2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) | 978-1-6654-6297-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927701

Towards a Patient-Centered Virtual Hospital Ecosystem: A Fine Grained VHealth-AC Model for Hospitals' Legacy Information Systems

1st Sara A. Alsalamah
Department of Computer Science
Virginia Tech
Falls Church, VA, USA
salsalamah@vt.edu
College of Computer and Information Sciences
Imam Mohammad Ibn Saud Islamic University
Riyadh, KSA
saialsalamah@imamu.edu.sa

2nd Shada AlSalamah
College of Computer and Information Sciences
King Saud University
Riyadh, KSA
saalsalamah@ksu.edu.sa
Department of Digital Health and Innovation
World Health Organization
Geneva, Switzerland
alsalamahs@who.int

3rd Hessah Alsalamah
College of Computer and Information Sciences
King Saud University
Riyadh, KSA
halsalamah@ksu.edu.sa
College of Engineering and Architecture
Al Yamamah University
Riyadh, KSA
H_alsalamah@yu.edu.sa

4th Chang-Tien Lu
Department of Computer Science
Virginia Tech
Falls Church, VA, USA
ctlu@vt.edu

***Abstract*—Virtual hospitals empower traditional hospitals to deliver more accessible, affordable, and comprehensive patient-centered (PC) care services. However, traditional hospitals' legacy information systems are ill-equipped to support virtual hospitals' needs. This is due to their deployed disease-centered access control (AC) models with multiple inconsistent policies, which pose risks on information whenever shared across- hospitals' boundaries. Therefore, this study bridges the gap in AC literature with a novel model that can mitigate the risks in legacy information systems to be incorporated into virtual hospital settings securely. This paper proposes a granular *VHealth-AC* model that seamlessly grants healthcare practitioners at a hub hospital remote access to such PC data at the right point of care. We deploy a granular 5-tier PC information classification scheme to enforce these information security rules across-hospitals. In addition, we validated the feasibility of the proposed model design through a technical wrapper implementation on top of autonomous heterogeneous information systems. This design represents the neutral collaboration context security domain (i.e virtual hospital ecosystem) where the virtual healthcare service points of care are held following a patient's treatment plan. Our unique *VHealth-AC* model for virtual hospital ecosystems will encourage the development of secure virtual hospitals, in general, and the practice of virtual healthcare services, in particular, for a secure personalized care.**

***Index Terms*—Access Control, Information Classification Scheme, Information Security, Patient-Centered Care, Virtual Healthcare Services, Virtual Hospital.**

978-1-6654-6297-6/22/$31.00 ©2022 IEEE

I. Introduction

Virtual healthcare is a fundamental healthcare delivery model significantly shaped by eHealth technologies [1]. It refers to the actual provision of remote care to patients outside of a health setting. This is achieved through different communication platforms, including, but not limited to, telephones, videos, mobile applications, and text-based messaging. These platforms utilize different technologies, such as cloud computing, the Internet of Things (IoT) [2], artificial intelligence (AI) [3], and blockchain [4]. Similar to other healthcare delivery models, virtual healthcare maintains individualized care at the heart of its services to deliver a holistic, integrated, and patient- centered (PC) care model [1] [5] [6]. The PC model places the patient at the heart of these healthcare services and tailors care around the patient's needs and current state [1] [7] [8]. Moreover, it encourages healthcare practitioners to adapt to these needs by collaborating as a PC team [9] and using shared decision-making processes to determine optimal treatment plans for patients they collaboratively care for [8]. Therefore, PC care aims to connect healthcare providers, practitioners, and patients to enable a seamless flow of medical information between healthcare settings to virtually form a complete electronic patient record to enable this PC model [1] [6]. Traditional disease-centered care focus primarily around the needs of healthcare practitioners treating the disease [1] [8], making the key emphasis in this model on record keeping [1].

Emerging digital technologies have disrupted healthcare and introduced the notion of virtual hospitals as novel ways to provide care to patients wherever and whenever needed. Although the notion of virtual hospitals was first introduced a few years ago with the establishment of the world's first healthcare facility fully dedicated to the provision of virtual healthcare services [10], the term was only introduced a few years later. A virtual hospital is a dedicated network of secondary and/or tertiary care hospitals based on a "hub-and-spoke" organization design [11], to provide remote specialized care services in a "provider-to-provider" model. In a virtual hospital setting, practitioners at a primary hospital (i.e., hub) provide inpatient and outpatient virtual healthcare services efficiently and effectively to patients at multiple secondary hospitals (i.e., spokes) [11]. Therefore, the ultimate goal of virtual hospitals is to empower traditional hospitals to deliver a more accessible, affordable, and comprehensive PC care [10] [12].

Since the onset of the COVID-19 pandemic, the global wave of interest in virtual healthcare practice helped realize the potential of this model of care delivery to become the new norm [12] [13]. As a result of limited medical resources and increasing healthcare pressure, many countries from all around the globe (examples include [14] [15] [16] [17] [18]), rolled out virtual healthcare centers, programs, and solutions to deliver virtual healthcare services to citizens that can assist in decision-making and overcome health-related challenges. Consequently, regulators and policymakers from all around the world convened global experts to publish policy recommendations that can ensure the safety and effectiveness of virtual healthcare practice, while mitigating the potential risks of this newly adopted model of care [19] [20]. Furthermore, a survey [21] conducted by the World Health Organization (WHO) in 2020 indicated that 63% of 105 countries representing five WHO regions chose to deploy telemedicine to replace in-person consultations as the second leading approach to overcome healthcare service disruptions. In addition, according to some predictions [22], virtual healthcare services will be the future of healthcare post-pandemic surges.

This study proposes a secure *VHealth-AC* model that integrates granular cross-hospital sharing of PC data. We validated the feasibility of the proposed model design through a technical wrapper implementation in addition to autonomous heterogeneous information systems. Such a design represents the neutral collaboration context security domain (i.e., virtual hospital ecosystem), where the virtual healthcare service points of care are held following a patient's treatment plan. This should facilitate the adoption of virtual healthcare services in general, and lay the foundation for the development of scalable and secure virtual hospitals. The technical contributions of this study are summarized as follows:

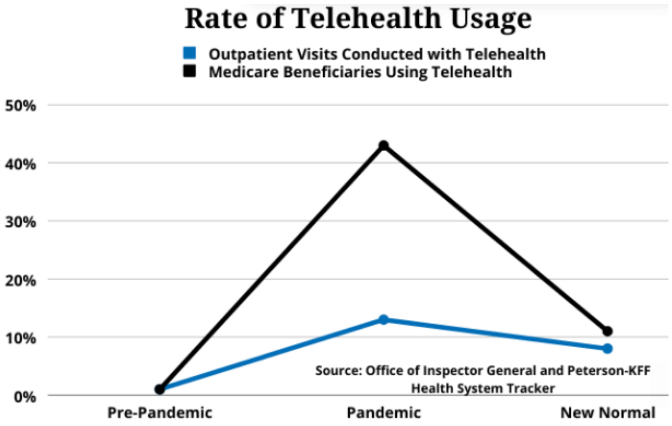

Fig. 1. Telehealth usage stabilized after pandemic surge [22]

1) We propose a novel *VHealth-AC* model that mitigates risks in legacy information systems to allow secure cross-hospital sharing with remote practitioners in a virtual hospital setting.
2) We designed a granular 5-tier information classification scheme that meets the information security needs of the virtual hospital ecosystem design.
3) We created a neutral security domain in the *VHealth-AC* that defines and enforces a neutral policy for sharing information across spoke hospitals' legacy systems. We enforced local policies that reside locally within the legacy information systems.

The remainder of this paper is organized as follows. Section 2 introduces the challenges in incorporating traditional hospitals into virtual hospital ecosystems. Section 3 discusses related work on access control (AC) models and their approaches. Section 4 introduces our proposed approach. Section 5 presents the design and implementation of the *VHealth-AC* model, and Section 6 concludes with a summary and future work.

II. Challenges in Incorporating Traditional Hospitals Into Virtual Hospital Ecosystems

Achieving information security in virtual healthcare services is one of the most important yet challenging issues in modern healthcare delivery models [23] [24]. On the one hand, sharing patient data across heterogeneous legacy information systems so that it is accessible to other care teams is fundamental for the successful implementation of the PC care model [25] [26]. This ensures that good-quality data are collected and subsequently shared to support the planning, commissioning, and transformation of services. On the other hand, WHO classifies health data as sensitive personal data or personally identifiable information [27]. This emphasizes the need to attain the right balance between confidentiality, availability, and integrity of personal health data using information security mechanisms [8] [23] [27]. Therefore, shared care in multiple healthcare provider settings places acute pressure on healthcare providers to address emerging privacy and security concerns, making trust management one of the most important challenges in this area owing to the open and anonymous nature of digital environments [26] [28]. Information security in the context of healthcare information systems means that only the right medical information is available to the right care team member at the right point in time [29]. This is because of the complicated system of global legislation that healthcare providers must comply with. Such legislation collectively aims to articulate how personal patient information must be handled and to provide clear rules on how processing of such information in a cross-system shared care environment should be carried out and controlled. Hence, healthcare providers who share patient information with other team members across their hospitals' information systems have no option but to carefully balance between making the right medical information available to the right user whenever needed and maintaining confidentiality. One of the most widely used security mechanisms deployed to control user actions in an information system to achieve information security goals is AC [8] [30] [31]. However, many hospitals' legacy information systems were designed as autonomous discrete information systems when disease-centered care was dominant [32]. Therefore, AC models deployed in such systems enforce an organization-driven information security policy that protects only local information resources [1]. This creates a single local point of control, limited by the system's physical perimeter, to meet the local information-sharing and security contexts of disease-centered care. Once this information is shared across the hospital's point-of-control boundaries, it compromises its availability, integrity, and confidentiality, as seen in Table 1 [33]. Furthermore, such threats result in legacy systems that block the flow of medical information [34]. This is because, first, legacy systems were designed to follow the traditional disease-centered model [29]; hence, they cannot enforce their policies outside their physical boundaries. Second, they lack a clear information security policy to govern exchanged patient-centered information at the collaboration level across healthcare provider systems. Consequently, such legacy systems cannot comply with the emerging information security needs of PC care to allow information to flow beyond a specific information system [1]. This renders information security in virtual healthcare services one of the most important yet challenging issues in modern healthcare delivery models [23] [24]. Therefore, this would require a new PC AC model that can address the information security limitations in legacy information system AC models and meet the information security needs of virtual hospitals.

III. Related Work

An AC model rationalizes access decisions and enforces them based on predefined access rules stored in the information security policy [35]. This policy is based on a deployed information classification scheme using three basic elements responsible for the storage, decisions, and enforcement of these rules in a controlled environment, creating a security domain. This is achieved through policy storage point (PSP), policy decision point (PDP), and policy enforcement point (PEP), respectively. This ensures that an authenticated user accesses only what they are authorized to access and determines whether authorization should be granted or rejected [36] [37].

TABLE I
INFORMATION SECURITY THREATS POSED BY HEALTH CARE LEGACY SYSTEMS [33]

Threat category	Threat description
Information Integrity	-Human error. -Inconsistent results in different systems.
Information Availability	-Disconnected systems at major sharing points. -Inconsistent information security policies. -Inflexible balance of information security in emergency cases. -Inconsistent user-hostile information system design. -Untraceable shared information. -Manual management of referrals between health care providers.
Information confidentiality	-Improper disclosure of medical information. -Hospital-wide access control.

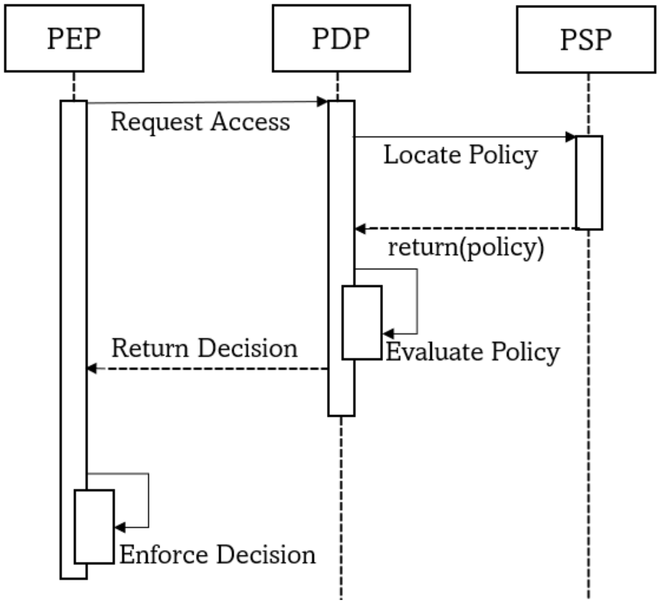

Fig. 2. Interaction between AC elements [44]

The three AC elements and their interactions are shown in Fig. 2.

Consider a scenario in which a virtual hospital service for outpatients is provided between a spoke and hub hospital security domain,D_S and D_H, respectively. Each hospital has its own local information security policies, P_S and P_H, respectively, which protect local information and are enforced by a single local point-of-control with a local AC model, AC_S and AC_H, respectively, which are independent and inconsistent. If D_S shares patient medical information,I_S, with D_H, this information must be protected when it leaves D_S's local point-of-control to reside in D_H. There are many proposals in the literature regarding approaches for cross-hospital information protection, ranging from unenforced, partially-enforced, to fully-enforced protection approaches.These proposals are classified into the following four groups:

A. Unenforced Protection Approaches

Traditional AC models [38] fall into this group, such as autonomous clinical portals. This group's security models are not designed to share information across the local AC model elements, and because this group cannot enforce P_S outside D_S, as a result, D_S loses complete control over its information when it leaves and D_H will have to make all the access decisions regarding this information comply with P_H at the expense of losing ownership over the information [38]. Consequently, hospitals may find it too risky to share information if it contains even a small range of sensitive content; thus, the effectiveness of collaboration is hindered in this group.

B. Partially-Enforced Protection Approaches

This group also hinders collaboration, as D_H controls the information coming from D_S using its policy P_H. In this group, a solution is used to help D_S govern its sensitive information by using its local rules when it is passed to D_H. A policy that reflects D_S needs is passed to D_H to be enforced. Although the solutions in this group agree that originators must govern their own information, they disagree on the best approach to make this possible. Sticky policies [39] [40] are examples of this group. This creates P_s, where P_S represents D_S's holistic information security policy, $P_s \subset P_S$ that is only limited to the protection of I_S in its new home in D_H. In addition, it recommends sticking this policy to the shared information using cryptographic mechanisms to communicate it securely to D_H and obliging D_H to enforce the policy using AC_H. However, all that D_S can do to guarantee the enforcement of its policy relies on D_H being a trusted authority that raises information security concerns. For D_H to enforce the stuck policy, it must interpret and express it at the lower levels of its information security design to enforce it at the machine level using its deployed AC_H model. This means that there is no guarantee that I_S will be protected in the same way or at the same level once it is located in D_H because the AC model deployed in D_H may not be compatible with all the rules in P_s stuck to I_S or even capable of implementing them.

Yau and Chen [41] and Begum *et al.* [41] proposed policy integration and conflict reconciliation solutions that can address two issues: multiple inconsistent policies and a lack of a common policy for D_H and D_S. This is addressed by enforcing one and only one sufficient neutral policy, P_N in both domains as a result of the integration of P_S with P_H [41]. This new policy aims to fully consider the local needs of both domains [41] while meeting the needs of the new sharing context created by the collaboration to govern any future information [41]. Therefore, both domains have to accept the resulting policy to govern all information resources used in the collaboration [41], P_N, which can be used locally in D_S and D_H without conflict with either P_S or P_H. However, these solutions are highly dependent on the interpretation of the received policies at the machine level. This interpretation introduces a threat to these collaborative environments by making them vulnerable to inaccurate or different interpretations by different organizations in the collaboration. This is because hospitals are constrained when implementing and enforcing these policies at the machine level, based on their existing applications and technology.

C. Tightly-Enforced Protection Approaches

Moreover, further proposals address the misinterpretation of policies in collaborative environments by sticking not only the policy with the information but also the AC_S elements. This maintains the same level of protection as the original rules regarding I_S remotely. Even after it moves to D_H as D_S's policy-enforcement model, AC_S is used, not D_H's AC_H. Digital rights management (DRM) in [42] is a well-known AC technology that can continue to be applied to information after it has been copied, transferred, and stored on another organization's information system and protects it using its original rules of D_S's AC model even after dissemination [38] [42]. This is achieved by not only moving the policy along with the information as suggested by Sticky Policies, but also all the other AC elements, PDP_S and PEP_S. This ensures P_S is properly enforced remotely [38] [42] using all D_S's AC elements to ensure a single obvious point-of-control with a maintained connection between the AC elements that are always stuck with the information and governing it. However, this solution is limited to the machine that it resides on and the number of users having access to it. Even if the user needs to listen to music on another machine, such as a tablet, this is limited to the number of times the watermarking technique and individualization that DRM employs are used [43]. This is because this technology does not allow policy update once the information, along with the stuck policy-enforcement point, leaves the physical perimeter [43] [44].

The Welsh Clinical Portal [45] solution addresses the static policy used in DRM to help D_S maintain its protection level even after information is shared with D_H, while allowing this information to be remotely changed at any time. This is achieved by choosing to use a unified AC model, with a neutral PEP_N that invokes a PDP_N, and thisPDP_N references the local PSP for each domain. This unified AC can access and enforce the PSP_S in D_H and enable the information owner, D_S, to access and modify this policy. The Welsh Clinical Portal is an electronic front door to various local autonomous clinical portals that creates a virtual electronic health record for patients [45]. This solution allows the PSP_S to move along with the information such that the unified AC can enforce it at any time and make it accessible locally for any later modification. This would allow each domain to maintain its local policy so that users at D_H can only view I_S based on D_S's local rules, P_S.

The usage control models in [38] [46] [47] attempt to address the static policy issue raised by DRM technology to provide a more flexible solution, but a different approach is used than the one adopted by the Welsh Clinical Portal. It modified the DRM solution by having two policy enforcement points in each domain linked together. This technique uses the concept of a "reference monitor" [38], an abstract concept that controls the rights and usage of rights on digital objects [38].

Usage control suggests having a reference monitor in D_S (the service provider in our scenario) named "server-side reference monitor," and another reference monitor in DB named "client-side reference monitor" [38]. This provides more flexibility by enabling both policy-enforcement points to make access right decisions for any number of access requests against the PA and enforce it equally in both domains to ensure consistency. However, like DRM, this technology cannot be used in collaborative environments of a heterogeneous nature, as it requires software to be used remotely, and all systems must be compatible with this software. Thus, although this group addresses the misinterpretation of policy problems by targeting the lower levels of D_H's information security design, this machine-level implementation only considers D_S, and hence does not consider D_H's information security needs fully in this collaborative context.

D. Fully-Enforced Protection Approaches

This last group addresses two issues presented by previous groups: first, the lack of consideration of the information security needs of both domains when meeting their new information-sharing and security contexts for collaboration, and not solely D_S needs. Second, this group addresses the misinterpretation issue resulting from the need to interpret inconsistent policies at lower levels. It aims to combine the strengths of each previous group to achieve a more holistic approach. This is achieved by creating a collaborative driven policy, P_N, which is different from the organizations' local ones and is common to all organizations reflecting the needs at upper levels. This policy is not organization-specific or a compromised integration of all of these policies; rather, it is a unified, neutral integration of all domains. Meanwhile, at the machine level, a unified neutral AC model, AC_N, is used to enforce this high-level policy equally in both D_S and D_H.

SPIDER, a self-protecting information for de-parameterized electronic relationships proposed by Burnap and Hilton [48] and its extension for healthcare applications in [49], is an example of such a holistic approach. For SPIDER to meet the common information protection needs in the collaborative information security context, it uses a unified information classification scheme for collaboration based on the widely used traffic light information classification scheme [43]. It enforces the policy using a unified neutral AC model, AC_N, which allows users in D_S to label the information they want to share with D_H with the right class. Then, the AC_N places the appropriate information security controls to meet the protection level of classified information only around labelled content within the information resource, which then creates the right information access rules for this labelled information before sharing takes place and stores it in a PSP_N. Once the information is shared with D_H, only the appropriate ranges of the information are accessed by the right user in the D_H through the PDP_N and PEP_N. The three AC elements are linked flexibly to ensure D_S's rules are enforced remotely regardless of where the information travels or resides. However, the traffic light classification scheme contains four classes adopted from the early developments of the lattice-based AC model [50], which address confidentiality issues concerning military information. This means it meets specific information-sharing and security contexts that may not be suitable for all types of collaborative environments with diverse needs as it is mostly concerned with the confidentiality of information without considering f the levels of information availability and integrity in the balance.

An Information Labelling Palette access control model by AlSalamah [43] proposed a solution that can target a wider range of collaborative environments by choosing a more comprehensive information classification scheme and developing a unified AC model as a plug-in for o Microsoft Word applications that can enforce this scheme at the machine level for any Word application user. Information Labelling Palette creates a set of reusable icon-based information classification schemes based on Protective Commons [43]. The solution uses nine "visual" icons to create a collaboration-driven policy at the upper level and communicate it to all participating organizations in secure officer- and human-readable formats. This is so that users understand the information security that d the icon providers for recipients to understand how to look after other people's information. Although, the classification scheme addresses the three information security goals in a collaboration, it is designed to meet the balance mainly in business application domains which makes it inappropriate for other domains. For example, medical information has a longevity characteristic meaning it is highly sensitive and confidential at all times [8] [32].

This final group provides a platform through either standalone software or a plug-in hosted by a widely used application. By using this platform, these solutions create a safe environment for policy enforcement that is unlikely to be compatible with disease-centered legacy information systems. In summary, this review of related works in the literature defines a clear gap in which existing disease-centered AC models cannot address the issues regarding traditional hospital legacy systems being incorporated into virtual hospital ecosystems.

IV. Proposed Approach

We conducted a study on a selected virtual healthcare service scenario for breast cancer, following a specific treatment plan for outpatients. This was done to identify the requirements for a secure virtual hospital ecosystem design in modern healthcare that incorporates traditional hospital information systems and mitigates the risks they pose. The proposed approach was conducted using the following four interrelated steps.

1) **Risk Assessment:** We conducted a comprehensive risk assessment of the selected scenario to identify the risks posed by legacy information systems on PC information in a virtual healthcare service context.
2) **Information Security Countermeasures:** We identified key information security countermeasures that need to be implemented in our system to mitigate these risks. The risk-assessment exercise findings and identified

information security countermeasures were extensively published in [35]. This study mainly focuses on the design and implementation of information classification and AC models.

3) **Information Classification Scheme:** Based on the countermeasures, we designed an information classification scheme that meets the information security requirements for this scenario through a PC-driven policy.
4) ***VHealth-AC* Model:** Based on the risk assessment exercise and identified information security countermeasures, we created a novel AC model that enforces the virtual hospital-driven policy from the classification scheme in an independent information layer based on treatment and lies on top of the interface of the currently used legacy information systems to formalize and manage a unique treatment journey.

V. VHealth-AC Model Design and Implementation in a Virtual Hospital Ecosystem

To validate the design and implementation of the *VHealth-AC*, a virtual hospital context based on cancer treatment needs to be defined as well, as it represents the collaboration information sharing needs where the AC model meets the information security requirements. This way, our proposal should meet both the information sharing, as well as, the information security contexts.

A. Design Components Overview

First, the proposed solution meets the collaborative information-sharing context in virtual healthcare services through a prototype system that constructs an independent information layer. This layer resides on top of the interface of the legacy information systems currently used in traditional hospitals to formalize and manage the information flow between the various spoke hospitals providing care to follow the mapped cancer treatment plan journey. In addition, this layer is designed as a loosely coupled wrapper-based system with legacy information systems to embrace local organization-centered access controls without interruption and sustain the balance of information security.

Second, the proposed solution meets the information security context in the treatment pathway by controlling access to information at each treatment point using the new AC model. This model creates a virtual hospital-driven information security policy based on the classification scheme at the collaboration level that meets the overall care goal and enforces this balance in a neutral security domain with a single authority point-of-control that stretches across hospitals anywhere within the virtual hospital environment (i.e., cooperation environment), while retaining the local medical information security of shared information among the care team.

B. 5-Tier Information Classification Scheme

The proposed fine-grained *VHealth-AC* model is based on a granular 5-tier information classification scheme, which controls and grants access to the health practitioner at a hub hospital seamlessly across hospitals at the point of care. Defining this collaboration-driven context should require access to information strictly on a “need-to-know” basis, which complies with healthcare regulations and data protection laws [51] [52]. Therefore, in order to provide the right set of data to the right care team member at the right time of treatment on a “need-to-know” basis, we propose a fine-grained *VHealth-AC* model that achieves this goal. We defined access rules for the *VHealth-AC* model based on the following five key interrelated elements (as illustrated in Fig.3): patient, PC care team assigned to this patient, PC care team’s member role, treatment plan, and virtual healthcare point of care. These elements define an information classification scheme suitable for the VHealth-AC model, where

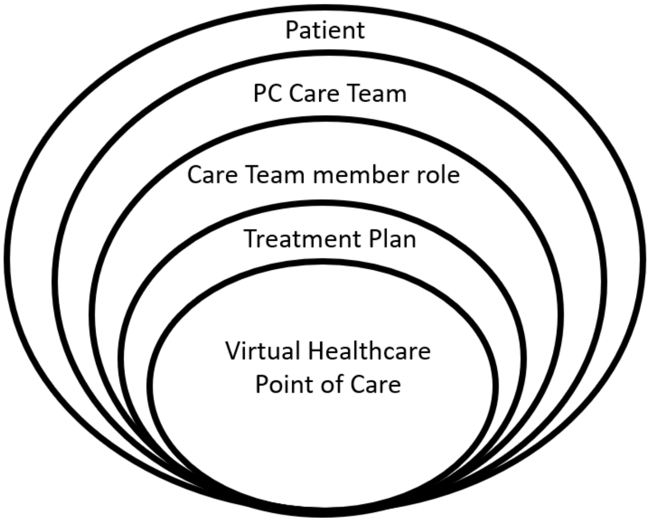

Fig. 3. 5-Tier Information Classification Scheme for *VHealth-AC* Model.

1) Each patient is looked after by at least one specialized PC care team that includes all specialized healthcare practitioners caring for that particular patient to treat his/her disease or condition. This means that if a patient has comorbidities (i.e., suffering from more than one condition or disease and following more than one treatment path), then he/she may have more than one PC care team.
2) Each authorized PC care team member (i.e., healthcare practitioner) should access PC data only for the patients he/she cares for and only if they play a role in their treatment plan.
3) Ultimately, at a virtual healthcare service point of care, the PC data should be accessible to each PC care team member who needs to access it to play his/her role in the current treatment plan for the provided service.

C. VHealth-AC Model in a Virtual Hospital Ecosystem

To bridge the gap in the AC literature, there is a need for a fully-enforced AC model AC_V that incorporates heterogeneous disease-centered legacy information systems. This

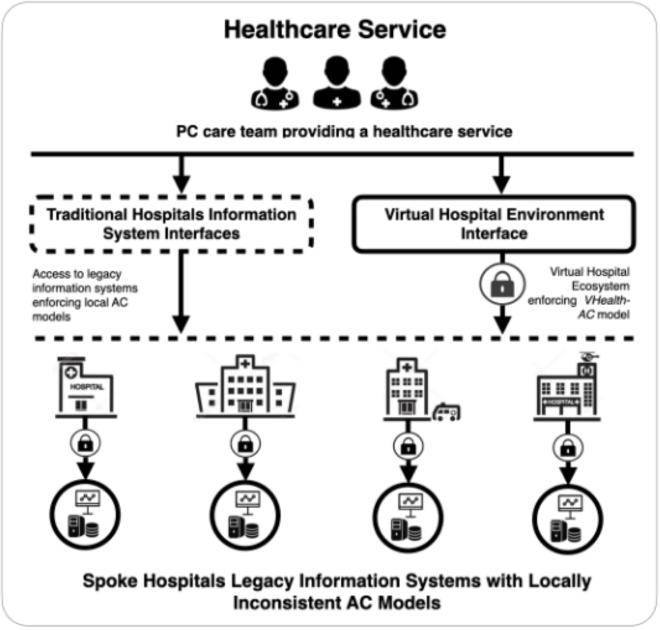
Healthcare Service
PC care team providing a healthcare service
Traditional Hospitals Information System Interfaces
Virtual Hospital Environment Interface
Access to legacy information systems enforcing local AC models
Virtual Hospital Ecosystem enforcing VHealth-AC model
HOSPITAL
Spoke Hospitals Legacy Information Systems with Locally Inconsistent AC Models

Fig. 4. The proposed *VHealth-AC* Model in a Virtual Hospital Ecosystem Design

AC model should enforce a neutral virtual hospital-driven policy (i.e., collaboration-driven) P_V that takes control over the information I_S wherever it resides within the collaborative environment (i.e., virtual hospital ecosystem) security domain D_V, without interrupting traditional hospital-driven policies (i.e., organization-driven) of disease-centered AC models in legacy information systems governing such information with local policies P_S as long as it is used locally D_S. This guarantees that each legacy system's AC model enforces the neutral policy P_V defined by *VHealth-AC* as long as the information resides in D_V. It enforces PS as long as it resides in D_S (see Fig. 4). This allows our model to attain the right balance of I_S information security in its targeted security domains without interruption.

To implement the *VHealth-AC* model, in a unified ecosystem design, a technical wrapper was designed on top of a traditional hospital legacy information system to represent the neutral collaboration context security domain (i.e., virtual hospital ecosystem D_V), where the virtual healthcare service points of care are held following a patient's cancer treatment plan. In this technical wrapper, the *VHealth-AC* creates the PSP_V, PDP_V, and PEP_V elements for this security domain and enforces access decisions in P_V for any PC care team member requesting access to the PC information I_S. These data are obtained from spoke hospital information systems that deploy the security domain D_S locally. Using this wrapper, the *VHealth-AC* model controls what should be viewed by the PC care team member to balance the fine line between the availability of patient information while preserving patients privacy. Finally, the *VHealth-AC* model should provide a secure, intelligent ecosystem that can transform traditional hospitals with a disease-centered system, and limited cross-hospital information-sharing into a secure and intelligent ecosystem.

VI. Conclusion and Future Work

AC models of legacy information systems do not meet the information security needs of virtual hospitals. Thus, the proposed solution addresses the inadequacy of legacy hospital information systems that hinder the flow of medical data for PC care continuity. We developed a granular *VHealth-AC* model that seamlessly grants healthcare practitioners at a hub hospital remote access to PC data at the right point of care. It deploys a granular 5-tier PC information classification scheme to enforce information security rules across hospitals. Our novel solution should empower patients, healthcare providers, and practitioners to deliver accessible, affordable, and comprehensive PC care. Furthermore, we plan to improve this work in the future by using fog computing and edge computing, not in real time, to enhance factors such as limited bandwidth and capacity.

References

[1] J. Dawson, B. Tulu and T. A. Horan, "Towards patient-centered care: The role of e-health in enabling patient access to health information," In: E. V. Wilson (Ed.) Patient-Centered E-Health, London, United Kingdom: IGI Global, 2009.

[2] P. Pace, G. Aloi, G. Caliciuri, R. Gravina, C. Savaglio, G. Fortino,G. Ibáñez-Sánchez et al., "Inter-health: An interoperable iot solution for active and assisted living healthcare services," In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), pp. 81-86, IEEE, 2019.

[3] T. N. Nguyen, N. P. Nguyen, C. Savaglio, Y. Zhang, and B. Dumba, "The Role of Artificial Intelligence (AI) in Healthcare Data Analytics," INTERNATIONAL JOURNAL ON ARTIFICIAL INTELLIGENCE TOOLS 30, no. 06 N 08, 2021.

[4] H. Kurdi, S. Alsalamah, A. Alatawi, S. Alfaraj, L. Altoaimy, and S. H. Ahmed, "Healthybroker: A trustworthy blockchain-based multi-cloud broker for patient-centered ehealth services," Electronics 8, no. 6 (2019): 602.

[5] J. Brunner, E. Chuang, C. Goldzweig, C. L. Cain, C. Sugar et al., "User-centered design to improve clinical decision support in primary care," International Journal of Medical Informatics, vol. 104, no. Suppl. 3, pp. 56–64, 2017.

[6] S. A. Alsalamah, H. A. Alsalamah, T. Nouh and S. A. Alsalamah, "HealthyBlockchain for global patients," Computers, Materials & Continua, vol. 68, no.2, pp. 2431–2449, 2021.

[7] Department of Health (DoH), "Equity and excellence: Liberating the NHS," London: HMSO, 2010.

[8] S. Alsalamah, "Information Classification Scheme for Next Generation Access Control Models in Mobile Patient-Centered Care Systems," In: the 12th International Conference on Cyber Warfare and Security (ICCWS), Dayton, Ohio, USA. pp.1-9, 2017.

[9] H. Al-Salamah, W. A. Gray, and D. Morrey, "Velindre Healthcare Integrated Care Pathway, in Taming the Unpredictable Real World Adaptive Case Management: Case Studies and Practical Guidance, L. Fischer, Ed. Lighthouse Point: Future Strategies Inc., p. 227, 2011.

[10] Mercy Virtual, "Delivering Care Wherever It's Needed," Mercy Virtual, 2022, https://www.mercyvirtual.net/about/.

[11] J. K. Elrod, and J. L. Fortenberry,"The hub-and-spoke organization design: an avenue for serving patients well," BMC Health Serv Res 17, 457, 2017, https://doi.org/10.1186/s12913-017-2341-x

[12] Mobifilia, "Virtual Hospitals: Future of Healthcare," Mobifilia, 2020, https://www.mobifilia.com/virtual-hospitals-future-of-healthcare/.

[13] S. Aziz, "Telemedicine Use Is Rising amid COVID-19 Pandemic. Will It Become the Norm? - National. Telemedicine Use Is Rising amid COVID-19 Pandemic. Will It Become the Norm?," Global News, 2021, https://globalnews.ca/news/7902460/telemedicine-future-covid-canada/.

[14] World Health Organization, “Supporting Argentina’s Regional Leadership in Telehealth,” World Health Organization, 2020, https://www.who.int/about/accountability/results/who-results-report-2020-mtr/country-story/2020/supporting-argentinas-regional-leadership-intelehealthftn1.

[15] T. Kene-Okafor, “New South African Partnership Gets $3M, Launches Telehealth Product,” TechCrunch, 2021, https://techcrunch.com/2021/06/10/new-south-african-partnership-gets-3m-launches-telehealth-product/.

[16] NZ Telehealth, “A Hinz Special Report into Telehealth at New Zealand Dhbs and the Impact of Covid-19, Telehealth,” 2020, https://www.telehealth.org.nz/news/a-hinz-special-report-into-telehealth-at-new-zealand-dhbs-and-the-impact-of-covid-19/.

[17] National Academy for State Health Policy, “States Provide Payment Parity for Telehealth and In-Person Care,” National Academy for State Health Policy, 2021, https://www.nashp.org/states-provide-payment-parity-for-telehealth-and-in-person-care/.

[18] N. A. Ganai, “How China Used Telemedicine to Fight COVID-19,” Health Analytics Asia, 2021, https://www.ha-asia.com/how-china-used-telemedicine-to-fight-covid-19/.

[19] Novartis Foundation, “Broadband Commission Working Group on Virtual Health and Care,” Novartis Foundation, 2022, https://www.novartisfoundation.org/transforming-population-health/ai-health-policy/broadband-commission-working-group-virtual-health-and-care.

[20] N. Hare, P. Bansal, S. S. Bajowala, S. L. Abramson, S. Chervinskiy et al., “Work Group Report: COVID-19: Unmasking Telemedicine,” The journal of allergy and clinical immunology, In practice, 8(8), 2461–2473.e3, 2020, https://doi.org/10.1016/j.jaip.2020.06.038

[21] World Health Organization. Pulse survey on continuity of essential health services during the COVID-19 pandemic: interim report, 27 August 2020. No. WHO/2019-nCoV/EHScontinuity/survey/2020.1. World Health Organization, 2020

[22] Insights by Xtelligent Healthcare Media, “Telehealth Growth and Development: Telehealth’s place in the Industry Beyond the Pandemic,” xtelligentmedia, 2021

[23] F. Khan, S. Khan, S. Tahir, J. Ahmad, H. Tahir et al., “Granular Data Access Control with a Patient-Centric Policy Update for Healthcare,” Sensors (Basel), 2021;21(10):3556, doi:10.3390/s21103556

[24] Y. Liu, Y. Zhang, J. Ling, Z. Liu,“Secure and Fine-Grained Access Control on e-Healthcare Records in Mobile Cloud Computing. Future Generation Computer Systems,” vol. 78, pp. 1020–1026.,2018, https://doi.org/10.1016/j.future.2016.12.027.

[25] Healthcare Information and Management Systems Society (HIMSS), The Evolution of Patient Engagement: Rethinking How to Best Engage Patients. HIMSS Media Lab: Himss17 In Focus, 2017.

[26] J. Goldwater, The Use of a Blockchain to Foster the Development of Patient-Reported Outcome Measures. Washington, D.C., United States: National Quality Forum, 2016.

[27] World Health Organization, “Global Strategy on Digital Health 2020–2025,” Geneva, Switzerland: World Health Organization, 2020.

[28] I. Abu-elezz, A. Hassan, A. Nazeemudeen, M. Househ and A. Abdalrazaq, “The benefits and threats of blockchain technology in healthcare: A scoping review,” International Journal of Medical Informatics, vol. 142, pp. 104246, 2020.

[29] S. Alsalamah, H. Alsalamah, A. W. Gray and J. Hilton, “Information security threats in patient-centred healthcare,” In: A. Moumtzoglou (Ed.) M-Health Innovations for Patient-Centered Care. Hershey: IGI Global, pp. 298–318, 2016.

[30] D. F. Ferraiolo, D. R. Kuhn and R. Chandramouli, “Role-Based Access Control,” Artech House, 2007.

[31] M. E. Whitman and M. J. Herbert, “Management of Information Security,” Cengage, 2019.

[32] S. Alsalamah, H. Alsalamah, A. Gray and J. Hilton, “Information Security Threats in Patient-Centred Healthcare,” In I. Management Association (Ed.), Health Care Delivery and Clinical Science: Concepts, Methodologies, Tools, and Applications, edited by Information Resources Management Association, IGI Global, 2018, pp. 1531-1552, https://doi.org/10.4018/978-1-5225-3926-1.ch077

[33] S. Alsalamah, H. Alsalamah, A. W. Gray and J. Hilton, “Information security threats in patient-centred healthcare,” in Health Care Delivery and Clinical Science: Concepts, Methodologies, Tools, and Applications. Pennsylvania, United States: IGI Global, pp. 1531–1552, 2018.

[34] S. Alsalamah, “Achieving a secure collaborative environment in patient-centred healthcare with legacy information systems, Cardiff University, United Kingdom, Ph.D. dissertation, 2015.

[35] S. Alsalamah, H. Alsalamah, A. W. Gray and J. Hilton, “Information Security Threats in Patient-Centred Healthcare,” In I. Management Association (Ed.), Health Care Delivery and Clinical Science: Concepts, Methodologies, Tools, and Applications, IGI Global, pp. 1531-1552, 2018.

[36] D. L. Pipkin, “Information Security: Protecting the Global Enterprise,” Prentice Hall PTR, 2000.

[37] A. Ferreira, R. Correia and L. Antunes, “Access Control in Healthcare: the methodology from legislation to practice,” Studies in health technology and informatics 160 Pt 1, pp. 666-70, 2010.

[38] J. Park and R. Sandhu, “Towards usage control models: beyond traditional access control,” in Proceedings of the seventh ACM symposium on Access control models and technologies, SACMAT ’02, New York, USA, pp. 57–64, ACM, 2002.

[39] S. Pearson and M. C. Mont, “Sticky policies: An approach for managing privacy across multiple parties,” Computer, vol. 44, pp. 60–68, 2011.

[40] S. Sicari, A. Rizzardi, G. Dini, P. Perazzo, M. La Manna et al., “Attribute-based encryption and sticky policies for data access control in a smart home scenario: a comparison on networked smart object middleware,” int. J. Inf. Secur, vol. 20, pp. 695–713, 2021, https://doi.org/10.1007/s10207-020-00526-3.

[41] S. Yau and Z. Chen, “Security Policy Integration and Conflict Reconciliation for Collaborations among Organizations in Ubiquitous Computing Environments,” in Ubiquitous Intelligence and Computing (F. Sandnes, Y. Zhang, C. Rong, L. Yang, and J. Ma, eds.), vol. 5061 of Lecture Notes in Computer Science, pp. 3–19, Springer Berlin Heidelberg, 2008.

[42] Q. Liu, R. Safavi-Naini and N. P. Sheppard, “Digital Rights Management for Con- tent Distribution,” in Proceedings of the Australasian Information Security Work- shop Conference on ACSW Frontiers, Vol. 21, ACSW Frontiers ’03, Darlinghurst, Australia, pp. 49–58, Australian Computer Society, Inc., 2003.

[43] S. Al-Salamah, “Towards Information Sharing in Virtual Organizations: The Development of an Icon-Based Information Control Model,” LAP Lambert Academic Publishing, 2010.

[44] P. R. Burnap, I. Spasić, W. A. Gray,J. C. Hilton, O. F. Rana et al., “Protecting Patient Privacy in Distributed Collaborative Healthcare Environments by Retaining Access Control of Shared Information,” 2012 International Conference on Collaboration Technologies and Systems (CTS), 2012, https://doi.org/10.1109/cts.2012.6261095.

[45] Robin Mann, “Welsh Clinical Portal Development: Functional Releases,” tech. rep., 2007.

[46] A. Lazouski, F. Martinelli, and P. Mori, “Usage control in computer security: A survey,” Computer Science Review, vol. 4, pp. 81-99, Science Direct, 2010.

[47] A. M. Reina Quintero, S. Martínez Pérez, Á. Jesús Varela-Vaca, and M. Teresa Gómez, “A domain-specific language for the specification of UCON policies,” Journal of Information Security and Applications, vol. 64, pp. 103006, Science Direct, 2022.

[48] P. Burnap and J. Hilton, “Self Protecting Data for De-perimeterised Information Sharing,” in 2009 Third International Conference on Digital Society, Cancun, pp. 65–70, IEEE, 2009.

[49] P. R. Burnap, I. Spasic, W. A. Gray, J. C. Hilton, O. F. Rana et al., “Pro- tecting patient privacy in distributed collaborative healthcare environments by re- taining access control of shared information,” in 14th International Conference on Collaboration Technologies and Systems (CTS), Denver, pp. 490–497, 2012.

[50] R. Sandhu, “Lattice-based access control models,” Computer, vol. 26, pp. 9–19, 1993.

[51] Participation, Expert. Data Protection Act 1998. Legislation.gov.uk, Statute Law Database, 16 July 1998, https://www.legislation.gov.uk/ukpga/1998/29.

[52] A. Greenough and Helen Graham, “Protecting and Using Patient Information: The Role of the Caldicott Guardian,” Clinical Medicine, vol. 4, no. 3, pp. 246–249,2004, https://doi.org/10.7861/clinmedicine.4-3-246. Office, 1998.