Cyber Security
and Privacy
Research Institute

THE GEORGE WASHINGTON UNIVERSITY

Secure Augmented Reality (AR) for Telehealth and Emergency Medical Services (EMS): A Survey

Tianyou Bao
Hurriyet Ok

July 22, 2021
Report GWU-CSPRI-2021-05

Secure Augmented Reality (AR) for Telehealth and Emergency Medical Services (EMS): A Survey

Tianyou Bao
Department of Computer Science
The George Washington University
Washington, D.C.
baot@gwu.edu

Hurriyet Ok
Cyber Security & Privacy Research Institute
The George Washington University
Washington, D.C.
hurriyetok@email.gwu.edu

ABSTRACT

This survey paper reviews the cybersecurity issues related to augmented reality (AR) applications, especially in context of Telehealth and Emergency Medical Services (EMS). AR systems are considered very valuable in the telehealth and EMS fields. The security and privacy of these systems are critical to protecting medical information and patient privacy. In this article, some security issues that AR systems must address will be discussed.

AR systems are vulnerable to cybersecurity attacks during data input, transmission, and output. The data collected by on-device sensors may contain private information. In the data transmission phase, outdated transmission protocols, simple authorization, and lack of security patches will increase data leakage risk. In terms of data-at-rest, failure to protect data can lead to unauthorized data access and modification. Therefore, AR systems should be protected against vulnerabilities to ensure the confidentiality and integrity of sensitive data. More research needs to be done on how to secure AR applications in the telehealth and EMS fields. Providing a secure method of transferring sensitive medical information and patient data using AR systems should help in the future development and adoption of AR devices for EMS and telehealth operations.

KEYWORDS

Cybersecurity, Privacy, Augmented Reality (AR), Mixed-Reality (MR), Extended Reality (XR), Telehealth, Telemedicine, Emergency Medical Services (EMS)

1 Introduction

Augmented reality (AR) technology overlays virtual information to the user's real environment, providing an intuitive interaction experience to the users. AR has been recognized as a viable technology to communicate situational information among frontline medical emergency rescue teams and first responders to reduce on-site confusion and offer a faster response and quicker decision-making to save lives [1]. With the widespread availability of digital communication and information technologies, telehealth has also made significant advancements in the past decades: from using telegram and voice for medical information exchange to the transmission of images (such as X-ray images), as well as videoconferencing consultation and even remote surgery [2]. Telehealth can now provide medical services to underserved rural areas, inaccessible sites, such as ships, aircraft and geographically remote regions, and disaster areas [3]. During the COVID-19 pandemic, the use of telehealth has increased dramatically [4]. Examples include using robots to classify patients prior to treatment, and doctors remotely viewing the patient's condition without physical contact [5]. For Emergency Medical Services (EMS), telehealth can help on-site nurses diagnose and classify patients to improve public medical resource utilization and increase patient satisfaction [6]. In addition, the data collected from the sensors on wearable devices can help EMS personnel monitor patients' vital signs [7].

Telehealth and EMS are already encountering challenges in the field of security and privacy. As medical records are protected by laws [8], any medical information about patients need to be processed properly and stored securely. Healthcare systems are already under extreme pressure from cyber-attacks. In a recent incident, Falls Church-based Inova Health System [9] and several others using Charleston, South Carolina-based software vendor Blackbaud suffered a ransomware attack [10], which encrypts files across computer networks and requires payment to unlock them. In 2016, MedStar Health was victim to a similar attack, when officials detected malware and shut down its online operations as a defense tactic [11].

This paper will introduce the security concerns that AR systems may be vulnerable to, as well as existing solutions. This section will introduce the use cases of AR in telehealth and EMS fields. In Section 2, we will focus on the security issues of AR systems used in EMS scenarios.

1.1 AR in Telehealth

In AR-enabled medical training, the original 2D teaching materials can be presented in 3D immersive content, such as surgical simulation. During preoperative communication, AR technology allows the patient to intuitively understand the condition of the disease and facilitates an effective communication between the doctor and the patient. Doctors initially used videos and images to discuss surgical plans, intraoperative guidance, and remote consulting services. AR technology can now convert 2D materials into 3D images, which can improve efficiency and improve accuracy [12]. In rural areas of many countries, the AR telemedicine system can provide remote training and remote guidance to improve relatively limited medical facilities [13].

Telehealth includes telemedicine and other remote healthcare services. At present, many telemedicine platforms use video calls or WebRTC (Web Real-Time Communication) based technology to transmit video or audio [14]. However, the telemedicine system using AR technology would be more intuitive, easier to use, and would allow users to focus on solving medical problems rather than looking away to view mentor's guidance through a monitor display [15]. AR use necessitates the communication of digital content from the incident scene or patient location through reality capture, in the form of video and real-time 3D mapping, in addition to geolocation data. Ponce et al. proposed an application that uses AR technology on mobile devices for early postoperative care. The application combines the doctor's annotation with the video stream captured by the patient's camera, allowing both parties to have a satisfying virtual interaction [16]. While Mobile AR is widely accessible and available, it requires users to hold the mobile device. The advantage of AR glasses or Head Mounted Displays (HMD) is that they free user's hands to hold equipment, tools, etc. In a training scenario, a mentor can create and edit graphical annotations on live video of the operating field and display the annotations directly onto the trainee's field of view, anchored to relevant regions of the operating field [15]. Bifulco et al. built an augmented reality application that allows untrained volunteers to perform electrocardiogram (ECG) tests on patients [17]. In addition, AR glasses allow remote users to obtain the video stream in the first-person view. The telemedicine platform designed by Carbon et al. uses an AR HMD to merge the remote doctor's hand or instrument with the images on the local doctor's side and transmit the images using Voice over IP (VOIP) software. The platform showed high image accuracy in the test [18].

1.2 AR for Emergency Medical Service (EMS)

In the face of an emergency or natural disaster, first responders may need to go to unfamiliar locations to save lives. AR technology helps with the navigation by providing timely and relevant information, such as geographic references and tasks, to the public safety personnel, which improves situational awareness, and reduces distractions and/or cognitive overload. The incident location can be displayed in 3D maps as holograms on AR headset. The camera on an AR headset can record the video of the scene or victims for immediate assessment by remote teams. THEMIS (disTributed Holistic Emergency Management Intelligent System) project is an example, in which AR is used by first responders in a context of disaster relief operations [19]. For EMS personnel, training and drills are also an essential part of developing skills to perform under stress. The AR and VR applications designed by Koutitas et al. provides EMS personnel an interactive training environment in a bus-sized ambulance for large-scale emergencies. The EMS trainees participated in such immersive learning exercise demonstrated a better retention and task effectiveness, compared to traditional training [20].

By expanding the types of data received from AR devices (such as biometrically inferred data), as well as the type of data sent to first responders (such as electronic health records (EHR)), AR technology enables first responders to interact securely and effectively with the many data sources presented. In a scenario where EMS members need victim patient assessment, the data types to be transferred, such as facial biometrics from AR systems and electronic health records (EHR) from authorized providers, must be secured end-to-end, to protect privacy, as well as comply with the HIPAA Security Rule. New solutions should ensure that integrity of these types of data and content privacy are protected when communicated through AR devices and AR integrated systems.

Opportunities exist to use AR to connect the dots between locating injured persons and search and rescue (SAR), assessing and stabilizing injured persons, and identifying specifics for delivering lifesaving care to injured persons. AR is an ideal technology to enable information collection and transmission in context, providing high visibility to incoming data points while enabling first responder attention to focus on scene safety and tasks at hand.

Ensuring the security and privacy of information is a critical aspect of the AR telehealth and EMS systems. In telehealth and EMS scenarios, the AR system needs to collect information (such as images, sounds, 3D-mapping, geographic location information, and biometric information) and send it to the cloud; and the system will receive sensitive information, such as EHR from the cloud. In the process of the data flow, any security vulnerability can affect the stability and security of the system, and even affect the lives of patients. This paper will survey the state of the research and academic thinking in secure AR in telehealth and EMS scenarios.

2 Securing AR Systems

AR wearable technologies are expected to become mainstream devices used daily like mobile phones [21, 22]. As AR glasses are adopted by businesses and consumers and use becomes more widespread, the cybersecurity and privacy risks associated with the functionalities of AR will increase [23]. Figure 1 presents a data flow model of an AR environment with the supporting data services. Possible security vulnerability points are during data input, data-at-rest, data transmission, and data output.

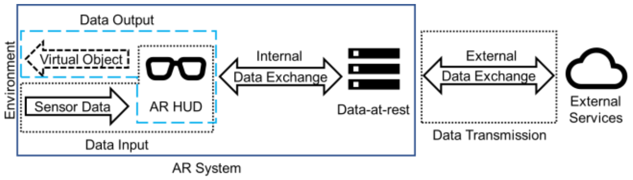

Figure 1: Data Flow of An Augmented Reality Environment with Data Services

Data input is mainly a process in which users, devices, and sensors obtain or collect data from the outside environment, the real world, and then store and process them. For example, users using the hand gesture to simulate the keyboard input can be regarded as the user's data input to the AR system. When using this gesture operation, the AR head-up display (HUD) will enable the camera and capture video of the scene. The action of streaming the video into the AR system can be regarded as obtaining data from the outside environment. The data-at-rest is the data locally stored on AR system, which could be generated by an on-device AR app, retrieved from sensors, or received from external services. Data transmission is the process of transferring data from an AR system to external services via the network or other medium. Data output is the process of displaying or rendering data received either from an on-device AR app or from an external service.

2.1 Secure AR for Telehealth and EMS

In telehealth practice and EMS, data security and privacy are very important to maintain compliance with HIPAA Security Rule [24]. For example, home telehealth devices will transmit information on activities in the household over the Internet. The sensors on a mobile device, such as camera, may inadvertently collect information about the activities of the patient and the family members [25, 26]. A security breach in an implanted device in patient's body can even be a matter of life-or-death [27]. If the patient's electronic health records and session data are not encrypted or lack authentication, they may also be obtained by unauthorized third parties [28]. By taking technical security measures in compliance with HIPAA, healthcare organizations can protect their networks and devices from data breaches [29, 30].

An AR-integrated EMS system can enable a paramedic to locate an injured person, successfully navigate to him/her, assess status, and identify relevant medical history information from his/her remote Electronic Medical Record (EMR) to provide best field treatment. Further, it is possible to share information back to the EMR and create a direct link with the relevant medical expertise remotely to the paramedic in the field. Figure 2 illustrates security vulnerability points for a potential EMS scenario where a first responder equipped with an AR system, EMS "Decision Center", a combined Public Safety Access Point (PSAP), and Emergency Medical Dispatch (EMD) are involved:

1. EMS Decision Center receives notification of emergency through 911 call as shown in Figure 2a.
2. The Decision Center sends the location and victim information to the first responders nearest to the victim. This information appears in the AR HUD for the first responder, who makes his/her way toward the location.
3. First responder arrives at location; takes video of victim with mobile device; begins working on patient assessment; video sent to Decision Center; facial recognition identification performed; full medical record pulled up; portion transmitted to first responder; (optionally) full record transmitted to doctor as illustrated in Figure 2b. The facial recognition is processed and linked to an EMR of the given individual. The Decision Center highlights relevant information for the first responder, such as allergies, cardiac events, and other medical history relevant to field trauma stabilization procedures. First responder confirms receipt of medical record detail and that event is logged.
4. The first responder keeps working, given new data; possibility of having a doctor send a new message to the first responder via open video or voice channel for real time guidance on the patient as depicted in Figure 2b. The Decision Center connects the EMR of the given individual to a relevant medical professional, according to the updates provided by the first responder's assessment of the patient's condition. A link is established through which the remote medical professional can provide real-time guidance via bi-directional voice memos, images and text messages delivered in the AR HUD.

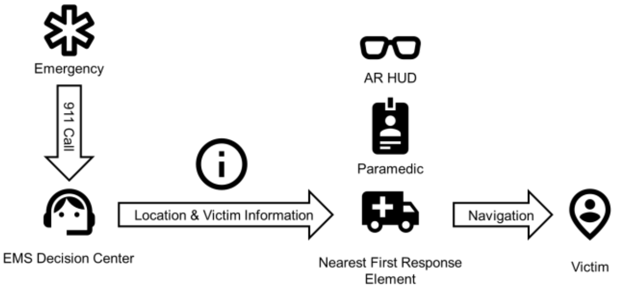

Figure 2a: An EMS Scenario Involving First Responders Equipped with an AR System

Figure 2b shows the vulnerability points in EMS scenarios. Vulnerability points exist in the real-time guidance communication between first responder and doctor; first responder reports the situation to decision center; patient EMR is transmitted to first responder and doctor; first responder archives the data to the log file. These vulnerabilities involve confidentiality (data leakage) and integrity (data tampering) in fundamental data security requirements. The following are the potential risks caused by these vulnerabilities:

- Insecure transmission of sensitive data, resulting in leakage of patient medical records.
- Wrong information exchange caused by tampering of the communication content between the first responder and the doctor or decision center.
- Delay or misdiagnosis caused by losing relevant vital patient information.
- Log file damage caused by insecure file storage, unauthorized data access or data tampering.

The next sections review the security and privacy concerns in an AR system using the data flow model of an AR environment as shown in Figure 1. Section 2.1.1 explains possible security vulnerability points during data input. Section 2.1.2 explains security challenges of data-at-rest. Section 2.1.3 discusses protection needs during data-transmission, and Section 2.1.4 reviews security issues of data-output with references to UX/UI privacy and user safety.

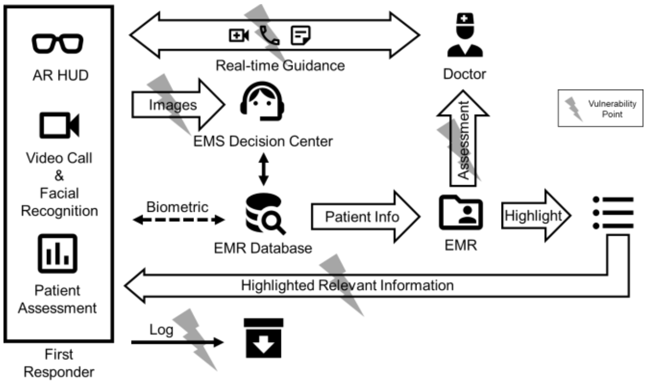

Figure 2b: An Emergency Response Scenario to Illustrate the Security Vulnerability Points where an AR System in Use.

2.1.1 Data Input

Mobile devices have many sensors such as image sensor, global positioning system (GPS) sensor, accelerometer, gyroscope, inertial measurement unit (IMU), magnetometer, ambient light sensor, and microphone [31]. Based on the mobile device technologies, AR systems use data from these sensors as the input source to enable immersive experiences. For example, GPS, IMU, and compass are used to provide location and movement information required by navigation applications. Accelerometers and gyroscopes can help applications determine the user's posture to display the position of virtual objects accurately. The combined data collected from these sensors may contain private information. There is a security risk of unauthorized access to such sensitive data during collection (data input), transmission, or storage (data-at-rest) [26].

2.1.2 Data-at-rest

Mobile computing is a key enabling technology for AR systems [32]. Data stored on AR devices have similar security challenges and vulnerabilities as modern mobile device hardware and operating systems (OS). Secure storage solutions based on software mechanisms are often vulnerable to attacks. Therefore, smartphone chip makers, such as Qualcomm Technologies, implement hardware-backed secure storage solutions in their mobile System-on-a-Chip (SoC) products [33]. Both Android and iOS leverage hardware-based features for protecting the privacy and security of sensitive data [34].

2.1.3 Data Transmission

Telehealth systems typically require sensitive data exchange between provider and patients. Sensitive data (e.g., audio and video conversations, medical images and records) should be kept private and securely transferred over the Internet for confidentiality [25]. AR systems integrated with cloud-based telehealth and EMS services are inherently more vulnerable to security attacks and privacy threats, compared to localized or standalone AR applications, such as training [35]. The data transmission over a network generally relies on traditional cryptographic protocols such as Transport Layer Security (TLS) and Virtual Private Networks (VPN) [36, 37]. None of these secure-communication solutions ensures the preservation of the integrity of the captured data end-to-end. Such protocols are known to have Man-in-the-Middle (MITM) vulnerabilities. Threats to data when in transit, such as interception and message modification using wireless medical sensor networks (WMSNs) are discussed by Kumar and Lee [38]. More research needs to be done on how to secure AR applications and sensors used in the Telehealth and EMS fields. Providing a secure method of transferring sensitive medical information and patient data using AR systems should help in the future development and adoption of AR devices for EMS and telehealth operations.

2.1.4 Data Output

AR applications collect input from AR device user's real-life environment and overlay output (e.g., visual, audio, or haptic feedback) directly on the AR display [39]. Displaying excessive information and virtual objects could distract the user by taking up too much of the user's field of view (FoV). In case of a security breach in an AR system, a malicious code could display undesired overlapping content, mounting a denial-of-service attack by preventing the user from seeing through the AR headset [40]. An attack on an AR navigation application could also cause deception by forging traffic signs (e.g., speed limits) or covering the real-world objects such as occluding pedestrians [41]. Playing loud sounds or intense haptic may also cause shock or physical injury [42].

Multi-user AR systems often share the same virtual space so managing access permissions is critical. Access permission, such as view and edit to objects and data in the virtual space, should be assigned according to the role of the users [41]. Additional AR output protections in shared resources, and physical access control to the output interfaces are discussed by Guzman and et. al [23].

2.3 Solutions

Immersive technologies, such as AR, provide unique and personalized experiences. AR applications offer fundamentally new human-machine interactions via novel input and output interfaces. AR systems require continuous sensing of the real-world environment, which often has sensitive data mixed with user input [43]. Hence, AR integrated systems, particularly in telehealth and EMS scenarios, should protect the user privacy.

The common approach to protect AR data input usually involves removing sensitive information which is also called input sanitization [23]. The confidentiality of the data-at-rest is achieved by implementing protected data storage solutions, such as personal data stores (PDS), with managed application access permission control [23]. The existing security solutions for data-in-transit are traditional cryptographic protocols such as Transport Layer Security (TLS) and Virtual Private Networks (VPN). Output access control methods are proposed as a framework on how to prevent adversaries from tampering or spoofing AR outputs, which can compromise user safety [23, 39, 41].

AR management platforms, like Enterprise Mobility Management (EMM), provide additional security services, such as enforcing policies for device restrictions, settings access control, application vetting, and encryption to protect telehealth and EMS communications [7, 44]. Given the diverse AR device landscape and enterprise AR use cases, EMMs could be deployed to learn and model the true security and privacy requirements for a particular AR application environment.

3 Conclusions

Augmented Reality (AR) systems collect data from real-world environments, which often have sensitive data mixed with user input, posing a risk to privacy. In this survey, we analyzed the vulnerability points in an AR environment using a data flow model as shown in Figure 1. Then we reviewed available solutions and approaches to avert the security and privacy risks in the context of AR integrated telehealth and emergency scenarios, as depicted in Figure 2.

Most of the AR implementations are focused on new use case and proof-of-concept applications for public safety and telehealth [45]. There is an opportunity for further research and development of security technologies for AR systems specifically used in emergency medical services (EMS) and law enforcement operations and tasks. Providing a secure method of transferring sensitive medical information and patient data should help in the adoption of AR devices by EMS agencies and telehealth service providers.

4 Possible Future Research Direction

The common approach today to capturing and transferring data, such as telemetry (GPS/location/other sensor values, etc.), pictures, authentication data, or video images, relies on traditional cryptographic protocols such as Transport Layer Security (TLS) and Virtual Private Networks (VPN). None of these secure-communication solutions ensures the preservation of the integrity of the captured data end-to-end. Such protocols are known to have Man-in-the-Middle (MITM) vulnerabilities. A CSPRI sponsored research could investigate novel solutions to overcome such weakness and protect communications of AR systems in the Telehealth and EMS applications.

Another CSPRI sponsored research could focus on the privacy requirements in Telehealth and EMS, which are briefly discussed in this report. Specifically, this AR security and privacy research would explore the topic from the perspectives of legal compliance, laws and regulations, standards, and frameworks.

ACKNOWLEDGMENTS

The authors would like to thank Dr. Fatih Çömlekoğlu, CTO of AppGuard, John Hanacek, CEO of AvatarMEDIC, Dr. Costis Toregas, Director of Cyber Security & Privacy Research Institute (CSPRI), Dr. Arkady Yerukumovich, Assistant Professor of CS Department at GWU, and Taly Walsh, Assistant Director of Women in Engineering (WIE) at GWU, for their valuable comments and feedback.

REFERENCES

[1] Phil Goldstein. 2020. NIST Promotes Augmented Reality for First Responders. *Technology Solutions That Drive Government*. Retrieved February 11, 2021 from https://statetechmagazine.com/article/2020/06/nist-promotes-augmented-reality-first-responders

[2] Michael Georgiou. 2020. AR in Healthcare: 9 Practical Use Cases with Examples. *Imaginovation*. Retrieved February 11, 2021 from https://www.imaginovation.net/blog/ar-in-healthcare-use-cases/

[3] B. Stanberry. 2000. Telemedicine: barriers and opportunities in the 21st century. *Journal of Internal Medicine* 247, 6 (2000), 615–628. DOI:https://doi.org/10.1046/j.1365-2796.2000.00699.x

[4] Lisa M. Koonin. 2020. Trends in the Use of Telehealth During the Emergence of the COVID-19 Pandemic — United States, January–March 2020. *MMWR Morb Mortal Wkly Rep* 69, (2020). DOI:https://doi.org/10.15585/mmwr.mm6943a3

[5] Judd E. Hollander and Brendan G. Carr. 2020. Virtually Perfect? Telemedicine for Covid-19. *New England Journal of Medicine* 382, 18 (April 2020), 1679–1681. DOI:https://doi.org/10.1056/NEJMp2003539

[6] James R. Langabeer, Michael Gonzalez, Diaa Alqusairi, Tiffany Champagne-Langabeer, Adria Jackson, Jennifer Mikhail, and David Persse. 2016. Telehealth-Enabled Emergency Medical Services Program Reduces Ambulance Transport to Urban Emergency Departments. *West J Emerg Med* 17, 6 (November 2016), 713–720. DOI:https://doi.org/10.5811/westjem.2016.8.30660

[7] Joshua M Franklin, Gema Howell, Scott Ledgerwood, and Jaydee L Griffith. 2020. *Security analysis of first responder mobile and wearable devices*. National Institute of Standards and Technology, Gaithersburg, MD. DOI:https://doi.org/10.6028/NIST.IR.8196

[8] Scott Moore. 2018. Data Privacy. *American Ambulance Association*. Retrieved January 15, 2021 from https://ambulance.org/2018/06/01/data-privacy/

[9] Heather Landi. 2020. Inova Health System latest hospital impacted by ransomware attack on software vendor. *FierceHealthcare*. Retrieved May 3, 2021 from https://www.fiercehealthcare.com/tech/inova-health-system-hit-by-software-vendor-breach-impacting-1m-people

[10] Fred Langston. Recent Spike in Healthcare Breach Reports Due To Blackbaud Ransomware Attack. *CI Security*. Retrieved May 3, 2021 from https://www.criticalinsight.com/resources/news/article/recent-spike-in-healthcare-breach-reports-due-to-blackbaud-ransomware-attack

[11] Jacqueline LaPointe. 2016. MedStar Ransomware Attack Caused by Known Security Flaw. *HealthITSecurity*. Retrieved May 3, 2021 from https://healthitsecurity.com/news/medstar-ransomware-attack-caused-by-known-security-flaw

[12] Hong-zhi Hu, Xiao-bo Feng, Zeng-wu Shao, Mao Xie, Song Xu, Xing-huo Wu, and Zhe-wei Ye. 2019. Application and Prospect of Mixed Reality Technology in Medical Field. *CURR MED SCI* 39, 1 (February 2019), 1–6. DOI:https://doi.org/10.1007/s11596-019-1992-8

[13] Shiyao Wang, Michael Parsons, Jordan Stone-McLean, Peter Rogers, Sarah Boyd, Kristopher Hoover, Oscar Meruvia-Pastor, Minglun Gong, and Andrew Smith. 2017. Augmented Reality as a Telemedicine Platform for Remote Procedural Training. *Sensors* 17, 10 (October 2017), 2294. DOI:https://doi.org/10.3390/s17102294

[14] Konrad L. Davis, Danilo Gasques Rodrigues, Yifei Zhang, Wanze Xie, Janet Johnson, Yuanyuan Feng, Zhuoqun Robin Xu, James Riback, Thomas Sharkey, Michael Yip, and Nadir Weibel. 2019. Augmented Reality Technology to Enable reMote Integrate Surgery (ARTEMIS): a review of technical considerations and study design. Orlando, USA. Retrieved from https://www.artemis.surgery/

[15] Daniel Andersen, Voicu Popescu, Maria Eugenia Cabrera, Aditya Shanghavi, Gerardo Gomez, Sherri Marley, Brian Mullis, and Juan Wachs. 2016. Avoiding Focus Shifts in Surgical Telementoring Using an Augmented Reality Transparent Display. *Medicine Meets Virtual Reality 22* (2016), 9–14. DOI:https://doi.org/10.3233/978-1-61499-625-5-9

[16] B. A. Ponce, E. W. Brabston, S. Zu, S. L. Watson, D. Baker, D. Winn, B. L. Guthrie, and M. B. Shenai. 2016. Telemedicine with mobile devices and augmented reality for early postoperative care. In *2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 4411–4414. DOI:https://doi.org/10.1109/EMBC.2016.7591705

[17] Paolo Bifulco, Fabio Narducci, Raffaele Vertucci, Pasquale Ambruosi, Mario Cesarelli, and Maria Romano. 2014. Telemedicine supported by Augmented Reality: an interactive guide for untrained people in performing an ECG test. *BioMed Eng OnLine* 13, 1 (November 2014), 153. DOI:https://doi.org/10.1186/1475-925X-13-153

[18] M. Carbone, C. Freschi, S. Mascioli, V. Ferrari, and M. Ferrari. 2016. A Wearable Augmented Reality Platform for Telemedicine. In *Augmented Reality, Virtual Reality, and Computer Graphics* (Lecture Notes in Computer Science),

Springer International Publishing, Cham, 92–100. DOI:https://doi.org/10.1007/978-3-319-40651-0_8

[19] Isabel L. Nunes, Raquel Lucas, Mário Simões-Marques, and Nuno Correia. 2018. Augmented Reality in Support of Disaster Response. In *Advances in Human Factors and Systems Interaction* (Advances in Intelligent Systems and Computing), Springer International Publishing, Cham, 155–167. DOI:https://doi.org/10.1007/978-3-319-60366-7_15

[20] George Koutitas, Kenneth Scott Smith, Grayson Lawrence, Vangelis Metsis, Clayton Stamper, Mark Trahan, and Ted Lehr. 2019. A virtual and augmented reality platform for the training of first responders of the ambulance bus. In *Proceedings of the 12th ACM International Conference on PErvasive Technologies Related to Assistive Environments* (PETRA '19), Association for Computing Machinery, New York, NY, USA, 299–302. DOI:https://doi.org/10.1145/3316782.3321542

[21] AR Insider. Smart Glasses: The Road to AR's Holy Grail. *ARtillery Intelligence*. Retrieved May 24, 2021 from https://artillry.co/artillry-intelligence/smart-glasses-the-road-to-ars-holy-grail/

[22] Parisis Gallos, Charalabos Georgiadis, Joseph Liaskos, and John Mantas. 2018. Augmented Reality Glasses and Head-Mounted Display Devices in Healthcare. *Stud Health Technol Inform* 251, (2018), 82–85.

[23] Jaybie A. De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2019. Security and Privacy Approaches in Mixed Reality: A Literature Survey. *ACM Comput. Surv.* 52, 6 (October 2019), 110:1-110:37. DOI:https://doi.org/10.1145/3359626

[24] Sarah Calams. 2020. 10 things EMS providers need to know about telehealth. *EMS1*. Retrieved June 1, 2021 from https://www.ems1.com/ems-products/mobile-data/articles/10-things-ems-providers-need-to-know-about-telehealth-Kf2qP7eLAWEqXPhE/

[25] Joseph L. Hall and Deven McGraw. 2014. For Telehealth To Succeed, Privacy And Security Risks Must Be Identified And Addressed. *Health Affairs* 33, 2 (February 2014), 216–221. DOI:https://doi.org/10.1377/hlthaff.2013.0997

[26] Timothy M. Hale and Joseph C. Kvedar. 2014. Privacy and Security Concerns in Telehealth. *AMA Journal of Ethics* 16, 12 (December 2014), 981–985. DOI:https://doi.org/10.1001/virtualmentor.2014.16.12.jdsc1-1412.

[27] Carmen Camara, Pedro Peris-Lopez, and Juan E. Tapiador. 2015. Security and privacy issues in implantable medical devices: A comprehensive survey. *Journal of Biomedical Informatics* 55, (June 2015), 272–289. DOI:https://doi.org/10.1016/j.jbi.2015.04.007

[28] VALERIE J. M. WATZLAF, LEMING ZHOU, DILHARI R. DEALMEIDA, and LINDA M. HARTMAN. 2017. A Systematic Review of Research Studies Examining Telehealth Privacy and Security Practices used by Healthcare Providers. *Int J Telerehabil* 9, 2 (November 2017), 39–59. DOI:https://doi.org/10.5195/ijt.2017.6231

[29] How to Comply With the HIPAA Security Rule | Insureon. Retrieved June 1, 2021 from https://www.insureon.com/blog/how-to-comply-with-hipaa-security-rule

[30] Office for Civil. 2008. The HIPAA Privacy Rule. *HHS.gov*. Retrieved June 1, 2021 from https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

[31] Sumit Majumder and M. Jamal Deen. 2019. Smartphone Sensors for Health Monitoring and Diagnosis. *Sensors (Basel)* 19, 9 (May 2019). DOI:https://doi.org/10.3390/s19092164

[32] Dieter Schmalstieg and Tobias Höllerer. 2016. Augmented Reality: Principles and Practice. In *Augmented Reality: Principles and Practice*. Addison-Wesley Professional, 411.

[33] Liang Cai. 2019. Guard Your Data with the Qualcomm® Snapdragon™ Mobile Platform. Retrieved June 2, 2021 from https://www.qualcomm.com/documents/guard-your-data-qualcomm-snapdragon-mobile-platform

[34] Chad Spensky, Jeffrey Stewart, Arkady Yerukhimovich, Richard Shay, Ari Trachtenberg, Rick Housley, and Robert Cunningham. 2016. SoK: Privacy on Mobile Devices – It's Complicated. *Proceedings on Privacy Enhancing Technologies* 2016, (July 2016). DOI:https://doi.org/10.1515/popets-2016-0018

[35] Yushan Siriwardhana, Pawani Porambage, Madhusanka Liyanage, and Mika Ylinattila. 2021. A Survey on Mobile Augmented Reality with 5G Mobile Edge Computing: Architectures, Applications and Technical Aspects. *IEEE Communications Surveys Tutorials* (2021), 1–1. DOI:https://doi.org/10.1109/COMST.2021.3061981

[36] Data Encryption in Transit Guideline | Information Security Office. Retrieved February 26, 2021 from https://security.berkeley.edu/data-encryption-transit-guideline

[37] AJ Kumar. 2017. Network Security Policy - Infosec Resources. Retrieved February 26, 2021 from https://resources.infosecinstitute.com/topic/network-security-policy-part-3/

[38] Pardeep Kumar and Hoon-Jae Lee. 2012. Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. *Sensors* 12, 1 (January 2012), 55–91. DOI:https://doi.org/10.3390/s120100055

[39] K. Lebeck, K. Ruth, T. Kohno, and F. Roesner. 2017. Securing Augmented Reality Output. In *2017 IEEE Symposium on Security and Privacy (SP)*, 320–337. DOI:https://doi.org/10.1109/SP.2017.13

[40] Kiron Lebeck, Tadayoshi Kohno, and Franziska Roesner. 2016. How to Safely Augment Reality: Challenges and Directions. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications* (HotMobile '16), Association for Computing Machinery, New York, NY, USA, 45–50. DOI:https://doi.org/10.1145/2873587.2873595

[41] K. Lebeck, K. Ruth, T. Kohno, and F. Roesner. 2018. Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End Users. In *2018 IEEE Symposium on Security and Privacy (SP)*, 392–408. DOI:https://doi.org/10.1109/SP.2018.00051

[42] Franziska Roesner, Tadayoshi Kohno, and David Molnar. 2014. Security and privacy for augmented reality systems. *Commun. ACM* 57, 4 (April 2014), 88–96. DOI:https://doi.org/10.1145/2580723.2580730

[43] Loris D'Antoni, Alan Dunn, Suman Jana, Tadayoshi Kohno, Benjamin Livshits, David Molnar, Alexander Moshchuk, Eyal Ofek, Franziska Roesner, Scott teSaponas, Margus Veanes, and Helen J. Wang. 2013. Operating System Support for Augmented Reality Applications. Retrieved January 22, 2021 from https://www.usenix.org/conference/hotos13/session/d%27antoni

[44] ThirdEye: Mobile Device Management -Enterprise Level MDM. Retrieved June 4, 2021 from https://www.thirdeyegen.com/mobile-device-management

[45] Nicholas Boyd, Jacob Hawkins, Thomas Yang, and Scott A. Valcourt. 2020. Augmented Reality: Telehealth Demonstration Application. In *Practice and Experience in Advanced Research Computing* (PEARC '20), Association for Computing Machinery, New York, NY, USA, 452–455. DOI:https://doi.org/10.1145/3311790.3399629