovery health index) could be used to assess the impact of recovery on the system and provide oversight over health and safety guidelines to repair the healthcare infrastructure. The recovery should be related to the system's architecture. Here, a systematic way could be developed to provide a sound basis for making objective decisions about design trade-offs and to enable accurate predictions about the system's capabilities and qualities free from bias and hidden assumptions.

F. Develop Dynamic Monitor for Healthcare Information Flow and Policy Change

Continuous monitoring of the health system's services helps identify bottlenecks in information flow. Such bottlenecks could cause delays, overload, and blockages in workflow processing, leading to dissatisfied health participants, loss of revenue, time, and wasted resources. Continuous monitoring creates a vast bulk of data that requires an expert system to perform analysis and processing dynamically.

To monitor the change within policy and control its impact on information flow, the interaction and the communication mechanisms of persistent data, processes, and sub-process should be analyzed and presented in various visual formats and charts. Current monitoring tools cannot provide information about patient health status, and they do not visualize all the recorded data on the same platform [23][57][58].

Furthermore, determining which system's service is not satisfactorily performing could make better decisions about reconfiguring components, services, and resources to run processes more smoothly. Heterogeneous computing resources should be reconfigured and scaled according to the monitoring data in a distributed environment. Here, system components and services might contain some redundant processes and dependencies, which introduce noise in a workflow that adversely impacts the performance of inline and real-time system analysis. Thus, noise reduction at the process level could be used to reduce computational complexity and achieve better system performance.

Hence, monitoring could be carried out at different system levels to provide continuous information flow monitoring with the policy rules that might change over time and incorporate every change into the system without causing service interruption. A notification also might be triggered for any workflow processes that might conflict with given policy rules without re-analyzing the whole workflow. Thus, the monitor mechanism should:

- Distinguish the discrete processing stages within the processes.
- Describe the information flow mechanism through a system.
- Characterize the type of data items that flow through the processes.
- Identify violations within information flow and policy rules.
- Find locations for inserting data validation monitors, insert data collection points for later analysis, and distinguish between data dependencies and control dependencies.

A monitor system should consider a real-time wireless transmission connection between the monitoring tool and the monitored device to improve the monitoring accuracy. Monitoring properties associated with a potential risk prediction should be further analyzed to overcome challenges such as unpredicted faults, massive data streaming, and detection accuracy. The amount of collected data from monitored properties is large and intractable. Hence, it is required that the monitoring system distinguishes between health degradation and faulty measurements.

G. Continuous Detection for Healthcare Information Flow and Policy Change

Detection is the process of comparing current normal processes with the observed ones to identify significant deviations. In such a case, policy properties (point-method) could be identified in the monitored data and the information flow, or a score (likelihood-ratio-method) could be associated with the arrived data to indicate how likely there is a change in the policy. In both methods, the main goal is to reduce detection delay.

Furthermore, label-method might be used to detect the policy change for each component in the system. However, in a dynamic multi-cluster environment, statistical methods do not provide accurate results due to the regular update of the system's processes and policy rules. They are ineffective in detecting real-time noise changes given limited information flow.

Here, multiple components could be existed within each cluster in a system, along with dependencies and precedence among them. In such a system, detecting the change in policy rules might be difficult because all the flow of information and processes among components should be understood according to the updated policy. Thus, continuous policy change within and across such a hierarchical system requires a complete understanding of policy rules and needs to trace executed and non-executed paths of information flow and processes. Hence, a detection mechanism might be trained with sufficient behavioral and temporal features, work on each sub-process, and decide whether a policy is changed to avoid policy conflict and prevent the system's workflow delay or bottleneck. According to [16][59], the detection mechanism should:

- Minimize the detection errors to provide an efficient system that can be managed remotely.
- Support low computational complexity and few amounts of memory to store training data.
- Be practical in health and medical applications to reduce redundancy within the monitored parameters.
- Classify different types of policy change based on the measured time series (e.g., regular time change, noisy time change, short time change, long time change).

Moreover, the detection mechanism should be self-adaptable to deal with dynamic changes within policies during runtime, identify relevant changes, and compare policies across and within a system. Once the change is detected, the mechanism might give a participant the ability to modify the information flow or policy rule during runtime and choose whether to continue, alternate, or abort the execution of a process. The detection should help spread the approved policy change to the rest of the system, considering the consent of its participants without causing policy conflict. For example, patients might enter personal information into a system to know whether or not they can get a refund for a surgery. The system provides only a refund for a specific type of surgery. When the system's policy rules change to incorporate other types of surgeries, the system should automatically update the rules and incorporate the changes without affecting the system's flow of information and processes.

H. Policy of Data Sharing and Consent

In a healthcare system, the change in data collection and the usage practices require the respective policy to be revised and updated to reflect that change. In such a case, the system participant's consent is taken to be able to gather and process the collected data. Hence, a policy should explain the implications of granting or withholding consent to the participants so that data could be gathered and shared safely between authorized participants across and within systems. Thus, the data sharing and consent policy should consider:

1) Comply With Standards: Data sharing of healthcare participants should comply with legal requirements and security standards (e.g., ISO 27001, ISO/TC 215, ISO/TS 1360, ISO/IEC 29100). Data sharing might require knowledge of data formats, methods for securing data from malicious attacks, knowledge of available data management tools and software, and a complete understanding of the used applicable regulations and consent models. Thus, formal and comprehensive information security policies with respective implementation guidelines should be adopted to cover information security, access to information and systems, application security, information classification, and related security standards. The data sharing policy should provide guidelines, including constraints of regulatory requirements on when specific access conditions should be implemented.

2) Policy Conflict Management: Policy conflicts could arise due to conflicting requirements related to policy changes. Here, participants have to understand the updated policy to understand the changes, which is a complicated task. Thus, most system participants cannot make informed decisions about their privacy. Hence, analysis techniques (e.g., network analysis) [60][61] are used to explore the structural features of data sharing policy, map their relationships, and minimize the delay cost of sharing data within a system. However, network construction in healthcare systems might be complex and time-consuming due to the time required to analyze various activities, processes, sub-processes, and resource constraints within the system. The main challenge relies on the variety of policy representation forms at different levels of the hierarchy converted later to different forms for processing, which add complexity to the system structure and lead to inefficiency concerns.

One way to handle the conflict is by utilizing static conflict detection methods [62] to explicitly detect conflicting rules, compare all the paired rules, and analyze the conflicting probability of each pair of policy rules. However, this way is not affected as with the increasing number of rules in healthcare; the detection becomes inaccurate because of the increasing size of the policy rules set.

Another way is to classify policy rules into a classification tree [63] to detect the conflict by checking the conflict between nodes and their inherited rules. Nevertheless, this way consumes more memory, time, and space. It is less appropriate for a system that needs to predict continuous change. Moreover, the reproducibility of a tree is exceptionally sensitive as a slight change in policy rules could bring an enormous change in the tree structure.

A quantitative method using a linear combination of policy change is used [64][65]. The method further abstracted policy into a simple one and used a correlation matrix to detect the conflict according to the matrix. However, this method is not suitable for the dynamic nature of healthcare policy change as the size of the matrix depends on the number of rules; hence it is not suitable for a large number of rules.

Machine learning techniques (e.g., gossip learning technique, federated Learning algorithms, deep neural network) addressed the dynamic policy change challenge [66]–[68]. Here, performance and convergence scale degradation might happen because of the frequent change in policy and a lack of communication in healthcare, which results in an overfitting model. Moreover, such techniques under specific communication topologies could substantially impact the model's convergence speed in a decentralized environment when the speed is correlated with the data distribution. The training and execution of these models require extensive computational resources [61] which could not be used in limited environments with minimal performance.

Thus, there is a need to have standardization for data formats, existing protocols, and algorithms to enhance the reliability, interoperability, and modularity of the healthcare system and its components.

3) Data Sharing Cost: Sharing data accelerates health service delivery and promotes data reuse between healthcare participants. Here, healthcare participants' have preferences to share data within and across the systems in a distributed environment, which leads to an overload at the workflow and system levels. Such overload might cause a delay in data sharing among the system's participants and might increase the cost of sharing, including the time spent on a specific process to share the data (e.g., reviewing and analyzing data).

Furthermore, the cost of data sharing might be impacted by the dynamic change in the system's processes and information flow. Thus, the cost of sharing should be included in the policy. The cost should consider the time spent on an activity specific to sharing and reviewing data. The data sharing policy should enclose other costs such as hardware, software, data storage, and staff expenses, including a description of data charges, if any, and how these are calculated. The policy should address the requirements for metadata standard (e.g., HL7 Functional Model for EHRs) that varies by a health organization, considering the cost of storage, data access, and data management plan.

4) Automated Policy Compliance: An automated method could be applied to detect data change policy based on identifying and extracting the policy changes by considering precedence, relationships, and dependencies between policies to resolve the conflicts. The method could provide a self-adaptive mechanism that automatically adapts the updated policy to new data descriptions, rules, and regulations. The adaptive mechanism ensures that participants' rights and preferences are protected as their data are being shared in a distributed environment. Such a method could be promoted through pilot initiatives and ad-hoc regulatory guidance, which enable case-by-case deliberations throughout the diverse data types, and the various uses of data. Moreover, the changes in data sharing policy could be classified further to describe the severity levels that reflect the impact of changes on participants' privacy, policy consent, and data quality. The adopted method could be scalable to deal with the increasing data capacity and provide privacy-preserving data sharing across and within systems. Moreover, it could support various versions of data, provide different levels of data access depending on the version, and

determine the best method of data sharing policy to ensure that system participants could use the data and prevent confusion, misuse, and misinterpretation.

VI. Conclusions

Real-world digital healthcare systems are complex, hierarchical, and decentralized. In such systems, communications, dependency, precedence, and information shared between system clusters and their components, might be impacted by changes in the policies that govern allowed data flows within the system. Here, many barriers might strangulate the information flow and drastically impact the overall system's performance. Managing information flow and policy change in such an environment generates massive amounts of data that need to be aggregated, processed, and stored. At the same time, optimizing the communication cost when processing the data should be considered while minimizing the overhead in terms of CPU and Memory. The paper provided a technical view of the challenges, opportunities, and future research direction of the information flow and policy change/update in healthcare systems.

References

[1] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *International Journal of Surgery*, vol. 88, no. April 2021, pp. 105906, 2021.

[2] F. Chaib and P. Garwood, "WHO releases first guideline on digital health interventions, 2019. [Online]. Available: https://www.who.int/news/item/17-04-2019-who-releases-first-guideline-on-digital-health-interventions. [Accessed: June 2022].

[3] Humanitas Group, "The timeline of digital health - Hunimed, 2022. [Online]. Available: https://www.hunimed.eu/news/the-timeline-of-digital-health/. [Accessed: June 2022].

[4] S. Kraus, F. Schiavone, A. Pluzhnikova, and A. C. Invernizzi, " Digital transformation in healthcare: Analyzing the current state-of-research," *Journal of Business Research*, vol. 123, no. February 2021, pp. 557–567, 2021.

[5] R. Sharma, and N. Kshetri, "Digital healthcare: Historical development, applications, and future research directions," *International Journal of Information Management*, vol. 53, no. August 2020, pp. 102–105, 2020.

[6] M. Senbekov *et al.*, "The recent progress and applications of digital technologies in healthcare: a review," *International Journal of Telemedicine and Applications*, vol. 2020, no. October 2020, pp. 1–18, 2020.

[7] Y. C. Lu, Y. Xiao, A. Sears, and J. A. Jacko, "A review and a framework of handheld computer adoption in healthcare," *International Journal of Medical Informatics*, vol. 74, no. 5, pp. 409–422, 2005.

[8] J. A. Powell, M. Darvell, and J. A. M. Gray, "The doctor, the patient and the world-wide web: how the internet is changing healthcare," *Journal of the Royal Society of Medicine*, vol. 96, no. 2, pp. 74–76, 2003.

[9] B. Müller, "Health and Care Futures Technology futures ," *Securing the future*, vol. 1, no. 1, pp. 1–26, 1999.

[10] H. S. Kim, I. H. Kwon, and W. C. Cha, "Future and Development Direction of Digital Healthcare," *Healthcare Informatics Research*, vol. 27, no. 2, pp. 95–101, 2021.

[11] World Health Organization, "Global strategy on digital health 2020-2025, 2021. [Online]. Available: https://apps.who.int/iris/handle/10665/344249. [Accessed: June 2022].

[12] World Health Organization and Regional Office for the Eastern Mediterranean, *Implementation guide for health systems recovery in emergencies: transforming challenges into opportunities*. IGO Publishing, 2020.

[13] C. Marcos, A. González-Ferrer, M. Peleg, and C. Cavero, "Solving the interoperability challenge of a distributed complex patient guidance system: a data integrator based on HL7's Virtual Medical Record standard," *Journal of the American Medical Informatics Association: JAMIA*, vol. 22, no. 3, pp. 587–599, 2020.

[14] M. B. Leavy and OMI, "Multinational Registries : Challenges and Opportunities," *Addendum to Registries for Evaluating Patient Outcomes: A User's Guide. 3rd ed. Rockville, MD: Agency for Healthcare Research and Quality*, vol. 3, no. February 2018, pp. 1–19, 2018.

[15] WHO and WORLDBANKGROUP, *Delivering Quality Health Services: A Global Imperative*. OECD Publishing, 2018.

[16] R. WHA74, "Strengthening WHO preparedness for and response to health emergencies," *Seventy-fourth World Health Assembly*, vol. 31, no. May 2021, pp. 1–14, 2021.

[17] Health IT, "What is an electronic health record (EHR)?, 2019. [Online]. Available: https://www.healthit.gov/faq/what-electronic-health-record-ehr. [Accessed: June 2022].

[18] C. Kirchberger, "Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of crossborder eHealth," *arXiv preprint arXiv:2108.04087*, vol. 22, no. July 2014, pp. 1–65, 2015.

[19] A. Kneck, M. Flink, O. Frykholm, M. Kirsebom, and M. Ekstedt, "The information flow in a healthcare organisation with integrated units," *International Journal of Integrated Car*, vol. 19, no. 3, pp. 1–10, 2019.

[20] M. J. A. Salomi and P. B. Claro, "Adopting Healthcare Information Exchange among Organizations, Regions, and Hospital Systems toward Quality, Sustainability, and Effectiveness," *Technol Invest*, vol. 11, no. August 2020, pp. 58–97, 2020.

[21] M. Hicks, S. Tse, B. Hicks, and S. Zdancewic, "Dynamic Updating of Information-Flow Policies," *Proceedings of the International Workshop on Foundations of Computer Security (FCS)*, vol. 20, no. June 2005, pp. 7–18, 2005.

[22] E. Daga, A. Gangemi, and E. Motta, "Reasoning With Data Flows and Policy Propagation Rules," *Semantic Web*, vol. 9, no. 2, pp. 163–183, 2018.

[23] G. L. Guernic and T. Jensen, "Monitoring Informa-

tion Flow," in *Workshop on Foundations of Computer Security-FCS'05*, 2006, no. May 2006, pp. 19–30.

[24] K. Chen, X. Guo, Q. Deng, and Y. Jin, "Dynamic Information Flow Tracking: Taxonomy, Challenges, and Opportunities," *Micromachines*, vol. 12, no. 8, pp. 1–16, 2021.

[25] M. Aydar, "Developing a Semantic Framework for Healthcare Information Interoperability," Ph.D. dissertation, Dept. Computer Science, Kent State Univ., Kent., 2015.

[26] S. H. Han, A. Nasridinov, and K. H. Ryu, "Information Flow Monitoring System," *IEEE Access*, vol. 6, no. May 2018, pp. 23820–23827, 2018.

[27] G. Michael, "Trust, Authority, and Information Flow in Secure Distributed Systems," Ph.D. dissertation, Faculty of the Graduate School, Cornell Univ., NY., 2020.

[28] B. Juliana, T. Webber, B. Euan, and V. Andreas, "A blockchain-based healthcare platform for secure personalised data sharing," *Public Health and Informatics: Proceedings of MIE*, vol. 31, no. May 2021, pp. 208–212, 2021.

[29] L. Tian, C. Pin, and S. K. Ting, "Blockchain-Based Healthcare Information Preservation Using Extended Chaotic Maps for HIPAA Privacy/Security Regulations," *Applied Sciences*, vol. 11, no. 22, pp. 1–16, 2021.

[30] M. K. Elghoul, "A Review of Leveraging Blockchain based Framework Landscape in Healthcare Systems," *International Journal of Intelligent Computing and Information Sciences*, vol. 21, no. 3, pp. 71–83, 2021.

[31] F. T. Lee, P. I. Chang, and S. T. Kung, "Blockchain-Based Healthcare Information Preservation Using Extended Chaotic Maps for HIPAA Privacy/Security Regulations," *Applied Sciences*, vol. 11, no. 22, pp. 10576, 2021.

[32] A. C. Myers and B. Liskov, "Protecting Privacy Using the Decentralized Label Model," *ACM Transactions on Software Engineering and Methodology, TOSEM*, vol. 9, no. 4, pp. 410–442, 2000.

[33] S. Mondal, and m. Nandini, "An efficient reachability query based pruning algorithm in e-health scenario," *Journal of Biomedical Informatics*, vol. 94, no. 1, pp. 103171, 2019.

[34] G. T. Nguefack, "Using bayesian networks to model hierarchical relationships in epidemiological studies," *Epidemiology and health*, vol. 33, no. June 2011, pp. 1–8, 2011.

[35] J. Rodon, and S. Leiser, "Exploring the formation of a healthcare information infrastructure: hierarchy or meshwork?," *Journal of the Association for Information Systems*, vol. 16, no. 5, pp. 1–43, 2015.

[36] C. Diana, and M. A. Martins, "Inconsistencies in health care knowledge," *IEEE 16th International Conference on e-Health Networking, Applications and Services Healthcom*, vol. 16, no. October 2014, pp. 37–42, 2014.

[37] R. Cruz-Correia *et al.*, "Automatic detection of patient data inconsistencies on integrated Health Information System," Ph.D. dissertation, Faculty of Medicine, Porto Univ., Porto., 2006.

[38] N. Angula and N. Dlodlo, "Towards a framework to enable semantic interoperability of data in heterogeneous health information systems in Namibian public hospitals," *Advances in Intelligent Systems and Computing*, vol. 721, no. January 2018, pp. 835–845, 2018.

[39] Health IT, "Health Interoperability 2030: Individual and Care Delivery Experiences, 2021. [Online]. Available: https://www.healthit.gov/topic/interoperability/health-interoperability-outcomes-2030. [Accessed: June 2022].

[40] Y. Wu, G. X. Yuan, and K. L. Ma, "Visualizing Flow of Uncertainty Through Analytical Processes," *IEEE Transactions on Visualization and Computer Graphics*, vol. 18, no. 12, pp. 2526–2535, 2012.

[41] Q. V. Dang, "Studying Machine Learning Techniques for Intrusion Detection System," in *International Conference on Future Data and Security Engineering*, 2019, pp. 411–426.

[42] Y. C. Chen, Y. J. Li, A. Tseng, and T. Lin, "Deep Learning for Malicious Flow Detection," *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, vol. 2017, no. October 2017, pp. 1–7, 2018.

[43] M. Tiwari *et al.*, "Complete information flow tracking from the gates up," *Proceedings of the 14th International Conference on Architectural Support for Programming Languages and Operating Systems*, vol. 37, no. 1, pp. 109–120, 2009.

[44] M. Shana *et al.*, "Dynamic Information Flow Tracking for Detection of Advanced Persistent Threats: A Stochastic Game Approach," *ArXiv*, vol. abs/2006.12327, no. June 2020, pp. 1–15, 2020.

[45] P. Ammann, S. Jajodia, and P. Liu, "Recovery From Malicious Transactions," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 5, pp. 1167–1185, 2002.

[46] J. Eder and W. Liebhart, "Workflow Recovery," *Proceedings - 1st IFCIS International Conference on Cooperative Information Systems, CoopIS*, vol. 19, no. June 1996, pp. 124–134, 1996.

[47] E. Aydemir and Y. Sahin, "Evaluation of Healthcare Service Quality Factors Using Grey Relational Analysis in a Dialysis Center," *Grey Systems: Theory and Application*, vol. 9, no. 4, pp. 432–448, 2019.

[48] Agency for Healthcare Research and Quality, "The CAHPS Ambulatory Care Improvement Guide: Practical Strategies for Improving Patient Experience, 2020. [Online]. Available: https://www.ahrq.gov/cahps/quality-improvement/improvement-guide/improvement-guide.html. [Accessed: June 2022].

[49] A. Niñerola, M. V. María-Victoria, and H. L. Ana-Beatriz, "Quality improvement in healthcare: Six Sigma systematic review," *Health Policy*, vol. 124, no. 4, pp. 438–445, 2020.

[50] L. Liqing, C. Zheng, and G. Xijuan, "Socially aware dy-

namic computation offloading scheme for fog computing system with energy harvesting devices," *IEEE Internet Things*, vol. 5, no. 3, pp. 1869–1879, 2018.

[51] S. Souravlas, and K. Stefanos, "Scheduling fair resource allocation policies for cloud computing through flow control," *Electronics*, vol. 8, no. 11, pp. 1348, 2019.

[52] Vigyanix, "Mirth Connect Series: Introduction, 2010. [Online]. Available: https://vigyanix.com/blog/mirth-connect-series-introduction/. [Accessed: June 2022].

[53] S. Jiang *et al.*, "Blochie: A Blockchain-based Platform for Healthcare Information Exchange," in *IEEE International Conference on Smart Computing, SMARTCOMP*, no. May 2019. IEEE, 2019, pp. 49–56.

[54] P. Pandey and R. Litoriya, "Implementing Healthcare Services on a Large Scale: Challenges and Remedies Based on Blockchain Technology," *Health Policy and Technology*, vol. 9, no. 1, pp. 69–78, 2020.

[55] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-Based Electronic Healthcare Record System for Healthcare 4.0 Applications," *Journal of Information Security and Applications*, vol. 50, no. February 2020, p. 102407, 2020.

[56] K. N. Griggs *et al.*, "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring," *Journal of Medical Systems*, vol. 42, no. 7, pp. 1–7, 2018.

[57] H. A. El Zouka and M. M. Hosni, "Secure IoT Communications for Smart Healthcare Monitoring System," *Internet of Things*, vol. 13, no. February 2021, pp. 1–14, 2021.

[58] J. Kharel, H. T. Reda, and S. Y. Shin, "An Architecture for Smart Health Monitoring System Based on Fog Computing," *Journal of Communications*, vol. 12, no. 4, pp. 228–233, 2017.

[59] Deloitte, "2022 Global Health Care Outlook Are we finally seeing the long-promised transformation?," *Deloitte Global Health*, vol. 4, no. 2022, pp. 1–52, 2022.

[60] R. Khelf, and N. Ghoualmi, "Intra and inter policy Conflicts Dynamic Detection Algorithm," *Seminar on Detection Systems Architectures and Technologies DAT*, vol. 1, no. February 2017, pp. 1–6, 2017.

[61] O. Salem, Y. Liu, M. Ahmed, and B. Raouf, "Online anomaly detection in wireless body area networks for reliable healthcare monitor," *IEEE journal of biomedical and health informatics*, vol. 18, no. 5, pp. 1541–1551, 2014.

[62] E. Syukur, S. W. Loke, and P. Stanski, "Methods for policy conflict detection and resolution in pervasive computing environments," *Policy Management for Web workshop in conjunction with WWW2005 Conference*, vol. 14, no. May 2005, pp. 13–20, 2005.

[63] L. Xueting, "A Method of Conflict Detection for Security Policy Based on B+ T," *IEEE Fourth International Conference on Data Science in Cyberspace DSC*, vol. 4, no. June 2019, pp. 466–472, 2019.

[64] X. Yuping, and W. Shengli, and Y. Zhan, "Statistical analysis of the linear combination method," *Journal of Computational Information Systems*, vol. 11, no. 18, pp. 6615–6620, 2015.

[65] J. Malczewski, "On the use of weighted linear combination method in GIS: common and best practice approaches," *Transactions in GIS*, vol. 4, no.1, pp. 5–22, 2000.

[66] L. Giaretta, "Pushing the Limits of Gossip-Based Decentralized Machine Learning," Master thesis., School of Electrical Engineering and Computer Science, KTH., Sweden., 2019

[67] R. Miotto, F. Wang, S. Wang, X. Jiang, and J. T. Dudley, "Deep learning for healthcare: review, opportunities and challenges," *Briefings in bioinformatics*, vol. 19, no. 6, pp. 1236–1246, 2018.

[68] A. A. Abdellatif *et al.*, "Reinforcement Learning for Intelligent Healthcare Systems: A Comprehensive Survey," *arXiv preprint arXiv:2108.04087*, vol. 1, no. August 2021, pp. 1–31, 2021.