HealthManagement.org

LEADERSHIP • CROSS-COLLABORATION • WINNING PRACTICES

VOLUME 22 • ISSUE 6 • € 22

ISSN = 1377-7629

Cybersecurity: Preventing the Worst-Case Scenario

THE JOURNAL 2022

9 771377 756005 06

HOLOGIC®

Minutes Matter

Real-time imaging for instant sample verification during breast biopsy procedures[1-3]

The Brevera® Breast Biopsy System helps you to make informed clinical decisions at the point of care, saving valuable time for a better patient experience.[1-3]

Part of the Hologic Breast Health Continuum of Care

CE 2797

Authorised Representative: Hologic BV, Da Vincilaan 5, 1930 Zaventem, Belgium

References: 1. Hologic data on file. VAR-05326. **2.** Hologic data on file. MISC-07678-EUR-EN. **3.** Hologic data on file. MISC-07662-EUR-EN

Brevera®
Breast Biopsy System

Editorial

Cybersecurity: Preventing the Worst-Case Scenario

Stephen Lieber
Chief Analytics Officer CHIME, USA
HealthManagement.org
Editor-in-Chief, Health IT

As healthcare has become ubiquitously digitised, we have reaped the benefits of more easily accessed and shared patient data. Clinicians know more about their patients' medical history and have digital tools to better assist in diagnosis and care. But this has also increased our risks.

Bad actors and recognising the monetary value of healthcare data are increasingly putting our healthcare practitioners and centres at risk for cybersecurity attacks. High-profile cyberattacks have become all too common for healthcare organisations, and with the continued implementation of network-connected devices, the risk from cyberattacks increases.

According to the 2022 Digital Health Most Wired (DHMW) survey recently released by the College of Healthcare Information Management Executives (CHIME), 97% of healthcare organisations rank security as an essential or high priority in 2023 as they continue to invest in their security capabilities and technology.

These risks are not going unaddressed. The DHMW survey found that among U.S. acute care facilities, 60% of healthcare organisations now have a Chief Information Security Officer (CISO) in place and responsible for information security. This is but one strategy to mitigate these risks.

In this issue, our contributors discuss the importance of **cybersecurity in healthcare** and present examples of efforts underway across the globe to achieve better cybersecurity and ultimately better protect our patients and the facilities that serve them.

Henrique Martins talks about the need for integrated hospital/healthcare organisation interoperability and cyber- and information security plans and the importance of protecting patient data within and in inter-organisational transfer processes.

Vito Petrarolo and Giovanni Maglio discuss measures that can be implemented to limit the likelihood of a breach or reduce its scale and consequences and the need for increased focus on building mission-critical systems with the goal of quickly recovering from both anticipated and unexpected attack scenarios.

Alexios Antoniou talks about the Internet of Medical Things (IoMT) and how it can deliver game-changing benefits to healthcare institutions, patients and society, the challenges IoMT systems face regarding security of interconnected components and recommendations for better security.

In other feature articles, Elisabetta Schiavone, Alessandra Sorrentino, Lara Merighi and co-authors highlight the importance of creating a safe and inclusive workplace for people with migraine and design criteria that can help reduce the presence of triggers.

This issue also includes interviews and articles that discuss strategies and recommendations to improve cybersecurity, unlocking the power of data to transform patient care, diagnosis, treatment and management of syncope, future trends in radiology and healthcare, a new standard of seizure care and transforming the dental industry with dental service organisations.

We hope you will enjoy this issue. As always, your feedback is welcome.

Happy Reading!

Contents

DISCLOSURE OF CONFLICT OF INTEREST:
Point-of-View articles are the sole opinion of the author(s) and they are part of the HealthManagement.org Corporate Engagement or Educational Community Programme.

Get your free subscription!

Subscribe here for FREE

Subscription Rates (6 Issues/Year)
One year: Euro 106 + 5% VAT, if applicable
Two years: Euro 184 + 5% VAT, if applicable

Production & Printing
Total circulation 50,000
ISSN = 1377-7629a

Legal Disclaimer
The Publishers, Editor-in-Chief, Editorial Board, Ambassadors and Editors make every effort to ensure that no inaccurate or misleading data, opinion or statement appears in this publication. All data and opinions appearing in the articles and advertisements herein are the sole responsibility of the contributor or advertiser concerned. Therefore the Publishers, Editors-in-Chief, Editorial Board, Industry and Regional Ambassadors, Editors and their respective employees accept no liability whatsoever for the consequences of any such inaccurate or misleading data, opinion or statements.

Verified Circulation
According to the standards of International Business Press Audits.

HealthManagement.org
is independently audited by TopPro Audit

Contents

DISCLOSURE OF CONFLICT OF INTEREST:
Point-of-View articles are the sole opinion of the author(s) and they are part of the HealthManagement.org Corporate Engagement or Educational Community Programme.

Contributors

Alexios Antoniou,
Cyprus

Alexios Antoniou is a cybersecurity consultant currently working at KPMG.

Internet of Medical Things: Threats and Recommendations 325

Joerg Aumueller,
Straumann Group

In his role as Vice President, Global Head of Enterprise Solutions at the Straumann Group, Joerg Aumueller focuses on developing enterprise solutions for dental service organisations (DSOs) by enhancing customer co-creation in digital transformation of DSO business and dental delivery models, and establishing transformational services to streamline dental operations.

Stability in the Face of Change 345

Dan Brown,
Agfa HealthCare

Dan Brown is Chief Technology Officer at Agfa HealthCare, overseeing the technical development of the Enterprise Imaging Solution, setting the technology direction and leading the Research and Development organisation. Dan is a high-performing business leader possessing unique global systems and engineering experiences.

Challenges, Strategies and Recommendations to Improve Cybersecurity 314

Elena Ruiz de la Torre,
Spain

Elena Ruiz de la Torre is a leading patient advocate and researcher. She leads the European Migraine and Headache Alliance, a nonprofit patient umbrella group that represents 33 patient groups from across the continent. She also co-led the creation of WHAM, the World Health and Migraine organisation, a patient-led coalition open to patient groups around the world.

How to Create a Migraine-Friendly Workplace 334

James Frith,
UK

James Frith is an academic geriatrician in Newcastle's Falls and Syncope Service. He has a particular interest in orthostatic hypotension, falls and non-pharmacologic treatments. He completed a five year NIHR Clinician Scientist fellowship evaluating non-drug therapies and their application and is now performing a trial in people with OH.

Syncope Diagnosis, Treatment and Management 329

Mathias Goyen,
GE Healthcare

Prof Mathias Goyen is the Chief Medical Officer, Europe, The Middle East & Africa for GE Healthcare. He is responsible for leading medical, clinical and evidence generation strategies for product modalities and provides leadership in healthcare economics, outcomes research and comparative effectiveness research for new and existing products.

Future Trends in Radiology and Healthcare 340

Tim Hill,
Agfa HealthCare

Tim Hill is the Global Information and Security Program Manager at Agfa HealthCare and supports the different business units in securing their processes, products and internal IT infrastructure. Tim has held many high level IT management positions with global experience across multiple sectors.

Challenges, Strategies and Recommendations to Improve Cybersecurity 314

Rowland Illing,
USA

Dr Rowland Illing is the Chief Medical Officer and Director of International Government Health for AWS. He has responsibility for public sector healthcare strategy and operations encompassing healthcare service delivery, research and genomics.

Unlocking the Power of Data to Transform Patient Care 322

Jarius Jackson,
Agfa HealthCare

Jarius Jackson is the Data Protection Officer and Security & Privacy Specialist at Agfa Healthcare, providing daily direction on data privacy topics and strategically increasing security awareness within the organisation. Jarius is an experienced business leader possessing a multidisciplinary skillset from his background in various industry sectors.

Challenges, Strategies and Recommendations to Improve Cybersecurity 314

Stephen Lieber,
USA

Stephen Lieber is the Chief Analytics Officer at The College of Healthcare Information Management Executives (CHIME). Lieber served as President and CEO of the Healthcare Information and Management Systems Society (HIMSS) for 17 years. He is a consultant and technical and business advisor to several associations and companies.

Editorial: Cybersecurity – Preventing the Worst-Case Scenario 298

Giovanni Maglio,
Italy

Giovanni is a lawyer and focuses his practice on digital transformation, data protection and cybersecurity in healthcare sector. He is Lead Auditor ISO/IEC 27001/2013 and teaches at university level. He is also author of several publications and participates in research projects on the above mentioned topics.

Cybersecurity: Preventing the Worst-Case Scenario 314

Henrique Martins,
Portugal

An internist MD, Management PhD and Master in Law, Prof Martins headed SPMS (Portugal), leading numerous nationwide eHealth projects and co-chaired the EU eHealth Network. He consults and teaches on Digital Health, health transformation, management and leadership.

Is it Safe to Exchange Data? The Need for Hospital/Healthcare Organisation Interoperability and Cyber- and Information Security Plans 308

Stephen Mayer,
USA

Stephen Mayer is the Director of Neurocritical Care and Emergency Neurology Services and Professor of Neurology and Neurosurgery. He is also a paid consultant for Ceribell.

Point-of-Care EEG in the ICU: Towards a New Standard of Seizure Care 342

Lara Merighi,
Italy

Lara Merighi is the National Coordinator of Alleanza Cefalalgici, Al.Ce. Group Italy CIRNA Foundation Onlus. She is in promoting training and information and giving support to patients suffering from headaches, in particular, migraine. She is Coordinator of the Support Forum on cefalea.it, promoter and organiser of conferences on headaches and participates in activities of the National Reference Guidelines for the Prevention and Treatment of headache in adults.

How to Create a Migraine-Friendly Workplace 334

Vito Petrarolo,
Italy

Vito has wide experience in planning and development of data warehouse and business intelligence systems about healthcare. He is currently Chief Digital Officer and Digital and Privacy office Manager in Health and Social Care Agency of Apulia (AReSS), and project manager of the "Telemedicine Operations Center for Chronic Conditions and Clinical Networks" (COReHealth) of Apulia Region.

Cybersecurity: Preventing the Worst-Case Scenario 317

Giorgio Sandrini,
Italy

Giorgio is former full professor of neurology in the University of Pavia, Italy. He was Chairman of the Department of Neurology and Neurorehabilitation at the Institute of Neurology, "C. Mondino" Foundation, and Director of University Centre for Adaptive Disorders and Headache (UCADH). His main research fields include headache, neurophysiology of pain and neurorehabilitation. He has published more than 300 articles concerning these topics.

Increasing Care Demand and Growing Workforce Shortage 334

Elisabetta Schiavone,
Italy

Elisabetta Schiavone is an architect and PhD in Technological Culture and Environmental Design at High School "G. D'Annunzio", Chieti Pescara University. Her research interests include universal design, inclusive safety and inclusive emergency management. She's partner and technical director of "Soluzioni Emergenti.

Reducing Burnout by Building Resilient Systems 334

Alessandra Sorrentino,
Italy

Alessandra Sorrentino is representative of the Alleanza Cefalalgici (Al.Ce.) in the European Headache & Migraine Alliance and blogger of "Le parole dell'emicrania". She has suffered from migraine since she was four. Two years ago she took the first steps towards her path of advocacy. Her aim is to support people with migraines by giving them accurate information about the disease, drug therapies and non-pharmacological strategies.

The Shortage of Health Professionals Worldwide – A Modern Human Resources Management Challenge 334

Upcoming Issue

Cover Story:

(non)Profitability in Healthcare

The goal of any healthcare facility is to provide quality care, improve patients' quality of life and ensure everyone gets the health services they need. How can healthcare organisations continue to afford to provide care? How can they balance costs and quality? How can they ensure access to all - those who can afford care and those who cannot? How can they continue to fund medical education and research?

Submit your abstract to
edito@healthmanagement.org

Editorial Board

Is it Safe to Exchange Data?

The Need for Integrated Hospital/Healthcare Organisation Interoperability and Cyber- and Information Security Plans

Henrique Martins | Associate Professor | ISCTE Business School | ISCTE-IUL, Lisbon | Faculty of Health Sciences | Universidade da Beira Interior | Covilhã, Portugal

One of the biggest health organisation challenges is to protect patient data within but also, and increasingly, in inter-organisational transfer processes. This challenge brings together three interconnected topics which are very important for effective, efficient, safe, sustainable and high-quality healthcare.

Key Points

- Patients can be at risk of harm due to breach in the safety of clinical procedures as well as when data and information systems security is breached.
- Different roles and multiple leadership is needed for a balanced approach to data usage and data security and protection.
- HL7® FHIR® does not increase risks for cyber- and information security.
- HoF (Hospitals/Healthcare Organisations on FHIR) can serve as a community of practice to stimulate further learning and cross-EU sharing and trust building.

Patients can be at risk of harm due to breach in the safety of clinical procedures as well as when data and information systems security is breached. They are equally at risk when information about them is not shared across the continuum of care, or research and new discoveries are delayed, new treatment solutions/approaches are not fund because of barriers to data sharing. Barriers to data exchange can cause the loss of lives or less optimal care.

One of the biggest health organisation challenges is to protect adequately patient data inside them but also, and increasingly, in inter-organisational transfer processes. This challenge brings together three interconnected topics which are very important for an effective, efficient, safe, sustainable and high-quality healthcare.

Different leadership roles are necessary for dealing with the interplay between digital transformation interoperability security and data protection as there is a constant need to balance four (only apparently) conflicting demands regarding healthcare organisational health data usage: 1) the needs of the Clinical Information Leads, 2) the needs of researchers who need to access data for secondary use; 3) the responsibilities

of personal data protection; 4) the cyber- and information security needs.

An integrated approach to interoperability at the organisational level with cyber- and Information security is needed to pave the way to the design and adoption of a truly effective Hospital/Healthcare Organisation Interoperability and Cyber – and Information Security (HICIS) Plan. Such document(s) should be the ongoing and live record and output of a joint collection of efforts.

Even though it doesn't impose any security model, the HL7 FHIR standard provides considerations on time keeping; communications security; authentication; authorisation/access control, audit, digital signatures, security labels; data management policies, and security/privacy event. The expectation of HL7 FHIR is in fact that the application of those security models does not impact the actual goal of HL7 FHIR that is enabling data sharing through an agreed health data model. Moreover, the Hospitals-on-FHIR (HoF) community of practice can be a forum for sharing not only best practices in interoperability but also on how it links to cyber- and information security as well as data protection.

Introduction

In most countries in the world, the population is growing old (OECD 2018), which, associated with unhealthy lifestyles and increased healthcare needs, is leading to healthcare systems sustainability challenges (OECD 2019). Health 4.0 (Bause et al. 2019) means a possibility for organisational change through the implementation of new digitalisation strategies and advanced information technologies. These, however, come with a new ever-increasing risk of "damage" to information. Cyber-attacks that impact or are directed to health units are ever more frequent due to the critical and intrinsic value of the information about humans which they harbour. There are multiple examples, often hitting public opinion and trust as they are mediatised. The Ransomware WannaCry, in 2017, led to British National Health Service disruption of service with over 20,000 appointments cancelled and estimated costs of 90M£. Recently, a cyberattack hit the second-biggest hospital in Czech Republic amid the coronavirus outbreak (Bîzg 2020). As a result of the attack on SingHealth, over 1.5 million patient personal data and medical records of over 160.000 appointments, including the prime minister's data, were exfiltrated in Singapore, a country known for its advanced cybersecurity policy, strategy and practices. These illustrate that healthcare can suffer in large cyberattack events even in countries with renowned national cross-sectorial cybersecurity capabilities and strategies, as it poses specific challenges. This can justify that special attention is needed within national defence strategies.

The increased digitalisation and datafication of health and care cannot be stopped, slowed down or even put into question due to fears of clinical harm in the face of raising concerns about the cybersecurity of health organisations and health systems. The way forward is to push for more, better efforts in both patient safety as well as cybersecurity, understanding that digital health indeed brings new risks as well as opportunities for patient safety, but inversely, patient safety methodologies and principles can inspire new ways of thinking in cybersecurity for health.

Different leadership roles are necessary for dealing with the interplay between digital transformation, interoperability, security, and data protection

The European Commission talks about cybersecurity as a "set of concerns and actions taken to protect cyberspace, both in the civil and military domains, against threats resulting from the interdependency of its information infrastructures and networks". It helps us as it places the cybersecurity realm into that of policy, leadership, managerial and even academic, concerns and not just actions. Sharing concerns about the topic is already a way to foster cyber resilience.

Digital Health is a priority worldwide, reiterated by the World Health Organization (WHO) and put into evidence by the COVID-19 pandemic response in all countries. Recently the WHO Europe announced its Regional Action Plan, which reinforced the idea that digitalisation and digital transformation of health and care is expected to increase the quality of care and clinical safety. Such safety is ever more univocally dependent on information systems security. A larger use of these technologies brings more efficiency and effectiveness to health and care, but the increasing dependency of productive processes on digital platforms expands risk surface and risk exposure. As healthcare digitalisation progresses, tampered information systems will lead to increasing problems in health and care services and with higher potential and real impacts on individual human health. It is, therefore, paramount to break this

negative cycle, thus enabling healthcare professionals and patients to take full advantage of the digitalisation of the health industry. This explains why there is a more declared interest of governments and health organisations in cybersecurity. There is, however, a severe lack of strategising, implementation of concrete actions and broad awareness of the severity of the matter. There is also a need to understand cybersecurity in the context of cyber- and information security interplay with interoperability needs and the concreteness of where these issues raise more pre-eminently – that is, in large healthcare organisations.

There should be no trade-off between minimum cybersecurity and patient safety. This is particularly relevant for telemedicine services. If a service requires privacy and security standards to be lowered, this service should not be performed as the risks associated with privacy and security breaches are high, and two types of consequences can be problematic: reputational and liability issues may arise to the hospital or other healthcare provider, and, more importantly, patient safety can be at risk. Security breaches can pose risks not just to patients and healthcare providers but, more generally, to the development of digital health as trust and goodwill may be eroded.

However, there is a need to move quickly to digital healthcare systems in all countries. Cybersecurity concerns should not stop this but rather increase its urgency. Developing and deploying eHealth services that fit and optimise existing healthcare systems is crucial to improve their performance, access, comfort and efficiency.

One of the biggest health organisation challenges is to adequately protect patient data within but also, and increasingly, in inter-organisational transfer processes. This challenge brings together three interconnected topics which are very important for effective, efficient, safe, sustainable and high-quality healthcare:

a) Healthcare cannot continue to be provided in stove pipes and isolated levels of care but rather in an integrated, holistic manner;
b) For a) to be enabled by coherent patient data, information systems have to be interoperable, allowing data exchange between all types of health institutions and the citizen's home;
c) For b) to be realised without service disruption, data modification, exfiltration or loss, the highest possible levels of cybersecurity must be in place. This, however, without limiting what was outlined in a) and without making interoperability described in b) a technical and economically unsustainable effort.

As interoperability and interconnections increase at a global scale, additional threats to data integrity will result from networks of health information between organisations and countries with different maturity levels, different attack surfaces and distinct technical and political vulnerabilities. Adequate security strategies, which include a solid data-sharing policy and inherent information exchange requirement, and a cybersecurity architecture, are needed for health organisations to be able to ensure confidential data is properly protected while shared when needed.

An integrated approach to interoperability at the organisational level with cyber- and information security needs to exist

Leadership and Information Management in Hospitals/Healthcare Organisations

While roles like that of the Chief Information Officer (CIO) or similar posts often under names like Director for IT (Information Technology) or IS (Information Systems), or Data Protection Officer (DPO) are well established, in governance frameworks like COBIT® or even through legislation (the General Data Protection Regulation, in the EU), others may be less well-known or even under-recognised as crucial in the proper management of information in large complex healthcare organisations. These include roles like a dedicated officer to cyber and information security – the so-called CISO, as well as Clinical Information Leads.

The CISO - Chief Information Security Officer – who does not necessarily need to be a staff member of the IS directorate, nor a technical person, as cyber- and information security includes but does not limit itself to digitally supported information and practices, is the person who ultimately is responsible for ensuring information integrity of the hospital or other healthcare organisation.

The clinical leads include, as a minimum (even if operating at a part-time capability), three important roles, the CMIO, CNIO and CPIO. The Chief Medical Information Officer (CMIO) is a medical doctor operating as an organisational boundary spanner between clinical and information systems directorates, to promote medical information representation needs

and all clinical aspects related to the use of IS. The Chief Nursing Information Officer (CNIO) equally acts to bridge between nursing and remaining non-medical informational needs, in articulation with the CMIO, to align the organisational multidisciplinary usage of information systems. Finally, the Chief Pharmacist Information Officer (CPIO) is a key player in ensuring closed-loop medication, appropriate drug and electronic prescription strategies, as well as several roles in digital approaches to patient safety.

Need for a Balanced Approach to Primary and Secondary Use of Health Data in Hospitals or Other Healthcare Organisations

There is a constant need to balance four (only apparently) conflicting demands regarding healthcare organisational health data usage:

1. The needs of the Clinical Information Leads, who represent genuine functional and business interests of clients (often patients) and healthcare professionals, encompass the highest possible Quality-of-Care demand for data exchange and interoperability to ensure better and more integrated care, including between organisations nationally and cross-border – primary use of health data.
2. The needs of researchers who need to access data for secondary use to promote internal but ever more increasingly interoperable research both inside the country in research networks but more importantly, EU-funded research and cross-border research efforts, paving the way to contributions to European Health Data Space related projects – secondary use of health data.
3. The responsibilities of personal data protection, incarnated by the DPO figure, are often more strongly empowered than the previous due to a clear legal basis for their role, and whose roles and responsibilities are relatively well established across the EU, although we see a wide range of more liberal or too conservative interpretations of similar situations rendering a too high degree of uncertainty to inter-organisational projects that may involve data sharing.
4. The cyber- and information security needs, seeking to secure information and critical information security systems, too often to the expense of practicality and health professionals' work effort and comfort or inducive of disproportional blockage to data sharing.

Finally, in most organisations the figure of a sort of Chief Interoperability Officer is completely absent. They could be the missing link between the four aforementioned demands. For now, and in most organisations, this role is to be played by a well-educated and well-prepared CIO. Interoperability, understood in its broadest sense and not limited to the technical layer but to include the legal, organisational and semantic (following the LOST model underneath the Refined eHealth European Interoperability Framework) needs to be seen as a cultural and procedural effort that is transversal to the organisation preparing it to cross-country and cross-border data sharing and care integration.

The HICIS Plan: Hospital/Healthcare Organisation Interoperability and Cyber – and Information Security Plan

Having a LOST-inspired plan to tackle the interplay between interoperability and cyber- and information security helps to align different dimensions, such as and not exclusively:

1. Technical alignment – If the technologies that are set up, in particular, the standards used and how they interrelate, are not promoting both data exchange and data security, professionals will find a (not so secure) way to exchange data if that is critically needed for patient care and do some not so good use of health data for research if the need is pressing.
2. Procurement alignment – If different parts of the organisation buy technologies or consult on processes which are not acting synergically, once the commitment to buy is firmly established it is followed by an implementation tension that leads to conflicts.
3. Education alignment - Education of internal and subcontracted IT staff as well as IT providers on the matters of interoperability, cyber- and information security, and data protection needs to be planned and considered holistically so that messages are consistent and coherent and not conducive to further tension raising. Clinical staff should also be included in such educational initiatives to help bridge the gaps between subcultures but also different needs.

When such an integrated approach to interoperability at the organisational level with cyber- and information security exist, we can talk about a truly effective HICIS Plan: Hospital/Healthcare Organisation Interoperability and Cyber – and Information Security Plan. Such document(s) should be the ongoing and live record and output of the joint efforts of two teams and focus of attention within the directorates for information systems: the interoperability team and the cyber- and information security team, both operating under the Chief Information Officer (CIO) or similar post but with dynamic and intense interrelations with Clinical Information Leads and the Data Protection Officer (DPO).

HL7® FHIR® and Cyber- and Information Security and the HoF Community

As explicitly indicated in the standard (http://hl7.org/fhir), HL7 Fast Healthcare Interoperability Resources (FHIR) is "not a security protocol, nor does it define any security-related functionality". This, at first glance, may seem a shortage, but is, on the contrary, a point of strength, allowing the adoption of various security protocols and models based on the interoperability paradigm chosen (e.g. document, REST, messages, services) and the context requirements (e.g., enterprise vs patient vs cross-enterprise centric model).

The expectation of HL7 FHIR is, in fact, that the application of those security models does not impact the actual goal of HL7 FHIR, that is, that of enabling the sharing of data through an agreed health data model.

Even though it doesn't impose any security model, the HL7 FHIR standard provides considerations on timekeeping, communications security, authentication, authorisation/access control, audit, digital signatures, security labels, data management policies, security/privacy event reporting and other related topics; documenting them in the HL7 FHIR standard security page.

Moreover, the standard defines specific FHIR resources as Provenance, Consent and AuditEvent, and metadata elements (e.g. security labels) for better supporting the adopted models. Additional and more detailed reflections on cybersecurity aspects associated with the HL7 FHIR standard can be found on their blog.

A community-of-practice approach to interoperability, cyber- and information security and data protection is perhaps the best way to help leaders deal with and learn from each other in such complex interconnected matters. The HoF (Hospitals/Healthcare Organisations on FHIR) constitute a growing community of practice promoting the use of interoperability standards and the exchange of experiences in how best to use the HL7® FHIR® standard and ultimately also the experiences around data sharing and, in the EU, the promotion of the generalised use of the European Electronic Health Record Exchange format (EEHRxF). Members of HoF have progressively asked to see a more intense discussion of the interplay between interoperability, in particular the use of FHIR and cyber- and information security, as well as data protection issues. This will be sought in the coming annual work plan of the HoF for 2023 as part of regular online sessions starting in January 2023.

Acknowledgment

The author would like to acknowledge the kind contribution of Giorgio Cangioli to the part of the article about HL7®FHIR® and information security, as well as Catherine Cronaki's and Valentina Tageo's continuous efforts to build and enlarge the HoF Community (www.hospitalsonfhir.eu).

Conflict of Interest

None. ■

REFERENCES

Bause M, Khayamian Esfahani B, Forbes H, Schaefer D (2019) Design for Health 4.0: Exploration of a New Area. Proceedings of the Design Society: International Conference on Engineering Design. 1(1):887–96.

Bîzgă A (2020) Mysterious cyberattack cripples Czech hospital amid COVID-19 outbreak. Available at https://www.bitdefender.com/blog/hotforsecurity/mysterious-cyberattack-cripples-czech-hospital-amid-covid-19-outbreak

OECD (2018) OECD Regions and Cities at a Glance. p. 160.

OECD (2019) Health at a Glance 2019.

Cybersecurity:
Preventing the Worst-Case Scenario

Challenges, Strategies and Recommendations to Improve Cybersecurity

Dan Brown | Chief Technology Officer | Agfa HealthCare
Tim Hill | Global Security and Privacy Program Manager | Agfa HealthCare
Jarius Jackson | Data Protection Officer & Security & Privacy Tech Specialist | Agfa HealthCare

Cybersecurity is vital for the effective functioning of healthcare organisations and protecting private and important patient information and data. HealthManagement.org spoke to Dan Brown, Chief Technology Officer, Tim Hill, Global Security and Privacy Program Manager and Jarius Jackson, Data Protection Officer & Security & Privacy Tech Specialist at Agfa HealthCare, to discuss the main challenges customers face regarding cybersecurity and what strategies they can implement to protect themselves against cybersecurity attacks.

Key Points

- A major ransomware attack can cripple an organisation and cost millions of dollars/Euros to recover from.
- Each healthcare organisation should create principles to be secure by default and by design.
- A single, unified enterprise-wide image management system not only provides health systems with improvements in productivity and workflows, but also reduces the total number of systems handling sensitive data.
- Agfa HealthCare's security patch management policy keeps the confidentiality, integrity and/or availability risks introduced by security vulnerabilities under control to help protect patient safety and privacy.
- Agfa HealthCare became one of the first companies to be named Cybersecurity Transparent Leader by KLAS Research and Censinet, recognising the company's willingness to continually improve cybersecurity maturity and support customers in the delivery of safe and secure patient care.

What are the main challenges and worries of your customers with regard to cybersecurity? Are the issues customers are facing similar around the globe? Or do you see differences?
Dan Brown: Major ransomware attacks are a key concern of our customers. A major ransomware attack can cripple a health organisation and cost millions of dollars/Euros to recover from – if at all, depending on their preparedness for major events. We have found through customer meetings that some customers are quite well prepared for business continuity scenarios, like a fire in a data centre, but not always equally prepared for ransomware attacks. Agfa HealthCare is continuing to find new ways to work with our customers to create both the awareness and the playbook that

is periodically practiced for what to do in event of a cyber emergency.

improvements in productivity and workflows, but they also reduce the total number of systems handling sensitive data. This means they have fewer gates to guard, with fewer access points and fewer opportunities for breach. Without Agfa's Enterprise Imaging, most customers have several different departmental solutions and even individuals storing data on their local PCs – each of which has to be secured by the hospital's IT staff. The unified Enterprise Imaging Platform also reduces the time that most hospital IT teams spend. Money is not wasted integrating multiple solutions and manually transferring data from siloed locations, simplifying the normally complex world of imaging information management. This allows Agfa's customers to focus security efforts and resources where they will have the most impact.

it will become mandatory in the U.S. We created additional tooling and process improvements to provide better visibility into not only Agfa's homegrown-software but also the potential vulnerability impact of third-party libraries and components used with the EI system.

As part of Agfa's vulnerability management programme, Enterprise Imaging systems are hardened using Security Technical Implementation Guidelines (STIG) from the Centre for Internet Security (CIS) and the Defense Information Systems Agency (DISA). Before delivery to customers, each system is scanned at both the operating system and application level, using industry standard tools. Through means of static code analysis, refresh training for development staff, and a targeted focus on OWASP development

With a single, unified enterprise-wide image management system, health systems not only have improvements in productivity and workflows, but they also reduce the total number of systems handling sensitive data

Do customers take cybersecurity risks seriously enough? Is it a top priority for your customers?
Tim Hill: It's on the minds of most organisations, regardless of their size. The challenge most organisations have is that they are often confronted with difficult trade-offs on how they spend their limited resources.

The reality is that malicious actors are out there, and they are getting more and more crafty. This constantly challenges organisations like Agfa HealthCare, our partners, and our customers. They have to be pragmatic and determined in their defence, approach, business planning and strategic alliances with partners, vendors, and suppliers, to make sure that if an unfortunate event happens, they can recover from it quickly to enable their systems and the services they provide to continue to be available. This is something Agfa HealthCare itself truly targets, making sure we're supporting the delivery of the best patient care and a stable and secure solution so that our customers will look at us with confidence and trust.

From a holistic and preventive point of view, how does Agfa team up with its customers to provide a secure solution?
DB: With a single, unified enterprise-wide image management system, health systems not only have

More practically, how are you helping your customers, which include large hospital networks, to protect themselves against cybersecurity attacks?
Jarius Jackson: We created a ransomware playbook that is both internally and externally facing. We have been meeting with customers to understand their concerns and challenges and offer advice. We developed and posted the Security Vulnerability Notifications for Enterprise Imaging on Agfa's customer portal for transparency and communication. We developed an SBOM (Software Bill of Materials) showing all of the components used in our software well ahead of when

principles, Agfa HealthCare has increased its vigilance being secure by design.

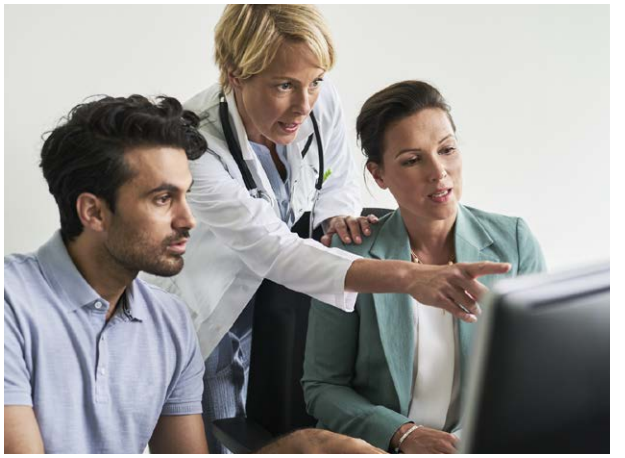
How do you keep up to date with ever-evolving security threats? How do you manage to stay ahead of the threats?
TH: Constant vigilance. This takes consistent and sustained effort from our teams inside Agfa HealthCare to stay on top of the constantly evolving landscape of security threats. We regularly scan our product for new vulnerabilities in our code and in all third-party add-ons we sell. We create our solutions to be safe by design, and we keep rigorous training for our employees, so they are at the top of their game to secure our customers.

You collaborate with KLAS Censinet on their Cybersecurity Transparency Leader initiative. Can you explain a bit more about this initiative?
JJ: KLAS Research and Censinet are strategic partners on a joint mission to improve cybersecurity preparedness in healthcare. They aim to help healthcare IT vendors and services firms improve their overall risk and security profile by driving greater trust and transparency to thousands of healthcare providers. They have assessed and rated more than 130 healthcare products on the Censinet RiskOps platform. Agfa HealthCare became one of the first companies to be named Cybersecurity Transparent Leader by KLAS Research and Censinet. This award recognises our company's willingness to share and continually improve overall cybersecurity maturity and our commitment to supporting customers in delivering safe and secure patient care. This isn't a one-time certification, but something we must stay on top of and work to improve upon each year.

There are several ISO certifications that include cybersecurity topics and a series of regional privacy regulations that you must consider. Does this multitude of regulations complicate your work with regard to cybersecurity and prevention?
TH: While Agfa HealthCare is committed to investing in what is needed to stay on top of all of these certifications, we also look to work smart, not just hard. Despite the variety of certifications, most are core security principles, so we commit to certifications where required in the regions we do business in. We prioritise the privacy and handling of sensitive data and ensure our solutions are designed and implemented to enable healthcare organisations to provide the best and most secure patient care possible.

As a conclusion, what would be your recommendations for hospitals and healthcare professionals to protect themselves from cybersecurity attacks?
TH: Each healthcare organisation should create principles to be secure by default and by design. Work with your IT partners to design a robust and secure solution upfront. As mentioned at the beginning, our experience from customer meetings, both before and after ransomware attacks, is that they usually cater quite well for disaster scenarios, like a fire in their data centre, but less so for ransomware attacks. Some practical advice and best practices include:

- Wherever possible, reduce complexity by minimising the number of unique systems.
- Make sure that your backups are segmented from your production infrastructure. We recommend investigating in immutable backup options.
- Regular vulnerability tests for systems exposed to the outside (i.e. penetration tests).
- Effective system life cycle management - keep your systems current in terms of supported versions. Too often, we see cases where legacy systems are still being used, running on unsupported platforms with no security updates.
- Awareness training for staff – In most organisations, mistakes made by individuals via phishing or loading unauthorised software or media from outside their organisation are the most commonly exploited entry points, not always high-tech hackers like we see in the movies.
- Develop Business Continuity Plans (BCP) to include a cyber-attack scenario.
- Invest in cyber insurance.
- Also, we recommend that organisations should dedicate 10-15% of their IT budget to Information Security and Privacy initiatives.
- Consider gaining a security certification like ISO 27001. The focus of the ISO 27001 standard is on a company's Information Security Management System (ISMS), which outlines how they have integrated information security into its business processes. ■



Cybersecurity: Preventing the Worst-Case Scenario

Vito Petrarolo | Chief Digital Officer and Digital and Privacy Office Manager | Health and Social Care Agency of Apulia (AReSS) | Project Manager | Telemedicine Operations Center for Chronic Conditions and Clinical Networks (COReHealth) | Apulia Region | Italy
Giovanni Maglio | Lawyer | AReSS Digital Transformation System Executive | Lead Auditor | ISO/IEC 27001/2013 | Italy

Cyber threats and vulnerabilities cannot be completely eliminated as no informatic system is completely impenetrable. However, certain measures can be implemented to limit the likelihood of a breach or reduce its scale and consequences. Effective leaders must focus on building mission-critical systems with the goal of quickly recovering from both anticipated and unexpected attack scenarios. Elements of the whole system must be integrated and coordinated to prevent the worst-case scenario.

Key Points

- The increasing digitalisation and systems interconnection in healthcare has left more exposed to and impacted by cybersecurity attacks.
- Cybersecurity must become an integral part of patient safety and should be considered an enabler for ensuring the resilience and availability of key healthcare services.
- The issue of cybersecurity is becoming a pervasive bullet on the agendas of healthcare companies and public administrations.
- Cybersecurity and personal data protection should not be the result of complying with a legal obligation but a cultural process to be implemented and continuously adapted to the changing reality.

The unstoppable increasing digitalisation and systems interconnection in the healthcare sector has left more exposed to and impacted by cybersecurity attacks. Healthcare is an already targeted sector, and we can expect more to arrive in years to come. The high propensity to pay a ransom, the value of patient records and often inadequate security are the main issues that attract cybercriminals.

Cybersecurity is crucial for patient safety, but it has often been underestimated. This requires that cybersecurity becomes an integral part of patient safety through changes in human behaviour, technology and processes as part of a holistic solution, and it should be considered as an enabler for ensuring the resilience and availability of key healthcare services.

It must not be forgotten that healthcare is a complex system in which multiple, heterogeneous and dynamic factors interact, including the plurality of healthcare services, specialised skills and professional, technical and economic-administrative roles, and the heterogeneity of processes and results to be achieved.

The ongoing drive to integrate systems, especially in the health sector (interoperability), makes the boundaries of the systems themselves ever wider and more

exposed, often involving those structures of organisations that, while not directly handling health data, represent entry points for attacks on the entire system and thus also on sensitive data.

As if this were not enough, the COVID-19 pandemic pushed the health sector to the limit and further highlighted the importance of protecting health services and medical data (personal and non-personal), both from a cybersecurity and data protection perspective.

According to Cost of a Data Breach Report 2022 issued by IBM Security, healthcare sector breach costs hit a new record high, with the average breach increased by nearly USD 1 million (about €953.000) to reach USD 10.10 million (about € 9.530.000). This new target has let the healthcare breach costs the most expensive industry for 12 years in a row, increasing by 41.6% since the 2020 report, followed by financial, averaging USD 5.97 million (about €5.700.000), pharmaceuticals at USD 5.01 million (about €4.780.000), technology at USD 4.97 million (about €4.737.000) and energy at USD 4.72 million (about €4.500.000).

In 2020, the World Economic Forum issued the Global Risks Report, where cyberattacks on critical infrastructure were rated the fifth top risk in the same year, becoming the new normal across sectors, among which, of course, healthcare stands in pole position. Such attacks have affected entire cities, and public and private sectors alike are at risk of being held hostage by organised cybercrime entities which are joining forces, even because their likelihood of detection and prosecution is estimated to be as low as 0.05% in the United States (Eoyang et al. 2018).

Thus, the issue of cybersecurity is becoming a pervasive bullet on the agendas of healthcare companies and public administrations, in view of the fact that they are considered critical infrastructures by almost all governments, and even due to the large spikes in malware in 2021: healthcare (121%) and government (94%), as SonicWall stated in its 2022 Cyber Threat Report.

Furthermore, the recent regulatory changes in the European Union, including the NIS (Network and Information Security) Directive (EU) 2016/1148, the European Regulation 2019/881 (the so-called Cybersecurity Act), the General Data Protection Regulation 2016/679 (EU) known as GDPR, and the so-called NIS2, just approved by the European Parliament, are part of this trend where cybersecurity is an integral part of Europeans' security, as clearly affirmed in the EU's Cybersecurity Strategy for the Digital Decade issued at the end of 2020.

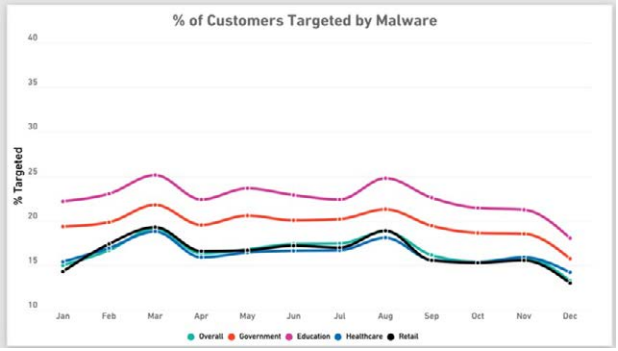


Figure 1: Customers targeted by malware. Source: SonicWall 2022 Cyber threat report

From an Italian perspective, the legal framework is quite composite and spans from the transposition of the European Directive to several internal regulatory acts, including the one establishing the National Cybersecurity Agency (ACN) and the one imposing the implementation of the National Framework on Cybersecurity for Public Administration, based on NIST Cybersecurity Framework. These regulatory standards are valuable tools, as well as unmissable opportunities to facilitate change.

At this stage, while a lot of professionals strive for additional governmental regulation to ensure patients and their data are protected, many healthcare leaders understand that voluntary compliance with the strictest standards is the only way to avoid further and, sometimes, onerous compliance regulations.

In this context, AReSS (Regional Strategic Health and Social Agency of the Apulia Region), which is part of the wider regional healthcare system, has decided to set its security posture according to this principle because cybersecurity and personal data protection should not be the result of complying a legal obligation, but a cultural process to be implemented and continuously adapted to the changing reality.

From the point of view of IT security, the Apulia Region, located in the south of Italy, in which the organisation AReSS is based, uses the cloud service provider Innovapuglia, an in-house company with 100% public participation. Innovapuglia deals with all aspects relating to the security of information systems, from the network to the cloud.

AReSS is entrusted with the internal management of security. AReSS has pinpointed four pillars on which it has established its security posture for a healthcare sector organisation:

- Increasing visibility
- Improving third-party security
- Raising staff awareness of cyber threats
- Complying with regulation

Security risks cannot be thwarted if they are not known. An attack surface monitoring solution immediately visualises all vulnerabilities associated with cloud solutions within a private network.

The Agency, via an external provider, has created an infrastructural and security audit and assessment service aimed at identifying the priority and necessary interventions to be implemented to raise the level of security and improve the performance of the infrastructure. This assessment involves:

- Listing the risks perceived by the customer and defining the main safety objectives;

Figure 2: Enisa 2022 threat landscape for supply chain attacks

- Verification of the existence and possible evaluation of a risk analysis required by EU; Regulation 2016/679 and related hypothesised countermeasures;
- Verification of the implementation of the AgID (Italian Digital Agency) minimum measures;
- Verification of the suitability of authentication mechanisms;
- Verification of the backup execution methods to evaluate their exposure to malware attacks;
- Verification of the current perimeter or similar security measures;
- Verification of tools to prevent virus/malware infections;
- Check coverage of necessary measures referring to provisions of a general nature of the Data Protection Authority (e.g. regulation about system administrators);
- Threat Intelligence services.

In 2014, IBM reported that 17% of breaches in the critical infrastructure industries were due to supply chain attacks where a third-party business partner was the attack vector, while in 2020, the revelation of SolarWinds already hinted at the potential of supply chain attacks to attackers (and defenders). In recent days, the European Union Agency for Cybersecurity (ENISA) mapping emerging supply chain attacks found 66% of attacks focus on the supplier's code.

These data say that a lot of data breaches occur via a compromised third-party provider. In other words, if incident response efforts only focus on internal cyber threats, the security teams have merely addressed less than half of the risks that facilitate breaches.

Improving the security posture of all third-party vendors requires an orchestrated effort between risk assessments, security assessments and vendor tiering. To this extent, AReSS has set a procedure where the procurement office should check that third parties provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the general security level will meet the requirements set by regulation. As a result, the security and risk management team partners with other offices to prioritise and manage risks to digital supply chains.

Furthermore, the Agency has planned and organised specific training courses for both the personnel involved in data processing and those who do not process the data because these are part of the Agency's security chain. In fact, they can represent potential entry points into the network and, therefore, into computers, and from there, who knows where else.

According to the 2014 IBM Cyber Security Intelligence Index Report, human error was a major contributing cause in 95% of all breaches, usually not directly, but providing access to cybercriminals against their will. More recently, in the 2022 Data Breach Investigations Report by Verizon, the human element continues to drive breaches, involving 82% of breaches; whether it is the use of stolen credentials, phishing, misuse, or simply an error, people continue to play a very large role in incidents and breaches alike. The World Economic Forum's Global Risks Report 2022, cited above, also confirms these estimates: 43% of breaches come from homegrown threats, and 95% of cybersecurity alerts are attributable to human error.

Investment in staff training in public healthcare administration is a key principle by which the principles of digitisation and dematerialisation, but above all, the security of processed data, can be developed. The effectiveness of an organisation's processes is directly related to how consistent its staff is in following these processes and policies. To this end, organisations should provide comprehensive training on IT security measures and the risks involved if staff members do

not comply with these procedures.

For example, AReSS staff is trained to recognise a suspicious email and not to open anything (attachment or embedded link) that could be potentially dangerous. They are also instructed to inform IT if they have any doubts about the authenticity of an email message, even by referring to free cybersecurity resources available online.

At AReSS, we think it's important to develop the ability to recognise that the threat is real; indeed, while it is easy to see how someone with malicious intentions might target a bank or a retail shop to illegally access tangible physical assets, it is often more difficult to see why and how someone might breach the systems of a healthcare organisation. In addition to the periodic training of staff, the Agency, under the guidance of the Chief Digital Officer, has published a series of thematic manuals, including one about cybersecurity and another about personal data protection.

However, the growing concerns about the security of personal data and health IT systems have led to the copious current legislation, trying to regulate in an attempt to create an organic and homogeneous protection system, even though full regulatory compliance is not easy to pursue due to high fragmentation of the legal framework.

Last but not the least, AReSS was partner in an Horizon 2020 European Research Project, named Threat-Arrest (www.threat-arrest.eu), which developed an advanced training platform incorporating emulation, simulation, serious gaming and visualisation capabilities to adequately prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk cyber systems and organisations to counter advanced, known and new cyber-attacks in three different sectors: maritime, energy and healthcare. AReSS was the pilot for healthcare systems and the staff was trained with this online platform.

Conclusion

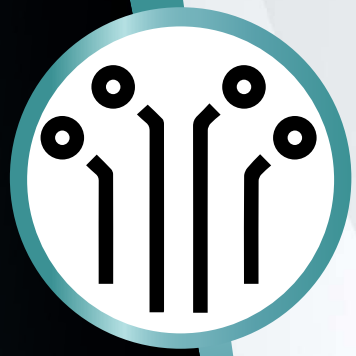
Obviously, threats and vulnerabilities cannot be completely eliminated, so reducing security risks is particularly challenging. While no informatic system is completely impenetrable, there are certain measures that organisations can implement to help limit the likelihood of a breach or at least reduce its scale and consequences. Today's organisation can never hope to entirely avoid security failure, and effective leaders focus on the organisational resilience of mission-critical systems with the goal of quickly recovering from both anticipated and unexpected attack scenarios. All the elements of the whole system must be integrated and coordinated to prevent the worst-case scenario since it is precisely between the folds of such dynamism and heterogeneity that threats and dangers to security may be concealed, aiming for a zero-trust security approach.

Conflict of Interest

None. ■

REFERENCES

Eoyang M, Peters A, Mehta I, Gaskew B (2018) To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors. Third Way.



Successful Digitalisation Pathways

Unlocking the Power of Data to Transform Patient Care

Rowland Illing | Director | Chief Medical Officer | International Public Sector Health | Amazon Web Services (AWS) | USA

Cloud computing revealed its tangible positive impact on health outcomes during one of the worst global health crises. But we're still only scratching the surface of what's possible.

Key Points

- By eliminating data silos and enabling providers to view complete medical histories, interoperability stands to provide a better patient experience and empower individuals to take greater control over their health care.
- The power of the cloud is democratising access to data, artificial intelligence (AI), and machine learning (ML) to bring about the next generation of healthcare solutions for use at the point of care.
- As healthcare organisations unlock the power of their data, they will be able to address pressing needs in diagnostics, preventive and predictive care, and access from anywhere.

The healthcare industry has worked to adapt and find new ways to get accurate information to patients and direct them to resources and care at scale. And much of this—from chatbots and remote patient monitoring to telehealth to electronic health record (EHR) systems—has relied on technology and the cloud. However, more can be done to enable transformative change for patients, caregivers, and providers.

To better support patients, the healthcare industry needs to look at how to securely access the right patient data, paired with advanced analytics, AI, and ML, to help enhance insights tied to outcomes in an accurate, scalable, secure, and timely manner. Additionally, the industry needs to come together to ensure that data connectivity, security, and privacy aren't barriers to achieving the promise of digital transformation.

Creating a Clearer View of Patients Through Healthcare Interoperability

With advances such as remote monitoring, EHRs, and wearable devices, significantly more health data is being captured today than ever before. However, that data is only useful if it is available, indexed, and structured in a way that allows clinicians to see and analyse it at the point of care.

With the current state of fragmented patient data, an estimated 80% of which is stored in unstructured medical formats (Kong 2019), important information might be overlooked or misinterpreted. Extracting information from patient data has traditionally been a labour-intensive and error-prone process, but now cloud tools such as Amazon HealthLake are designed to take on the monumental task of normalising, indexing, structuring, and analysing data to make it useful for providers in understanding patients' entire medical histories.

EHR systems do not follow patients on their care journey beyond the hospital or clinic walls, but cloud technology is also being used in remarkable ways to facilitate interoperability and address this. Change Healthcare, for example, launched a service that allows for the free exchange of medical records between facilities. With access to prior lab results and previously siloed patient-history data, physicians can avoid costly duplicate testing, diagnose patients more easily, and initiate treatment faster. Change Healthcare's clinical data interoperability services also give patients improved access to their medical records by aiding in document retrieval, identity management, and record location.

Progress has been made in developing open standards

like the Fast Healthcare Interoperability Resources (FHIR) from Health Level Seven (HL7) and application programming interfaces (APIs) that facilitate data sharing across systems—although adoption and scaling has been slow. When a health system uses interfaces that are proprietary or conform to earlier standards, they can fail to support true interoperability. Open source software toolkits such as FHIR Works on AWS enable customers to build interoperability into their platforms, as Black Pear Software has done for the National Health Service (NHS). And Amazon API Gateway, a service designed to allow developers to create, publish, monitor, and secure APIs easily at any scale, enables the building of innovative solutions that help healthcare organisations share data.

Interoperability stands to provide a better patient experience anywhere, and cloud-based services are making a clearer, more comprehensive view of patients possible while empowering individuals to take greater control over their healthcare journeys.

Better Insights and Outcomes with Cloud-Enabled Technologies

With ongoing emphasis on value-based care, interoperability paired with AI and ML models are helping healthcare organisations optimise use of their data, increasing diagnostic accuracy and efficiency, making preventive and predictive care a reality, and improving patient access and experience.

AI and computer vision can aid with diagnosis across radiology, oncology, ophthalmology, and dermatology, as well as in the prediction of disease and health events. With this, unnecessary imaging examinations and clinical procedures are reduced, errors that contribute to poor outcomes are minimised, and costs decrease.

To predict the prognosis of hospitalised COVID-19 patients, the Centro Diagnostico Italiano, Bracco Imaging, and a group of Italian institutes and hospitals created an AI model to forecast the trajectory of disease using chest x-rays and medical records as training input. This non-profit project, called *AIforCOVID*, was funded through the AWS Diagnostic Development Initiative, and it helps doctors identify those likely to experience a serious form of disease and intervene faster with an appropriate level of care.

These technologies also put more power in the hands of patients. Netherlands-based SkinVision developed a solution for early detection of skin cancers using images. The algorithm trained on hundreds of thousands of images to detect melanoma and other types of skin cancer. To use SkinVision, a patient uploads a picture of their skin spots into the app. The patient can also indicate symptoms such as itching and bleeding. Within 30 seconds, the images are analysed and tagged as low or high risk. Low risk advises to set a reminder to recheck, and high risk advises the patient to see a doctor. With SkinVision, instead of mole checks happening every two or three years, patients can check themselves more regularly. The sensitivity of the algorithm now means that 95% of skin cancers will be detected if they appear in the image.

Advanced computing power and improved database capabilities also enable population health analytics and preventative care. In 2021, Omada Health unveiled the Omada Insights Lab, a data analysis engine that uses over 1 billion proprietary data points from over half a million members' real-world interactions with Omada Health programmes, to yield recommendations for optimising and personalising care. Data continuously ingested from glucose monitors used by prediabetic and diabetic programme members is then securely analysed with ML models. Ninety-six data points per day per patient are produced, yielding deep insights and metrics-based alerts for clinicians that can improve care and health outcomes on both individual and population levels.

Interoperability paired with AI and ML models are helping healthcare organisations optimise use of their data, increasing diagnostic accuracy and efficiency

Telehealth and remote monitoring have also found their place in routine clinical practice like never before. With an urgent need to monitor and identify trends in vulnerable cohorts remotely during the pandemic, London-founded Huma established a solution so clinicians can track vital signs using biomarkers collected by portable, wearable, and implantable digital devices. Clinicians can view these metrics from a single dashboard, allowing them to care for 50% more patients at a time, and patients have the confidence of knowing their healthcare professionals are monitoring their vital signs.

Cloud-enabled technologies also provide better patient experiences and help connect in-need populations with resources. Early in the pandemic, the NHS worked with AWS and technology consultancy Slalom to set up an automated service that aimed to reach 1.5 million of the UK's most vulnerable people to help

them register to receive social and medical care and essential supplies. The service, which was set up in 48 hours using the flexibility of cloud tools and technology, enabled the NHS to act quickly to reach vulnerable groups as the country prepared to enter lockdown. Another example that demonstrates the benefit of being able to scale with cloud is Nye Health in the UK. Nye Health built a scalable, NHS-compliant platform that allows all NHS staff to offer consultations from any device, anywhere. In 2020, the platform covered more than 10 million patients, was growing by as much as 150% weekly, and was servicing thousands of patient consultations each week.

Virtual care tools like automatic speech recognition and natural language understanding applications also allow providers to offer patients highly engaging, lifelike conversational interactions that recognise the intent of voice and text transactions. Additionally, translation services convert text from one language to another so providers can support patients in multiple languages.

Addressing Security, Privacy, and Compliance

With purpose-built cloud solutions, healthcare organisations can improve their ability to meet core security and compliance requirements. Based on AWS's Shared Responsibility Model, customers evaluate their compliance requirements, and we continually monitor the evolving privacy, regulatory, and legislative landscape to identify changes and determine what tools our customers might need to meet them. Additionally, AWS customers control their data by using powerful services and tools to determine where it is stored, how it is secured, and who has access to it. These solutions help ensure that IT infrastructure is compliant with changing policies and regulations, allowing in-house IT teams to focus on projects centred on patients and providers.

AWS regularly achieves third-party validation for thousands of global requirements, like Europe's General Data Protection Regulation (GDPR), as well as country-level regulation like Digital Health Applications Ordinance (DiGAV) in Germany and Hébergeurs de Données de Santé (HDS) certifications in France, as well as non-government programmes like Health Information Trust Alliance (HITRUST).

Delivering on the Promise of Digital Transformation in Healthcare

More and more healthcare organisations are recognising the benefits of cloud-based solutions and will rely on cloud to scale data storage, analytics, and ML looking ahead. It has been estimated that the global healthcare cloud computing market will grow at a CAGR of 18.74% between 2021 and 2028 (Vantage 2021). With this growing adoption by healthcare organisations, interoperability and wider use of open standards will help extract more meaningful insights from patient data.

Increased use of cloud can also result in reduced computing costs, enabling providers to reinvest savings. In fact, a new Amazon Web Services analysis (2022) identified 14.4 billion euros in potential IT savings across the European Union and UK healthcare sectors over the next five years—the equivalent of 5,665 euros per hospital bed—through migration of IT systems to the cloud.

Working together, healthcare and technology organisations have the opportunity to support a future that delivers more effective, efficient healthcare centred around patients' individual needs. As organisations move to the cloud, they can move from a system-centric view to a patient-centric view and, as a result, move more toward predictive and preventive care. This fundamental shift is what will ultimately deliver meaningful improvement in care decisions and overall patient outcomes. ■

REFERENCES

Alldredge BK et al. (2001) A comparison of lorazepam, diazepam, and placebo for the treatment of out-of-hospital status epilepticus. N Eng J Med. 345(9):631-7.

Silbergleit R et al. (2011) RAMPART (Rapid Anticonvulsant Medication Prior to Arrival Trial): a double-blind, randomized clinical trial of the efficacy of intramuscular midazolam versus intravenous lorazepam in the prehospital treatment of status epilepticus by paramedics. Epilepsia. 52(Suppl 8):45-7.

Strein M, Holton-Burke JP, Smith LR, Brophy G (2019) Prevention, Treatment, and Monitoring of Seizures in the Intensive Care Unit. J Clin Med. 8(8): 1177.

Sutter R (2016) Are We Prepared to Detect Subtle and Nonconvulsive Status Epilepticus in Critically Ill Patients? J Clin Neurophysiol. 33(1):25-31.

Vespa P et al. (2020) Evaluating the Clinical Impact of Rapid Response Electroencephalography: The DECIDE Multicenter Prospective Observational Clinical Study. Crit Care Med. 48(9):1249-1257.

Internet of Medical Things: Threats and Recommendations

Alexios Antoniou | Cybersecurity Consultant | KPMG | Cyprus

Internet of Medical Things (IoMT) aims to deliver game-changing benefits to healthcare institutions, patients and society. It supports more accurate diagnoses, improved treatments, and better availability of care. IoMT systems face challenges, such as the security of all the interconnected components. This article aims to present a few vulnerable components and point out recommendations for better security.

Key Points

- Internet of Things (IoT) denotes all electronic devices (apart from traditional computers) that are connected to the internet.
- In 2018, the IoMT market value was $44,5 million and is expected to reach $254.2 million by 2026.
- As with any device connected in the cyber realm, IoMTs are also exposed to threats and cyber-attacks.
- Since some security challenges for IoMT are new and different, an adapted application of measures is necessary.

Internet of Things (IoT) denotes all electronic devices (apart from traditional computers) that are connected to the internet, and their aim is to collect, analyse, and transmit information or respond to remote commands. IoT has been an enabler for many different sectors, such as manufacturing, transportation, utility organisations and healthcare institutions. Internet of Medical Things (IoMT) refers to the ecosystem of advanced digital devices and systems which can collect, transfer and analyse data regarding someone's health condition. IoMT enables the transfer and processing of medical information through a network without human interaction and allows for remote, automated, 24hr healthcare services.

There are different IoMT device categories according to their purpose and their use. In total, there are the following five categories.

1. Fitness Tracking Devices: Used to monitor someone's physical activity. These devices can be wristbands or smartwatches.
2. Clinical Grade Wearable Devices: Used to improve a user's chronic health conditions. These devices can be smart belts that are capable of detecting falls and informing a carer.
3. Monitoring Devices: Used to keep a patient under constant monitoring. It can be a blood glucose monitor.
4. Smart Pills: Used in medication administration compliance. Smart pills are similar to traditional pills, with the only addition being that they have ingestible sensors.
5. Hospital Devices: Used to monitor hospitalised patients. These devices refer to infusion pumps, MRIs, CT scanners and Ultrasound Scanners.

In 2018, the IoMT market value was $44,5 million and is expected to reach $254.2 million by 2026. The four main pillars that contribute to the raised market value are medical devices (32.91%), system and software (31.01%), technology (17.72%) and services (18.36%).

The workflow in the IoMT ecosystem starts with the IoMT devices. These devices, which are equipped with sensors, collect users'/patients' medical data and forward it to cloud services through gateways such as smartphones over wired or wireless network technologies (i.e. Infrared, Bluetooth, Zigbee, Wan etc.). Depending on the underlying communication protocols,

encryption methods are used to secure device communication. Upon receiving information, the gateway then needs to transfer it directly to the cloud or to a fog server. A fog server collects data generated by IoMT devices processes, analyses and summarises it before forwarding it to the cloud services. The purpose is to reduce the bulk of information transmitted to the cloud services reducing the communication bandwidth as well as the required cloud storage capacity. When the information arrives at the cloud services, data aggregation, processing, visualisation and knowledge distribution to healthcare professionals take place. In some cases, the cloud services are connected to external applications such as Clinical Decision Support Systems (DSS), which aid clinicians when they have to make complex and tough decisions regarding a patient's medication/therapy.

Secure IoMT device authentication and communication is implemented through enterprise-wide cryptography policies. The number of IoMT devices in a healthcare ecosystem is vast, and manual management of digital identities is impractical. IoMT devices' performance and scalability are essential. The use of an automated machine identity management system will increase efficiency and effectiveness. Such systems offer automatic device registration and de-registration, automatically update device identities and credentials, and support standard-based authorisation. They also reduce the window of exposure when facing a cyber-attack or when responding to a newly announced vulnerability.

The amount of information generated in the IoMT realm is enormous. The application of edge computing technologies has been proposed to address capacity and node communication bandwidth challenges. According to edge computing, nodes with processing capability are installed at the edge of the network, near the physical location of IoMT devices. These edge nodes process the generated data, and only aggregated data sets are forwarded to the cloud. According to Dilibal (2020), edge computing in healthcare could minimise communication latency and data streaming, reduce alarm notification and response delays, and decrease the cost of healthcare monitoring platforms.

IoMT-based solutions have also been proposed to remotely run medical examination tests which are otherwise expensive to carry out. Detection of sleep apnoea is such an example. Sleep apnoea is a potentially serious sleep disorder where breathing stops and starts periodically many times during a night's sleep, affecting the sleep quality and, as a result, the mental, physical and emotional functioning of the patient. Haoyu et al. (2019) proposed a scheme that uses IoMT to detect sleep apnoea incidents in real-time and promptly inform patients and doctors. The system utilises a SpO_2 sensor to monitor blood oxygen levels and heart rate. Data is transferred through a gateway to the cloud for diagnosis and further processing. Tests have proven the proposed scheme to produce at least 97% accurate diagnoses.

As with any device connected in the cyber realm, IoMTs are also exposed to threats and cyber-attacks. Numerous vulnerabilities have been identified and reported for a significant number of devices. Organisations like NIST (National Institute of Standards and Technology) and CISA (Cybersecurity and Infrastructure Security Agency) maintain records on known vulnerabilities, including a detailed description of the problem, threat scoring, affected units, and recommended mitigation actions. This section presents four such cases and critically examines the probable impact on a healthcare institution due to successful exploitation. Vulnerability severities have been assigned by NIST using the Common Vulnerability Scoring System (CVSS) version 3. CVSS's base score takes into account five exploitability metrics (Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR), User Interaction (UI), and Scope (S)), capturing how complicated exploitation is. Three additional metrics capture the impact on Confidentiality (C), Integrity (I) and Availability (A). Classification is expressed as a vector of attributes for the eight parameters and a numeric score from 0 to 10. A score of 9.0-10.0 is classified as Critical, 7.0-8.9 as High, 4.0-6.9 as Medium and 0.1-3.9 as Low. A high classification denotes higher risk for which mitigation actions should be prioritised.

A threat actor with access to a vulnerable IoMT device could potentially escalate privileges to admin, modify operating parameters, implement denial of service or gain access to sensitive information

The first vulnerable component is named ExactaMix1200, developed by Baxter, and the affected-vulnerable versions are from 1.1 to 1.5. Compounding, with regards to medical sciences, is the preparation of a custom combination of medication to be administered to a specific patient suffering from a condition that cannot be dealt with commercially available medicines.

ExactaMix1200 is an automated compounding system manufactured by Baxter that aims to increase efficiency, accuracy, production levels, and compounding effectiveness. Its primary function is to compound sterile ingredients into a finished product in a single bag. It integrates seamlessly with order entry calculation software as well as pharmacy workflow management software.

According to CISA, ICS Medical Advisory ICSMA-20-170-01 Etxacta Mix 1200 units, versions 1.1, 1.2, 1.3, 1.4 and 1.5 suffer from CVE (Common Vulnerabilities and Exposures) CVE-2020-12016. This CVE has a CVSSv3.0 score of 8.1 (High). The device uses a hard-coded password set by the manufacturer, transmits sensitive data in clear unencoded form, stores data in clear form, allows booting from a live USB, does not restrict non-administrators from changing the start-up script and does not validate input via a port (SMBv1) which can affect control flow of the system.

A Threat Actor (TA) with access to such a device could achieve administrator's privileges, modify operating parameters, implement denial of service and gain access to sensitive information, including Patient Health Information (PHI). This could have a major impact on operations, endanger patients' lives and cause significant financial losses if ransom payment is required. Moreover, an event of such a scale could severely impact patients' confidence in the services provided by the institution.

The second vulnerable component is named Outlook400ES, developed by B.Braun Medical Inc. Outlook400ES is a medical infusion pump that is used to deliver fluids into a patient's body in a controlled manner. The Outlook 400ES system was designed to provide reliable intravenous medication administration and has wireless drug library capabilities to simplify medication composition and control. It supports an open design that enables interconnection with a large number of external vendor applications. According to a security announcement by B. Braun, Outlook 400ES is affected by the following vulnerabilities: CVE-2020-11906 with a score of 5.3 (Medium), and CVE-2020-11903 with a score of 5.0 (Medium).

The combination of the above vulnerabilities may allow a TA to read sensitive information from other memory locations or cause a crash exposing the healthcare facility to disruption of operations, leakage of sensitive patient data and finally to ransomware demands. Such an event could carry a significant impact both on the profits of the institution as well as on customer confidence.

The third vulnerable component is named Volution730, developed by General Electric, and the affected versions are the BT05 and BT08. Volution 730 is an ultrasound station which uses high-frequency sounds to produce an image of a woman's bladder, fallopian tubes, ovaries, uterus and cervix. It is used to monitor pregnancy and to evaluate medical conditions regarding the aforesaid female body organs. According to CISA, this device is affected by vulnerability CVE-2020-25179 with a score of 9.8 (Critical) because it employs unprotected transport of credentials and exposes sensitive system information.

A TA with access to the network to which such a device is connected can log in to the system with privileges comparable to a GE service user account. Sensitive PHI is exposed, arbitrary code can be run on the machine, and PHI can be modified. The TA can use these as leverage towards the healthcare institution imposing their demands for payment to release control of the systems and avoid releasing PHI to the public domain.

The final vulnerable component is named RapidPoint500 and was developed by Siemens. RAPIDPoint 500 is an automated blood analyser. It can test blood gas, electrolytes, glucose, lactate and full CO-oximetry. It supports multiple sample types and can perform hands-free automated sampling to reduce biohazards.

According to an announcement by Siemens, the device is affected by CVE-2018-4845 with a score of 8.8 (High) and CVE-2018-4846 with a score of 7.3 (High). The first CVE allows a remote attacker with credentials to the "Remote View" feature to achieve elevation of privileges, compromising confidentiality, integrity and availability of the system. Exploitation metrics are assigned high values indicating that special skills or user interaction are not required for a successful exploit. The second CVE refers to a factory set account with a hardcoded password, allowing remote control over TCP port 5900. Once again, no special skills or user interaction is required, and device confidentiality, integrity, and availability are compromised.

A TA could effectively control the device, make it inoperable and demand a ransom before releasing it. The impact of an institution relying on such devices to deliver accurate and quick blood analysis results could be critical, as operations may be put on hold until the situation is resolved. Patients may turn to other facilities for their tests, and the institution's brand might be damaged irredeemably.

As has been mentioned, the IoMT components are vulnerable to cyber threats. The whole ecosystem must perform in a safe and secure environment. Security principles that have been studied for many years still apply; however, since some security challenges for IoMT are new and different, an adapted application of measures is necessary.

This article concludes with recommendations to be implemented at procurement, deployment, and management, significantly reducing the attack surface and minimising exposure to cyber-attack threats. During the procurement stage, all devices that run outdated operating systems should be avoided as these devices are no longer supported, and no security updates will be released. Healthcare institutions should opt for manufacturers who apply the 'secure by design' principle,

where security is considered and implemented into a product at every development stage. Such devices implement exploitation mitigation techniques like software verification at boot and encryption of data stored or transmitted and will be much more difficult for TAs to exploit. They should also opt for devices supporting control by an automated identity management system and for providers who apply a policy to disclose regularly and promptly any vulnerabilities identified for their devices. Moreover, healthcare institutions should make sure that the devices' vendors will be delivering device security updates at regular intervals covering the whole lifecycle of the product. Finally, it is not recommended to use any devices that are factory programmed with hardcoded, non-unique credentials, as these may be easily exploited by TAs.

During the deployment stage, healthcare institutions should apply the defence in depth principle by using a series of layered security controls so that in case of an attack, the multiple security layers will make accessing sensitive devices or PHI data more difficult. They should also implement security zoning by isolating computer networks that serve different functions so that a TA who gains access to a network can be contained and apply the principle of least privilege, which means that the devices will have access only to data and functions that are needed to complete a required task. Finally, healthcare institutions should make sure that the data storage processes align with regulations, legislations and codes of practice such as the General Data Protection Regulation (GDPR).

When managing the IoMT devices, once again, healthcare institutions should apply the principle of least privilege to operators so that each person will have the minimum privileges required to perform his/her daily tasks. This way, in case of leakage of credentials, the attack surface is much more limited. Further, it is recommended to install an automated identity management system. These systems enforce higher device security, reduce maintenance costs through automated identity management, ensure compliance with security standards and manage secure firmware updates. They also allow for a much quicker response if multiple identities need to be revoked or reworked because of a security incident. Lastly, it is also recommended that healthcare institutions run system security evaluations periodically by utilising the services of companies specialised in the IoMT domain.

Conflict of Interest

None. ■

REFERENCES

All the Research (2020) Global Internet of Medical Things (IoMT) Market – Segment Analysis, Opportunity, Competitive Intelligence, Industry Outlook 2016-2020. Available at https://www.alltheresearch.com/report/166/internet-of-medical-things-market

Alqahtani B, AlNajrani B (2020) A Study of Internet of Things Protocols and Communications. 2nd International Conference on Computer and Information Sciences (ICCIS), 13-15 October. IEEE.

BBraun (2020) B. Braun Statement on Cybersecurity Vulnerability with Ripple20 Communications Software. Available at https://www.bbraunusa.com/content/dam/b-braun/Ripple20

CISA (2020) Baxter ExactaMix (Update A). Available at https://us-cert.cisa.gov/ics/advisories/icsma-20-170-01

CISA (2020) GE Healthcare Imaging and Ultrasound Products. Available at https://us-cert.cisa.gov/ics/advisories/icsma-20-343-01

Dilibal Ç (2020) Development of Edge-IoMT Computing Architecture for Smart Healthcare Monitoring Platform. 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (SMSIT).

First.org (2021) Common Vulnerability Scoring System version 3.1: Specification Document. Available at https://www.first.org/cvss/specification-document

Haoyu L, Jianxing L, Arunkumar N et al. (2019) An IoMT cloud-based real time sleep apnea detection scheme by using the SpO2 estimation supported by heart rate variability. Future Generation Computer Systems, 98 pp.69-77.

Jaidka H, Sharma N, Singh R (2020) Evolution of IoT to IIoT: Applications and Challenges. International Conference on Innovating Computing & Communications (ICICC) University of Delhi, 21-23 February Springer. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3603739

Kamani V (2020) A Detailed Guide to IoMT Implementation in 2020. Available at https://arkenea.com/blog/iomt/

Key factor (2021) State of Machine Identity Management Report 2021. Available at https://www.keyfactor.com/state-of-machine-identity-management-2021/

For full references, please email edito@healthmanagement.org or visit https://iii.hm/1isd

Syncope Diagnosis, Treatment and Management

James Frith | Clinical Senior Lecturer | Consultant Physician | Faculty of Medical Sciences| Newcastle University | UK

James Frith is a consultant physician and geriatrician in Newcastle, England. He is also a researcher at the Newcastle University. His academic interests focus on orthostatic hypotension, in particular, the non-drug treatments of orthostatic hypotension that significantly overlap with falls and syncope. HealthManagement.org spoke to Dr Frith on the importance of accurate syncope diagnosis and effective treatment and management strategies for this condition.

Key Points

- Syncope is a transient loss of consciousness caused by a reduction in blood flow to the brain.
- Anybody could be affected by syncope - roughly 40% of the population will have syncope at some point in their life.
- Finding the cause of syncope can be quite challenging as an attack of syncope could be a year between events.
- The European Society of Cardiology Guidelines for the diagnosis and management of syncope is very comprehensive and useful for clinicians.
- Simple treatments are the best. However, if simple things don't work, it is time to refer to a specialist; ideally, a syncope unit, where the guidelines can be followed, and the diagnosis is reached much more quickly.

Why is syncope an important topic? How has awareness of syncope changed over the past ten years?
Syncope is a transient loss of consciousness, and the word transient is important here. The loss of consciousness always recovers spontaneously. It's caused by a reduction in blood flow to the brain, and that can either be caused by a problem with the blood leaving the heart or a problem with the blood pressure. Typically, there is a sudden profound drop in blood pressure. That means not enough blood gets to the brain, and there's a loss of consciousness.

There are lots of different reasons why syncope is important. It's important to the individual who experiences syncope. They have a reduced quality of life – the quality of life of people with syncope is comparable to those with rheumatoid arthritis or moderate depression. Syncope can also result in serious injuries. A large proportion of people will have a road traffic accident if they have syncope at the wheel. They can also break bones when they lose consciousness and collapse to the ground.

There are more wide-reaching reasons why syncope is important. It's so common that significant resources are needed within healthcare systems to investigate and treat syncope. Hence, it is a costly condition for healthcare systems. But the other wider implication is that it affects people's ability to drive and sometimes their ability to work. That's important for wider societal reasons.

From my point of view, the biggest change we've seen in the last 10 to 20 years has been the use of cardiac monitoring, specifically in the area of falls. Older people present to the hospital or primary care as having a fall when in fact, they've had syncope. In the last 10 to 20 years, there's been increasing amounts of research showing that problems with the heart or heart rhythm

i.e., arrhythmias contribute to a large number of unexplained falls, particularly in older people who're experiencing syncope.

What does a typical syncope patient look like?

Syncope is so common that anybody could be affected by it. Roughly 40% of the population will have syncope at some point in their life. There is no one typical syncope patient. However, there are two main groups. The first group is the young adult, roughly from the age of around 18 to 23. Young people have very elastic blood vessels, so their blood pressure can drop very low. As a result, they are more prone to fainting episodes, which is extremely common in this age group. Over time, as we age, the incidence of syncope decreases, but above the age of 60, the incidence of syncope rapidly increases again. It is much more common in the older generation when it is more complicated because they are already on several medicines and suffer from other conditions. Therefore, the older generation tends to have more worrying causes of syncope.

What challenges does syncope present for healthcare systems?

One of the biggest challenges is that syncope can present in different areas in the hospital or primary care. Someone who needs to see a specialist with syncope may be referred to neurology, cardiology, or geriatric medicine. Sometimes they might be referred to ENT for dizziness that isn't syncope. Hence, patients can end up seeing multiple specialists. Hospitals need to have a syncope unit with people specialising in syncope. That's one of the challenges for healthcare systems.

What are the challenges in diagnosing syncope? What issues face syncope patients getting diagnosed? What are the issues facing syncope patients after the diagnosis?

The challenge for the specialists trying to find the cause of syncope is that typically people will have normal physiology between their attacks of syncope. Finding the cause can be quite challenging because, in an ideal world, it would be useful to know the blood pressure and the heart rate during an attack of syncope. But an attack of syncope could be a year between events, and that's the challenge for clinicians.

In young people, the symptoms tend to be lightheadedness, dizziness, nausea and weakness. People might notice that they look very pale and sweaty before collapsing to the ground and losing consciousness. That would be in a typical episode of syncope related to the commonest cause, vasovagal syncope, which is syncope or fainting from low blood pressure. Sometimes people don't get any warning before they lose consciousness, which might make us think there's something cardiac behind the syncope. Also, older people are much more likely to forget any symptoms before they collapse and lose consciousness. That is why older people sometimes present with falls rather than syncope. There are also differences in the recovery period. Younger people recover much more rapidly, whereas older people might feel washed out and tired for longer periods afterwards. Older people are more likely to experience incontinence if they have a syncope attack.

It is important to identify the cause of syncope. When someone presents to a clinician with syncope, they undergo several tests unless the cause is apparent initially. The clinician will take a thorough history from the patient to try and determine what happened. In most cases, history will give us the answer. If the answer isn't clear, there will be a need to do cardiac and blood pressure tests. If the answer still isn't clear, it can be a very lengthy process. For example, one of the tests that might be used in syncope is a device that sits under the skin and monitors the heart's rhythm. If people have one of those devices, the average length of time to reach a diagnosis is almost two years. Hence, it is a lengthy process to reach a diagnosis.

One of the other difficulties people face is driving restrictions with syncope (different in different countries). In the U.K., for example, some people might have to stop driving for a year. People may face occupational issues and childcare issues; some may develop a fear of having syncope, particularly if it's unpredictable, and that can affect their quality of life and confidence to leave the house.

What diagnostic tools are required or do you consider important for diagnosis?

The single most important thing for the diagnosis is the history or the story of the event. That usually gives us the most clues. Also, it's useful to have a witness to describe the patient's appearance, as that can give us clues. It's useful to have that information as close to the event as possible so people can recall what happened. After that, a 12 lead ECG is useful because it helps us understand what risk the patient might be of having a serious cause of syncope or a less worrying cause of syncope. Alongside an ECG, there is a lying blood pressure and standing blood pressure to see if there are any problems with blood pressure control. There are more specialised tests, such as the tilt test, where we try to make people faint or force them to have a syncope episode and specialised cardiac tests where we monitor the heart for longer periods to catch an episode of syncope.

Are there international standards for assessing syncope? Could you specify the Newcastle protocol for syncope assessment? What is the difference compared to other protocols?

The international standards that we use in Newcastle are the European Society of Cardiology Guidelines for the diagnosis and management of syncope. These are very comprehensive guidelines that are useful for different clinicians, which range from the start of the patient journey in the acute situation in A&E and the emergency room through to the people who are working in syncope units to advise on which tests should be used and not used and the treatment guidelines.

There are very few differences between the Newcastle Protocol and the European Society of Cardiology guidelines. The main difference is that the Newcastle Protocol is more pragmatic and tries to give useful advice to clinicians on what they can do and use in their clinic.

Where can a patient turn to or go when he has the problem of fainting?

The most important thing is to be safe. Patients who feel they're about to faint or lose consciousness need to move somewhere safe. Most people will move to a seated position, ideally with the head between the knees, or lie on the floor if it's safe. They need to pull over and stop if they're in a car. If they are near water or any other dangerous environment, they should try and move away and lie down. It's not always easy to lie down where a patient is. In such circumstances, there are simple measures which might buy a bit of extra time to move away somewhere safe. This includes squeezing muscles in the body to temporarily increase the blood pressure or pulling the hands apart which will temporarily increase the blood pressure so that someone can move somewhere safe to lie down.

What are the treatment options when syncope is diagnosed?

The commonest cause of syncope is fainting from low blood pressure. Simple treatments are the best. The first thing is to avoid triggers. Heat is a very important trigger for causing low blood pressure and syncope. People should be advised to avoid prolonged standing in the heat or unwrap and remove heavy layers of clothing. Other triggers might be alcohol, which can lower blood pressure; drugs such as cannabis and large meals can also trigger fainting. Some people may have specific triggers, such as the sight of blood. Then there are some very specific triggers which we call situational syncope. People should try and avoid these where they can. Another simple advice is to avoid dehydration. Water is very important in the management of syncope. Young people might consider increasing their salt intake to help increase blood pressure. An important study published in the last few years was about the manoeuvre of using the muscles in our body to temporarily increase blood pressure (van Dijk et al. 2006). It is an effective and proven treatment to abort an attack of syncope or fainting.

What message would you pass on to syncope patients?

Simple things work. Unfortunately, simple things are not always easy to stick to. For example, we need to avoid dehydration but drinking lots of water can be difficult, especially for busy people. Some people will find it embarrassing to lie down somewhere to avoid syncope and might not do that. In the older age group, people might not remember to do the simple measures, but they are the most important, and they work. There are important messages for clinicians as well. In recent years, a VD stop study (Solari et al. 2017) showed that reducing medications lowered blood pressure. If we reduce them, we can reduce the number of syncope events people have without increasing the risk of cardiac or cerebrovascular events. Some other studies have also been published in the last few years evaluating drugs to prevent syncope. One was fludrocortisone and another was midodrine (Sheldon et al. 2016; Sheldon et al. 2021). In very select patient groups, these drugs can be useful. My message to patients and clinicians is that simple lifestyle measures are the most important.

If you were a syncope patient, what would you want to tell other patients suffering from fainting?

I would tell them to drink plenty of water. If they are young, I would tell them to eat more salt. I would also have a very positive outlook for young people because as they get older, their syncope should start to reduce naturally. For the older generation, I would start to look at other things, such as protecting their bones. I would tell them to have a diet and a lifestyle that would be healthy for the bones to help reduce any fractures. I would also stress the importance of exercise, which is good for blood pressure control and bones.

What would you like to tell your colleagues in other departments who might be confronted with fainting patients?

Syncope is so common that just about every clinician will come across it at some point. The important message for people who see the acute side of syncope, usually in the emergency room or primary care, is that when they see the patient, they should do a risk assessment to determine whether the cause of syncope is high-risk. Could it be cardiac syncope? Could there be something wrong with the heart that needs treatment urgently? On the other end of the spectrum, the patient can be reassured and given simple advice if it's low-risk syncope. For other clinicians who might be seeing syncope, I would say if simple things don't work, it is time to refer to a specialist; ideally a syncope unit, where the guidelines can be followed, and the diagnosis is reached much more quickly.

What have been essential achievements in syncope assessment over the past 10-20 years?

The link between falls and syncope is incredibly important, and much work has been done on that in the last 20 years. The management of people who present with falls has changed due to this, and guidelines now very strongly recommend that when people present with a fall, they must be assessed for cardiovascular reasons for why they're falling, which is syncope.

What new innovations do you expect for syncope assessment and management in the next five years?

One of the problems is that people have normal

physiology between the attacks of syncope. We need more non-invasive ways of monitoring blood pressure and heart rhythms remotely so people can be monitored at home. There has been progress in recent years. As I mentioned earlier, there is a device that is implanted underneath the skin which can monitor the heart rhythm. There are now devices available in the form of stickers which sit on the skin and monitor the heart for prolonged periods. I expect to see more development of those kinds of devices. One of the things we've never had is prolonged blood pressure monitoring. Blood pressure is quite difficult to monitor, especially remotely. The equipment used is quite bulky, but recent advances have seen devices that can be stuck onto the skin to monitor blood pressure. Those offer real potential in the future.

With recent advances in TeleHealth and IoT, what role do you see for home care and remote monitoring for syncope management?

Telecare has been around for a while but isn't used very often. I don't know if that's because it's expensive. I'm also not sure whether it's because the biggest healthcare users in Western countries are older people, but remote monitoring and telehealth trends are all technology, and technology isn't always designed to work with older people. Moving forward, we must ensure that such technology is easy to use, acceptable, cheap and accessible for older people. From a clinician's point of view, we need to ensure that telemonitoring transmits important results without many erroneous results. Otherwise, there simply isn't enough time to look at all the information that can come from telemonitoring. We need to make it more pragmatic and user-friendly.

One of the best examples I've seen of telecare, more in the field of falls and syncope, is a simple device that is plugged into a socket, and then a device such as a kettle is plugged into that device so that when someone uses the kettle, a text message is sent to someone else, for example, a family member. Hence, they would know that their parent or grandparent is up and making a cup of tea. If they don't get a text message by e.g. 10:00 in the morning, they know something is wrong. That's one of the best devices that I've come across.

What are your desires for the future regarding syncope assessment?

I would love some sort of continuous blood pressure monitor that people could wear during their daily lives and that could measure blood pressure during a syncope attack. Such a device could help reduce the number of unexplained syncope episodes we see. ■

REFERENCES

Sheldon R, Faris P, Tang A et al. (2021) Midodrine for the Prevention of Vasovagal Syncope: A Randomized Clinical Trial. Ann Intern Med. 174(10):1349-1356.

Sheldon R, Raj SR, Rose MS et al. (2016) Fludrocortisone for the Prevention of Vasovagal Syncope: A Randomized, Placebo-Controlled Trial. J Am Coll Cardiol. 68(1):1-9.

Solari D, Tesi F, Unterhuber M et al. (2017) Stop vasodepressor drugs in reflex syncope: a randomised controlled trial. Heart. 103(6):449-455.

van Dijk N, Quartieri F, Blanc JJ et al. (2006) Effectiveness of physical counterpressure maneuvers in preventing vasovagal syncope: the Physical Counterpressure Manoeuvres Trial (PC-Trial). J Am Coll Cardiol. 48(8):1652-7.

Clinical Care Management

How to Create a Migraine-Friendly Workplace

Elisabetta Schiavone | Architect | Technical Director Soluzioni Emergenti | Italy
Alessandra Sorrentino | Representative of the Alleanza Cefalalgici (Al.Ce.) at European Migraine and Headache Alliance | Blogger, "Le parole dell'emicrania"| Italy
Lara Merighi | National Coordinator of Al.Ce | Italy
Elena Ruiz de la Torre | Patient Advocate and Executive Director of European Migraine and Headache Alliance | Spain
Giorgio Sandrini | President of CIRNA Onlus Foundation | Italy

Is it possible to create a safe and inclusive workplace for people with migraine? Yes, it is. Companies need to be aware that an environment that meets the specific needs of those suffering from invisible diseases can become a facilitator and that it is necessary to apply design criteria that reduce the presence of triggers.

Key Points

- Work is where the majority of people of working age spend most of their day.
- The impact of the work environment and of workplace relationships on the individual's psycho-physical well-being has a significant and decisive influence on various aspects of their lives: their quality of life, their decision to enter (and subsequently to remain in) the working world, and the company they choose to work for.
- From the workplace to the work environment: a change in perspective is needed in order to identify what and how many factors affect the workplace well-being of people with migraine. These include the physical and social environment, collectively known as environmental factors, that, for the individual, can act as barriers or facilitators (ICF, WHO 2001).
- Inclusive safety is a passe-partout to achieve a multidisciplinary and multidimensional approach to the concept of accessibility in emergency prevention and emergency planning, an approach that considers the autonomy of every individual according to their specific needs.

Introduction

Migraine is a very complex disabling neurological disease, and currently, a large proportion of patients are only partial responders or non-responders to the available treatments. According to the WHO, migraine is the leading cause of disability in the under 50s and the second cause of years lived with disability worldwide. A recent study, in agreement with other previous studies, "revealed a high prevalence and disease burden among employees with migraine that is associated with substantial losses in productivity and employer cost" (Shimizu et al. 2021) and suggested that the development and implementation of programmes to improve migraine management in the workplace could reduce the burden and costs associated with lost workplace

productivity.

The considerable social, familial, and economic impact of migraine is confirmed by epidemiological data showing that the condition occurs in 1 out of 5 women; 1 out of 16 men; 1 out of 11 children; and 1 out of 4 families. Given the marked negative impact of this disease on the quality of life and the productivity of those affected by it, its socio-economic costs are clearly very high. Unfortunately, a stigma surrounds migraine, and this has profound implications on everything concerning migraine patients, from the allocation of healthcare resources to patients' efforts, both individual and collective, to reduce the negative impact of the disease (Parikh and Young 2019). Understanding the stigma of migraine and learning how to develop effective ways to mitigate it can increase the quality of life of these patients. The Alliance for Headache Disorders Advocacy, for example, has sought to address the structural stigma inherent in discriminatory policies of employers, government agencies, and public institutions. Such efforts can help considerably to improve the conditions of these patients (Shapiro 2020), as well as reduce the negative impact of workplaces that fail to meet their needs.

On 14 July 2020, in Italy, an important law concerning primary chronic headache was passed. Law 81/2020 recognises headache as a social disease. It represents a fundamental step towards having clear, certain, and well-defined regulatory references and a system designed to guarantee the patient prompt entry into the healthcare system, a correct diagnosis, and adequate therapies.

Recognition of migraine as a social disease, however, does not automatically imply its recognition as a disabling disease. For many migraine sufferers today, being recognised as a person with disability seems to be the only way they can legitimise their status as "sick people" in workplaces that they continue to find absolutely inadequate for the needs of people with invisible diseases.

In an economic and social context in which companies are increasingly building their policies around the concepts of social sustainability and employee well-being, it has become necessary to rethink the workplace in such a way as to make it more inclusive for those suffering from diseases that cause temporary, permanent or dynamic disability. We need to rethink the workplace in terms of a work environment that is expressed in several dimensions: spatial, organisational, and relational.

This goal can be achieved only if the accommodations made stem from an awareness of the extent to which the environment can be a facilitator or an obstacle in our daily lives.

Gaining this awareness demands a change in perspective. The workplace has to stop being a place you need to escape from when you are sick, an environment full of triggers, where migraine is a taboo subject and those affected by the condition are stigmatised as "shirkers".

We need to rethink the work environment in terms of making it a welcoming and safe place that helps people with migraine to manage their disease and, as such, provides them with additional support alongside the drug therapies and other non-pharmacological strategies that can help them to manage their disease and feel better.

What effects would a change of this kind have?

- Reduced presenteeism and absenteeism and increased productivity.
- Reduced social costs of migraine.
- Reduced impact of the disease on the lives of those who have it.
- Reduced impact of the disease on social relations at work.

Recognition of migraine as a social disease does not automatically imply its recognition as a disabling disease

The Workplace as a Facilitator

Work is where the majority of people of working age spend most of their day. Attention to the well-being and safety of people in the workplace is therefore crucial not only to their experience of both the work and the place but also to their whole quality of life.

Companies and organisations, in general, are becoming more and more oriented towards discovering, embracing, and managing diversity, a trend that sees them valuing the uniqueness of people through the application of a philosophy of inclusivity in different areas: communication and attitudes, organisation and procedures, environmental planning, and safety.

Diversity and inclusion are the focus of the "ISO 30415:2021 - Human Resources Management - Diversity and Inclusion" standard, a reference document that helps those organisations that value diversity as an essential condition for business growth and greater efficiency and competitiveness to integrate this principle into their management systems. Its aim is to help organisations to develop inclusive workplaces by addressing inequalities in their systems, policies, processes, and practices, as well as in people's conscious and unconscious biases and behaviours.

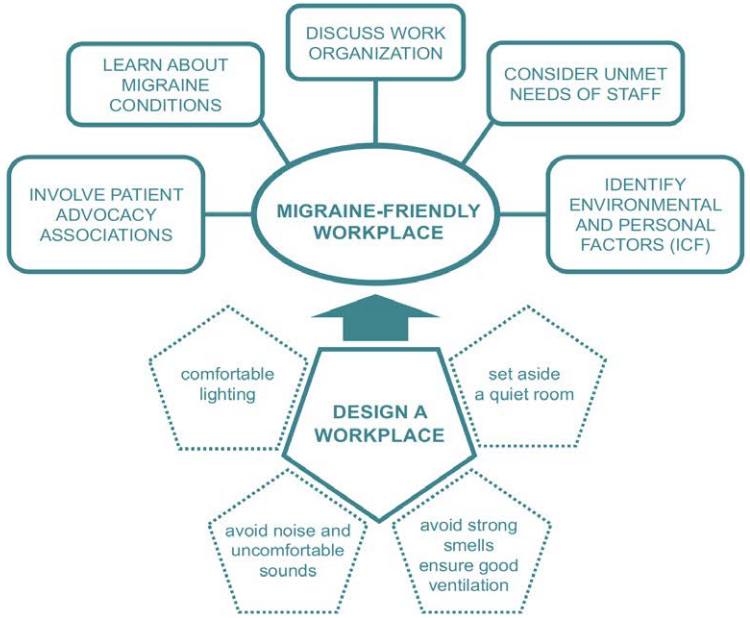


Figure 1: How to design a migraine-friendly workplace

It is important to consider that workplaces are not frequented exclusively by workers, but also by occasional or regular visitors (e.g., customers, users, maintenance technicians, etc.), who may spend anything from minutes or hours to whole days, or longer, there. In fact, workplaces include schools, health facilities, places of cultural interest, hospitality facilities, commercial establishments, sports facilities, public entertainment venues, and all production facilities and public offices. Many of these places, such as cinemas and shopping malls, are crowded, and some activities are carried out in open spaces.

Although these places differ structurally and in terms of their spaces, fittings and functions, as well as the people who use them, they all seem to be designed with more attention to the "container" and its intended use than to the performance levels determined by the interaction between the environment and people.

In other words, the aspect that most designs seem to neglect is precisely the human component: people and their different needs and abilities. Or, at best, they employ models that do not really reflect human variability and its nuances and are thus based on a representation of this component that does not correspond to reality.

It is important to promote awareness of how an environment can hinder or facilitate the autonomy in ordinary situations of each person in it, not to mention individual performances, and thus the collective response, in emergencies (Schiavone 2021).

In the International Classification of Functioning, Disability and Health (ICF), disability is conceived as an umbrella term covering impairments, activity limitations, and participation restrictions. It denotes the negative aspects of the interaction between a person's health condition(s) and that same individual's contextual factors (environmental and personal factors).

Unfavourable environmental conditions with respect to individual health conditions can indeed cause disability (albeit not certifiable disability) or, in any case, limit autonomy and generate discomfort and malaise.

One example of how context can represent a barrier for many, or sometimes al people is that of an emergency situation, where the effects of some major event, be it a fire, earthquake, flood or other, change the whole scenario, with the result that the services provided in ordinary circumstances are no longer guaranteed or adequate.

This example underlines the importance of designing workplaces according to the criteria of inclusive safety and of including, in the emergency prevention and management system, solutions that also enable people with disabilities to respond independently to emergency situations. Or in any case, solutions that envisage adequate training of operators and rescuers take into account the possibility of needing to help or rescue people according to their specific individual needs (Zanut and Schiavone 2021).

There are several ways to help support people with migraine in the workplace and increase their productivity. These include workplace migraine education and management programmes, the creation of migraine-friendly work environments, migraine treatment optimisation, and advocacy (Dodick et al. 2018). Adapting the workplace to patients' needs could also significantly

improve their condition.

Below we examine several elements that can improve the performance of the environment vis-à-vis people who suffer from migraine and represent facilitators for those with other disabilities too.

Designing a Workplace That Considers the Needs of People With Migraine

In research conducted by the University of Rochester School of Medicine and Dentistry (Rochester, NY), the following emerged: "Migraineurs often describe environmental triggers of their headaches, such as barometric pressure change, bright sunlight, flickering lights, air quality, and odours. Environmental aspects of indoor spaces and workplaces are also implicated in migraine experiences. Comprehensive migraine treatment programmes emphasise awareness and avoidance of trigger factors as part of the therapeutic regimen" (Friedman and De Ver Dye 2009).

In light of new knowledge, efforts to improve the workplace user experience, for workers generally and for those with migraine, in particular, should focus more on the correlation between trigger factors and symptoms, both to prevent headache attacks and also to facilitate recovery from them.

Below we provide a concise (and therefore not exhaustive) overview of migraine symptoms and possible measures, useful for creating a more inclusive and accessible environment for people with this and also certain other conditions.

Photophobia: hypersensitivity to light

- Who has this sensitivity? It occurs in more than 80% of people with migraine and can also be found in neurological diseases such as multiple sclerosis (MS), autism spectrum disorders, eye diseases, and as a side effect of some drugs;
- What does it entail? It can cause migraine in predisposed subjects, but also discomfort and ocular pain;
- What are its environmental triggers? Sunlight and artificial light.

Environmental facilitators to prevent and reduce the impact of photophobia:

- Use shading systems for windows and glass walls that make it possible to adjust the intensity and direction of natural light;
- Use artificial lighting systems that allow the environment to be adapted to specific situations, work phases, or users' temporary needs;
- Avoid lighting fixtures in which the light source is directly visible;
- Opt for indirect lighting;
- Equip workstations with adjustable lighting systems (adjustable direction, luminance, and light temperature);
- Avoid reflective surfaces.

Phonophobia: an aversion to sounds that are normally tolerated, i.e., normal ambient sounds

- Who has this sensitivity? This symptom is found in 70-80% of migraine patients during an acute attack; in general, people with sensory hypersensitivity can also experience these symptoms, including people on the autism spectrum and people with hyperacusis, misophonia, tinnitus, or neurodegenerative conditions such as MS;
- What does it entail? It can cause migraine in those who suffer from the condition; sensory stimulation can be a cause of meltdown in autistic subjects.
- What are its environmental triggers? Sounds, music, and noises whose frequency and volume are not tolerated (tolerability is subjective), such as the sounds of traffic, dishes, loud conversations, sirens, and alarms.

Environmental facilitators to prevent and reduce the impact of phonophobia:

- Avoid creating environments liable to generate echoes and reverberations;
- Avoid bells, ringtones, and loud music;
- Avoid loud alarms, sirens, and voice messages;
- Adopt noise mitigation measures (e.g., sound-absorbing panels and furnishings) in large, highly crowded environments and wherever else they are considered necessary.

Osmophobia: increased sensitivity and intolerance to some smells

This is subjective and varies from individual to individual. In some predisposed subjects, strong smells are a migraine trigger, while in others, sensitivity and intolerance increase during headache attacks.

- Who has this sensitivity? It affects 84% of patients suffering from migraine with aura, 74% of those affected by migraine without aura, and 43.3% of those with tension-type headaches. It can also occur in some psychiatric disorders, in pregnant women, and in people whose sense of smell is affected by the drugs they are taking.
- What does it entail? It can cause migraine (in migraine sufferers), nausea, and vomiting;
- What are its environmental triggers? The most offensive smells are strong perfumes, food smells, and cigarette smoke.

Environmental facilitators to prevent and reduce the impact of osmophobia:

- Avoid perfume diffusers;
- Choose odourless cleaners and disinfectants;
- Use extractors in kitchens and wherever processes are being carried out that involve the use of solvents, paints, or other materials with smells/perfumes that can trouble the most sensitive people;
- Ensure good air exchange through natural ventilation;
- Use air purification systems where necessary.

Given the subjective nature of migraine symptoms,

triggers, and intensity, in addition to taking all the basic precautions to ensure the well-being of workers, it is always advisable to share with them any decisions on specific environmental measures to be implemented.

The various environmental facilitators listed are all expedients that, if duly considered in the design phase, together with any solutions necessary for customising the environment, can easily be regulated during the use of the building.

A design approach that takes into account the variability of human needs will improve the quality of the environment as a whole, guaranteeing full accessibility and safety of spaces, equipment, and services for everyone. Involving workers in the sharing of needs and related choices is essential for the creation of an inclusive workplace. In the context of efforts to meet the needs of people with migraine, this approach should be extended, beyond issues concerning the physical space, to a discussion of the organisation of work and of individual behaviours that can act as triggers, such as wearing perfume or smoking cigarettes, including e-cigarettes.

It is essential that teams designing work environments include technicians with expertise in accessibility, lighting, and acoustics so as to guarantee the creation of environments capable of responding and adapting to the specific needs of people and contexts.

In addition to working on elements capable of reducing the risk of the onset of symptoms and of mitigating their impact, it is useful to provide, where possible, an environment where people affected by migraine can isolate and recover.

A quiet room can be appreciated not only by people with migraines but also by those with autism spectrum disorders recovering from a meltdown, by those with MS fatigue, or with other specific needs. Soft furnishings where people can lie down, low saturation colours, plants, and colour-adjustable lights are some of the measures that can be adopted in the quiet room. The design of the emergency prevention and management system, including the orientation and wayfinding system, the emergency devices, the alarm system, and the escape routes, must also take into account the specific needs described above since a stressful situation, like an emergency, can trigger an attack and consequently impair the individual's ability to adequately respond (Schiavone 2022).

Conflict of Interest

None. ■

REFERENCES

Dodick D, Edvinsson L, Makino T et al. (2018) Vancouver Declaration on Global Headache Patient Advocacy 2018. Cephalalgia. 38(13):1899-1909.

Friedman DI, De Ver Dye T (2009) Migraine and the Environment. Headache The Journal of Head and Face Pain. 49(6):941-952.

Parikh SK, Young WB (2019) Migraine: stigma in society. Curr Pain Headache Rep. 23(1):8.

Schiavone E (2022) Progettare la sicurezza inclusiva: da dove iniziare? in PdE, Rivista di psicologia applicata all'emergenza, alla sicurezza e all'ambiente, Anno 19, numero 63, Giugno 2022, ISSN 2531-4157 (p. 7/10).

Schiavone E (2021) Dalla sicurezza dei luoghi alla sicurezza delle persone, in PdE, Rivista di psicologia applicata all'emergenza, alla sicurezza e all'ambiente, Anno 18, numero 60, Ottobre 2021, ISSN 2531-4157 (p. 7/10).

Shapiro RE (2020) What will it take to move the needle for headache disorders? An advocacy perspective. Headache. (9):2059-2077.

Shimizu T, Sakai F, Miyake H et al. (2021) Disability, quality of life, productivity impairment and employer costs of migraine in the workplace. J Headache Pain. 22(1):29.

Zanut S, Schiavone E (2021) Persone reali e sicurezza inclusiva. Il contributo della progettazione inclusiva alla sicurezza di tutti, in ANTINCENDIO n.1/2021(p. 56/71), EPC Editore.

Medical Imaging

Future Trends in Radiology and Healthcare

Mathias Goyen | Chief Medical Officer, Europe, The Middle East & Africa | GE Healthcare

An overview of the big trends in radiology/healthcare and what this means for the future of radiology, GE Healthcare and the industry.

Key Points

- Data will need to be more integrated to provide longitudinal insights, enabling quicker and more impactful decision-making with Artificial Intelligence (AI).
- Staff shortages and burnout among radiologists have been an issue for years and are now more widespread than ever.
- Technology will play a key role in reducing disparities in outcomes by making care more accessible in rural and remote areas.
- Demand for theranostics, a combination of the terms therapeutics and diagnostics, is expected to increase.

Four key trends in radiology/healthcare were highlighted during the Radiological Society of North America (RSNA) Congress in Chicago this year. These include:

Using AI to Transform Data into Actionable Insights

There is an abundance of data in healthcare, but it is spread across too many places and is not actionable. The clear expectation from our customers is to make data more integrated to provide longitudinal insights, enabling quicker and more impactful decision-making with Artificial Intelligence (AI).

On-device AI continues to be important, meaning AI embedded into the device, the CT/MR/ultrasound scanner, but the clear feedback was that GE Healthcare was already pretty good with regard to pixel AI. However, departmental AI or enterprise AI will become more important in the future. This includes GE Healthcare's no-show app, Imaging Insights, or the Edison Orchestrator - the workflow management system that simplifies the selection, deployment, and usage of AI.

Healthcare Workforce Shortages & Burnout

Staff shortages have been a top priority for leaders across healthcare. Burnout among radiologists has been an issue for years and is now more widespread than ever. There is also the problem of rad-tech shortages.

Work overload is commonly cited as one of the main causes of burnout. But workload may not be the root cause in radiology. Burnout in radiology may be more related to a radiologist's ability or the amount of time they need to provide the kind of care they want.

AI can provide intelligent assistance in the radiologists' workflow, automating repetitive and tedious tasks, so they can focus more of their time on the actual read and put together their insights to provide a narrower differential diagnosis. Also, a less focused benefit of AI is that it can reduce a radiologist's diagnostic uncertainty. It also supports them in creating richer and more definitive reports that can translate into more informed clinical decisions with higher diagnostic confidence. Using AI this way can increase radiologists' satisfaction with their work. This could help reduce stress, leading to less radiologist burnout.

Therefore, when considering the adoption of AI into

practice and workflows, think beyond increasing productivity or reporting turnaround times. Instead, find ways in which it can assist with providing more meaning and higher levels of work satisfaction.

ultrasound images. Areas in rural India, Sub-Saharan Africa, and other parts of the world where there is little or no access to medical care or imaging, in particular, could benefit from such a device. With a device like this, a doctor or midwife can examine, for example, a pregnant woman and decide if the pain she's having is normal or if she needs to travel probably 15 hours to get medical care.

the terms therapeutics and diagnostics and describes the combination of using one radioactive drug to identify (diagnose) and a second radioactive drug to deliver therapy to treat the main tumour and any metastatic tumours. It is expected that the demand for theranostics will increase as imaging equipment is needed for many uses. This is especially significant following the FDA approval of several new drugs and therapies, including Lutetium-177 PSMA-617 – an exceptional therapy for advanced prostate cancer. GE Healthcare is "all in" with regard to theranostics. ■

AI can support radiologists in creating richer and more definitive reports that can translate into more informed clinical decisions with higher diagnostic confidence

Using Technology to Increase Access to Care

Technology will play a key role in reducing disparities in outcomes by making care more accessible in rural and remote areas.

The Vscan Air, for example, may be called the doctor's new stethoscope. It is a portable ultrasound system that fits into the pocket and can generate high-quality

Imaging Technology Will Be Used In New, Innovative Ways

Think of theranostics. Theranostics is a combination of

Point-of-Care EEG in the ICU: Towards a New Standard of Seizure Care

Stephan Mayer | Director | Neurocritical Care and Emergency Neurology Services | Westchester Medical Center Health System | USA

Nonconvulsive status epilepticus (NCSE) is often invisible or impossible to distinguish from other sources of altered mental status. Without immediate and continuous access to EEG monitoring, physicians must treat without confirmation or delay their diagnosis. Point-of-Care EEG is helping to close both these gaps and make EEG accessible across health networks.

Key Points

- Electrographic seizures have major implications for patients' lives, ranging from neurological damage to the possibility of a permanent coma.
- While anti-seizure medication is effective and widely available, the limitations of conventional EEG undercut the timely treatment of this serious threat to patient health.
- The operation and interpretation of conventional EEG means most physicians must wait hours and sometimes days to reach a diagnosis of nonconvulsive status epilepticus (NCSE).
- A point-of-care EEG-enabled brain monitor from Ceribell meets the needs of the critical care unit by detecting suspected seizures without the presence of a neurologist or EEG technician.

When left untreated, electrographic seizures have major implications for patients' lives, ranging from neurological damage to the possibility of a permanent coma. As in the condition of nonconvulsive status epilepticus (NCSE), these seizures are often invisible or impossible to distinguish from other sources of altered mental status without the use of electroencephalography. Thus while anti-seizure medication is both effective and widely available, the limitations of conventional EEG have long undercut the timely treatment of this serious, prevalent threat to patient health (Sutter 2016).

The operation and interpretation of conventional EEG means most physicians must wait hours and sometimes days to reach a diagnosis of NCSE, even in the best of circumstances. Without immediate and continuous access to EEG monitoring—including the technicians to operate the equipment and interpret the results—physicians must either treat without confirmation or delay their diagnosis, leading to a need for more medication, increased monitoring, worse injury, and a longer length of stay.

These delays negatively impact patient outcomes even at large medical centres specialising in neurocritical care. The problem is even more pronounced at smaller community hospitals, where it is not just the delay in diagnosis but the lack of EEG access altogether that poses the greatest challenge. Without a way to rule out NCSE, physicians typically have to transfer any patient with suspected seizure activity.

To address the drawbacks of this default approach to seizure care would mean expanding access to neurological monitoring beyond hub medical centres—and eliminating the delays in diagnosis and monitoring gaps

that remain even within those centres. Point-of-care is helping is helping to close both these gaps and make EEG accessible across health networks.

The Extent of the Problem

Epidemiologic evidence shows that electrographic seizures that can only be picked up by EEG, with minimal or no clinical manifestations, are detected in around 13% of patients with sepsis-associated encephalopathy and and around 30% of patients with haemorrhages into the brain, subdural haematomas, intercerebral haemorrhages, and the like (Strein et al. 2019). In fact, what we've learned from our vantage point in the ICU is that the vulnerability of the brain to injury extends far beyond the conventional neurocritical care population of patients with strokes, brain haemorrhages, and trauma. Being critically ill for any prolonged amount of time can do damage to the brain by increasing vulnerability to encephalopathy, delirium, and disorders of consciousness.

To assess all of these cases requires more EEG capacity than we currently have. Many hospitals—particularly smaller hospitals or community hospitals—have fewer conventional EEG machines than they would need to appropriately diagnose nonconvulsive seizures. The cost of the equipment is often not the greatest barrier, though: it's the technicians who operate and maintain it, in addition to the neurologists needed to interpret its results. Both of those roles are ones smaller hospitals have difficulty filling.

In some ways, this lack of personnel has ended up clouding the question of how aware we are of this highly prevalent, highly damaging condition. Most neurocritical care units do see a large number of patient transfers specifically for EEG monitoring, however, which suggests that it's not limited awareness but limited resources that are slowing down the diagnosis and treatment of NCSE.

Similarly, it's not the availability or even the complexity of the treatment which limits our ability to care for these patients: it's simply knowing with certainty who needs it and who doesn't. And then, for those who do need medication, when have we given enough? Whether to make a diagnosis after initial seizure activity or to assess the efficacy of anti-seizure treatment, more than a third of all critical patients will require continuous EEG—and those with refractory status may need a week or more of monitoring. Traditionally, the demand for such resource- and time-intensive monitoring could only be fully met at a few hub hospitals with the expertise and staff power to perform it. In nearly all contexts, then, the need for EEG has always outstripped the supply.

> It's not limited awareness but limited resources that are slowing down the diagnosis and treatment of NCSE

A Breakthrough Tool

Attempts have been made to address this gap. Prior to the advent and FDA approval of rapid-EEG technology, device manufacturers experimented with a limited montage that anybody, not just a trained technician or neurologist, could put on the patient. For a variety of reasons, however, these attempts have not worked out.

A new, point-of-care EEG-enabled brain monitor from Ceribell meets the NCSE needs of the critical care unit by delivering automated seizure detection without the presence of a neurologist or EEG technician. The device consists of a headband with an array of ten EEG contacts that anyone can apply—doctors, trainees, nurses, techs, respiratory therapists—as well as an AI-powered algorithm tthat NCSE takes about five minutes to produce a yes/no notification for seizure activity. A 2020 multi-centre observational study showed that this technology improved the sensitivity of physicians' seizure diagnosis from 78% to 100% and increased the specificity of diagnosis from 64% to 89%; the time it took to reach these diagnoses was about five minutes, opposed to the hours of delay with conventional EEG (Vespa et al. 2020). Like other vital sign monitors, this device can be applied immediately and then left on the patient.

The ease of use and clarity of this new brain monitor has two related benefits for hub-and-spoke health systems like the Westchester Health Network. Our system consists of smaller feeder hospitals and a hub, the Westchester Medical Center, a large quaternary care stroke and trauma centre north of New York City. Our feeder hospitals, which have the ability to transfer complex patients to the hub, can shift from zero access to EEG to having access with Ceribell. For the hub hospital, it means we can start EEG monitoring for patients immediately, regardless of EEG technician availability. Because the headband monitor can be left on the patient to provide EEG monitoring in the off hours, we can deliver a consistent standard of care even when EEG technicians are off duty or otherwise occupied. Spoke hospitals can determine with accuracy

whether or not a patient must be transferred, and our hub can perform what we call "far forward monitoring," which includes catching NCSE before it has the time to develop into refractory status, which responds less well to treatment.

The gold standard for EEG monitoring and assessment is always going to be a human, an expert encephalographer. Point-of-care EEG is not a one-to-one replacement for conventional EEG. For one, it doesn't have the same spatial resolution: it measures brain electrical activity on the lateral aspects of the hemisphere in a straight line along each side of the temple. With its additional electrodes, conventional EEG includes additional electrodes towards the vertex or top of the head. point-of-care monitor is not replacing conventional EEG; it's replacing no EEG, or EEG that is inaccessible at the time when it is most needed.

Case Examples

On a recent night, a patient came into the ICU with convulsive seizures. The patient was intubated and started on midazolam. For whatever reason, the EEG tech wasn't there that night, so we hooked up Ceribell's brain monitor and started it between 10:30 and 11:00 PM. Without point-of-care, we would have had to wait eight or nine hours—until the tech came back to work in the morning—to assess the patient for seizure activity. We had given medication to treat her seizures, but without EEG, we had literally no way of knowing if we were successfully eliminating the seizures or not. The monitor let us know definitively that the patient had received enough medication to suppress the seizures. If we had seen any additional activity, this case could be considered an example of "far forward monitoring," where we find out early if we have to escalate our intervention.

The other use case is at our feeder hospitals, which may have a neurologist see a patient for a change in the level of consciousness when the CT is unrevealing. Whereas in the past, the patient would have had to wait hours or a day simply to get a 30-minute spot EEG—which again is not as sensitive as prolonged monitoring—these hospitals can now perform this monitoring themselves with Ceribell. What that earns those feeder hospital physicians is situational awareness: they can be confident that they have ruled out NCSE have ruled out seizures after several hours of automated monitoring (where a clear alarm notifies them if there is suspected seizure activity). If seizures are detected, and they realise they'll be hard to treat, the patient can be transferred to the neurocritical care unit at our hub hospital. If not, they can avoid transferring the patient simply to get a conventional EEG. And the more those hospitals become practiced in using Ceribell, the more we are able to establish and refine our tele-ICU service, extending our neurocritical expertise and enabling our hub intensivists and neurologists to help assess potential transfers.

Towards a New Standard of Care

Stroke is acknowledged to be a massive public health problem and, as such, has been positioned squarely in regulators' crosshairs. Standards of care have been established and disseminated—sometimes to the public as well as to healthcare provider organisations—and these standards are now used to measure and incentivise healthcare organisation performance. Similar measures are in place for evaluating and certifying comprehensive epilepsy centres offering outpatient treatment and epilepsy surgery programmes.

The emergency treatment of status epilepticus has not evolved to that level yet. As early as a 2001 clinical trial (Alldredge et al. 2001) and certainly since the Rapid Anticonvulsant Medication Prior to ARrival Trial (RAMPART) (Silbergleit et al. 2011), it has been well established that seizures are more responsive to treatment the earlier they are treated. Yet even with that knowledge, there are still no guidelines to help hospitals meet the challenge of treating status epilepticus as a. time-sensitive neurological emergency. Part of the reason may be the historical lack of tools to allow hospitals to meet those guidelines—i.e., the lack of a quick, accurate, accessible way to assess for seizures.

Now that we actually have the tools, it's time to rigorously study different treatment approaches in-depth and work towards establishing a new standard of care. ■

REFERENCES

Alldredge BK et al. (2001) A comparison of lorazepam, diazepam, and placebo for the treatment of out-of-hospital status epilepticus. N Eng J Med. 345(9):631-7.

Silbergleit R et al. (2011) RAMPART (Rapid Anticonvulsant Medication Prior to Arrival Trial): a double-blind, randomized clinical trial of the efficacy of intramuscular midazolam versus intravenous lorazepam in the prehospital treatment of status epilepticus by paramedics. Epilepsia. 52(Suppl 8):45-7.

Strein M, Holton-Burke JP, Smith LR, Brophy G (2019) Prevention, Treatment, and Monitoring of Seizures in the Intensive Care Unit. J Clin Med. 8(8): 1177.

Sutter R (2016) Are We Prepared to Detect Subtle and Nonconvulsive Status Epilepticus in Critically Ill Patients? J Clin Neurophysiol. 33(1):25-31.

Vespa P et al. (2020) Evaluating the Clinical Impact of Rapid Response Electroencephalography: The DECIDE Multicenter Prospective Observational Clinical Study. Crit Care Med. 48(9):1249-1257.

Stability in the Face of Change

Joerg Aumueller | Vice President and Global Head of Enterprise Solutions | Straumann Group

An interview with Joerge Aumueller providing an overview of the changes in the dental industry giving rise to dental service organisations and the challenges they face in fulfilling the promise of consolidation, creating a greater end-to-end experience for patients and strengthening operations and efficiency.

Key Points

- Dental service organisations (DSOs) can lead the way in dentistry's transformation as a technologically advanced field.
- DSOs need to ensure standardisation in the quality of care, build meaningful relationships with patients and consumers, enhance reputation and brand recognition, and increase efficiency.
- DSOs are ideally suited to capture the benefits of the dental industry's consolidation and growth.
- The key challenges for DSOs are integrating technologies to deliver a high-quality, end-to-end patient experience, creating a supportive clinician environment and ensuring cost-effective business operations.

Opportunities for Growth

Dental service organisations (DSOs) are facing unique challenges. These include operational inefficiencies, lack of standardisation, and a shortage of qualified dental staff. This is mainly an outcome of being built from the ground up and acquiring practices with differing philosophies, systems, and protocols.

There is a need for DSOs to discover ways of ensuring standardisation in the quality of care, building meaningful relationships with patients and consumers, enhancing reputation and brand recognition, and increasing efficiency within highly fragmented workflows and diverse infrastructures. Today, patients are digitally empowered and better informed and have become a catalyst of rising healthcare consumerism and an increase in demand for personalised treatment.

End-to-end oral health enablement can be the pathway to improve patient experience and outcomes. The Straumann Group understands these needs and can become a long-term partner to help unlock the potential of oral health through the following measures:

- Activating growth potential by generating additional consumer demand across specialties and mining for high-value treatment opportunities.
- Sustaining clinical excellence by ensuring high treatment quality and reduced variability in care delivery.
- Improving operational efficiency by increasing case efficiency and throughput and optimising workflows.

There has never been a more important time for DSOs to transform business operations by finding efficiencies across the patient pathway, enhancing technology, activating patients, and establishing clear and harmonised standards of care.

Transforming the Dental Industry

The dental industry today is consolidating as clinicians seek relief from pressures ranging from dental school debt, business headaches and rapid technological change. According to a report from the American Dental Association (ADA), independent practices in the U.S. have dropped from nearly 85% of dentists in 2005 to 73% in 2021. Solo practices have declined even further, to just over 46% of dentists. As standards of living rise and more consumers are able to access quality care, the U.S. and global dental services markets

are expected to grow at an average of 6.4% per year, reaching more than $550 billion by 2028 (Grandview Research 2021).

DSOs are ideally suited to capture the full benefits of the industry's consolidation and growth. They can serve and support dental practices, offer back-office business management, access to laboratories, marketing, hiring of support staff, professional training, and more. DSOs represent about 10.4% of U.S. dentists as of 2019—the most recent available ADA estimates (American Dental Association Health Policy Institute 2020) but are expected to grow almost 100% from 2018 to 2025 and triple their market share by 2035.

DSOs can lead the way in dentistry's transformation as a technologically advanced field serving more consumers than ever before and ensuring high-quality standards and affordable dental care. However, this will be challenging to achieve. Despite consolidation, the dental industry still remains highly fragmented - from the technologies for specific procedures to the business processes that general dentists, specialists, and laboratories use to interact and exchange information.

The two key challenges facing DSOs include ensuring standardisation and quality of care and integrating clinicians with different levels of experience and at different stages of their careers. DSOs must also build greater patient trust, activate leads, maintain efficient communication and production schedules with labs, and increase workflow productivity. In addition, dental practices need to educate patients on the most appropriate treatment options.

DSO Value Proposition

With an ageing population and an increase in demand for tooth replacement, the global implant market is expected to grow to $6.7 billion by 2026, up from $4.6 billion in 2019 (Research and Markets 2021). Cosmetic dentistry, including implants, prosthetics, teeth whitening, and other treatments, is expected to grow globally by 7.9% per year to more than $41 billion by 2028 (Research Dive 2021). These trends are encouraging for the industry and are likely to benefit all dentists, whether it is a solo practice, group practice, or a DSO-affiliated practice.

Many dentists, particularly younger ones, find value in the DSO model. DSOs offer stable income compared with the uncertainties of building a practice—some DSOs even help pay off loans. According to recent figures from ADA, dentists 34 and younger are four times as likely as dentists in their 50s and early 60s to join DSOs. DSOs enjoy economies of scale in purchasing equipment and supplies, and their financial resources can help during uncertain times.

Serving Consumers Across their Journey

Consumers today are better educated and more selective about treatments and clinicians. For DSOs, the challenge is not limited to attracting new patients but also retaining them. For example, software investments can make a big difference in the customer experience, such as apps allowing patients to schedule their appointments. As consumers become more informed and selective, dentists have to become more professional and service-oriented. Dental practices need to have a range of disciplines, from paediatric dentists to implant specialists. Offering multiple services under one roof can attract multigenerational families, increase the chances of keeping a patient for life, and promote patient loyalty. DSOs also need to connect with consumers at an emotional and intellectual level. This can help patients open up about their conditions and their needs.

The influence of DSOs will continue to grow as the global dental market expands, complexities of running a dental practice escalate, and use of advanced technologies becomes standard practice

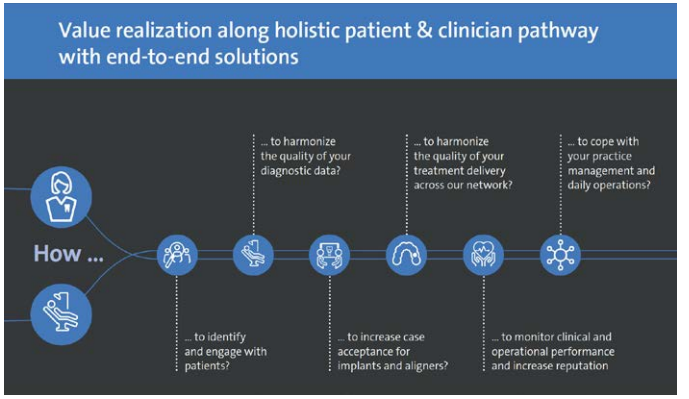


Figure 1: Value realisation along holistic patient and clinician pathway with end-to-end solutions

Digital Transformation of Dentistry

New technologies are reshaping how dentists treat patients. For example, in recent years the growing adoption of digital intraoral scanners and handheld devices offer the ability to obtain accurate, real-time images of a patient's mouth. Similarly, cone-beam computed tomography or CBCT can take multiple images from different angles and create a 3D image of a patient's teeth, jaw, and neck. There is also technology that can digitise patient records. The next iteration of dental technology will be artificial intelligence (AI). In future, AI will play a greater role in the early diagnosis and prevention of oral cancer and other diseases.

Clinician-Based Culture

DSOs must use their size and financial resources to lead the way as quality care providers. This will include prioritising clinicians and patient care, focusing on transparency, and involving clinicians directly at the highest levels of decision-making. Clinicians should be encouraged to learn best practices from one another and harmonise and elevate the quality of care. In addition, they should be directly involved in a DSO's key decisions. Clinicians have frontline experience treating patients and can bring valuable perspectives on elevating treatment quality and the patient experience.

Conclusion

Successful companies empower dentists to grow and develop with the organisation. Every organisation has its own culture. The influence of DSOs will continue to grow in the years to come as the global dental market expands, the complexities of running a dental practice escalate, and the use of advanced technologies becomes standard practice. With their financial resources and national to international reach, DSOs are well-positioned to support clinicians, serve consumer needs, and define the future of oral health. Organisations that grow with purpose, help clinicians, do the work they love, and earn the loyalty and trust of consumers will be the ones that truly cement the DSO model. ■

Does your DSO offer these benefits to patients?

- **A seamless patient path from problem to solution in an all-in-one treatment model.** You are able to cover the expectations of different patient groups and actively create and test new care options.
- **Holistic care and best-in-class experience.** You deliver high-quality treatment and preventive care every day and the patient is engaged in every stage of their care.
- **A revolutionary new experience enhanced by digital technologies.** You guarantee flexibility and care collaboration through online services and top-level visit organizations.
- **Strong trust-based patient-provider relationships.** You develop long-term relationships with the patients that are based on trust and loyalty. In addition to clinical competency, care providers demonstrate people skills that allow them to form bonds with patients.
- **A healthy smile as a 365-day experience.** Patients sense that their oral healthcare provider cares about helping them prevent disease and enjoy optimal oral health at all times.
- **24/7 care with advanced digital support for customers.** Patients feel confident that they can contact their affiliated dental practice from the moment an oral health concern arises.

REFERENCES

American Dental Association Health Policy Institute (2020) How Big are Dental Service Organizations? Available at https://www.ada.org/-/media/project/ada-organization/ada/ada-org/files/resources/research/hpi/hpigraphic_0720_1. pdf?rev=832fb3ea006946bab3030d023c3694e7&hash=4707F315F0EB8FE5BFC77B45DDF1788A.

Grand View Research (2021) Dental Services Market Size, Share & Trends Analysis Report By Type (Dental Implants, Cosmetic Dentistry), By End Use (Hospitals, Dental Clinics), By Region (North America, Europe, APAC, LATAM, MEA), And Segment Forecasts, 2021-2028. Available at https://www.grandviewresearch.com/industry-analysis/dental-services-market-report.

Harvard Business Review (2022) Growing with Purpose to Transform the Dental Industry. Available at https://hbr.org/sponsored/2022/07/growing-with-purpose-to-transform-the-dental-industry

Research Dive (2021) Global Cosmetic Dentistry Market Expected to Generate a Revenue of $41,496.0 Million by 2028, Growing at a CAGR of 7.9% from 2021- 2028. Available at https://www.prnewswire.com/news-releases/global-cosmetic-dentistry-market-expected-to-generate-a-revenue-of-41-496-0- million-by-2028--growing-at-a-cagr-of-7-9-from-2021-2028-197-pages-reveals-by-research-dive-301432772.html.

Research and Markets (2021) The Dental Implants Market Is Projected to Grow at a CAGR of 5.66% to Reach $6.711 Billion Globally by 2026. Available at https://www.prnewswire.com/news-releases/the-dental-implants-market-is-projected-to-grow-at-a-cagr-of-5-66-to-reach-6-711-billion-globally- by-2026--301451440.html.

Innovation and Technology in Healthcare

Thales. Innovative Technologies Will Address Health System Challenges. 22(3):171.
https://iii.hm/1gpf

Remote Patient Monitoring

Sourabh Pagaria. Expanding the Use of Remote Technologies in Healthcare. 22(4):203-206.
https://iii.hm/1hk8

Disease Assessment and Management

Michele Brignole. The Importance of Syncope Assessment Diagnosis and Management. 22(1):30-32.
https://iii.hm/1f89

James Frith. Syncope Diagnosis, Treatment and Management. 22(6):329
https://iii.hm/1iss

AI: Opportunities, Capabilities and Limits

Henrique Martins, Giorgio Cangioli, Catherine Chronaki. Hospitals-on-FHIR: Preparing Hospitals for European Health Data Space. 22(3):112-118.
https://iii.hm/1gow

Rafael Vidal-Perez. Artificial Intelligence and Echocardiography: Are We Ready for Automation? 22(3):119-121.
https://iii.hm/1gox

Konstantinos Petsios, Maria Chortaria, Simos Kokkovos, Panagiotis Minogiannis. Artificial Intelligence in Radiology: Realities, Challenges and Perspectives from a Tertiary Cardiac Centre in Greece. 22(3):122-125.
https://iii.hm/1gov

Sai Pavan Kumar Veeranki, Diether Kramer, Michael Schrempf. Learning From Each Other: An Artificial Intelligence Perspective in Healthcare. 22(3):130-131.
https://iii.hm/1gp0

Thomas Kau. The Current State of AI in Diagnostic Imaging and How to Improve its Clinical Value. 22(3):132-134.
https://iii.hm/1gp1

Eleonora Barcali, Martina Orlandi, Linda Calistri, Anna Peired, Leonardo Bocchi, Cosimo Nardi. Artificial Intelligence and Radiomics at the University of Florence. 22(3):135-137.
https://iii.hm/1gp2

Ronald B Schilling. The Knowledge Model and Enabling Artificial Intelligence. 22(3):141-143.
https://iii.hm/1gp4

Simon Wilson. Network Modernisation: The Key to the Future of Healthcare. 22(3):144-145.
https://iii.hm/1gp5

Ashley MacNaughton, Deepa Shukla. Digital Twin Technologies - Shortening Waiting Lists and Reducing Inefficiencies. 22(3):146-147.
https://iii.hm/1gp6

Affidea. One Ring to Rule Them All in AI – Affidea's Experience. 22(3):148-149.
https://iii.hm/1gp7

Sourabh Pagaria. Application of Artificial Intelligence in Healthcare. 22(3):162-164.
https://iii.hm/1gpc

Comarch. Telemedicine Care Combined with AI: Capabilities and Benefits. 22(3):168-170.
https://iii.hm/1gpe

Richard Dasselaar. Artificial Intelligence in Healthcare – Realising the Benefits. 22(4):241-242.
https://iii.hm/1hkj

Zisis Sotiriou. A New Era in Operational Excellence - Predicting with Precision to Enable Better Patient Care. 22(5):283-284.
https://iii.hm/1idk

Connected Patients in Light of Big Data

Diogo Neves, Henrique Martins. Linking Patients with Data: Brain-Computer Interfaces and Healthcare Innovation.22(4):187-192.
https://iii.hm/1hk5

Eugene Fidelis Soh, Ong Jing Fang, Dawn Cheng Yi. Flipping Healthcare Through a Population Health Stack. 22(4):193-199.
https://iii.hm/1hk6

Srdjan Babic, Masa Petrovic, Branko Lozuk, Milovan Bojic. Data Science in Modern Healthcare. 22(4):200-202.
https://iii.hm/1hk7

Francisco Maestre, Ana Paula Sorrell Meriño, Christian Mata Miquel, Miguel Cabrer. DICOM Metadata - A Useful Resource for Big Data Analytics. 22(4):207-210.
https://iii.hm/1hk9

Jörg Schwarz. How to Utilise the Massive Amount of Health Data Collected by Consumers to Improve Health Outcomes. 22(4):211-214.
https://iii.hm/1hka

Betsabe Melcon, Josep M Picas, Francesc Lopez Segui, Juan Antonio de los Cobos,Joan Guanyabens. In Search of Gold in Health Data. 22(4):219-220.
https://iii.hm/1hkc

Ashley MacNaughton, Phil Smart, Scott McBride. Transforming Outpatient Services is Key to Delivering and Sustaining Elective Care Recovery. 22(4):221-223.
https://iii.hm/1hkd

Effective Workforce Transformation

Iris Meyenburg-Altwarg. Interprofessional Competence Acquisition in Times of VUCA. 22(5):259-262.
https://iii.hm/1idd

Donna Prosser. Reducing Burnout by Building Resilient Systems. 22(5):263-265.
https://iii.hm/1ide

Michael Seraskeris. The Shortage of Health Professionals Worldwide – A Modern Human Resources Management Challenge. 22(5):270-272.
https://iii.hm/1idg

Brian Hill. Building Winning Recruiting Practices in a Labour Shortage. 22(5):273-274.
https://iii.hm/1idh

Isabella Mellits Lopez, Bonita Dozier, Theresa Rohr-Kirchgraber. Female Physician Infertility in the U.S. 22(5):279-281.
https://iii.hm/1idj

Cybersecurity: Preventing the Worst- Case Scenario

Jonathan Lee. What Can the NHS Learn from Public Sector Supply Chain Attacks? 22(3):166-167.
https://iii.hm/1gpd

Henrique Martins. Is it Safe to Exchange Data? The Need for Integrated Hospital/Healthcare Organisation Interoperability and Cyber and Information Security Plans. 22(6):308
https://iii.hm/1isn

Dan Brown, Tim Hill, Jarius Jackson. Challenges, Strategies and Recommendations to Improve Cybersecurity. 22(6):314
https://iii.hm/1iso

Vito Petrarolo, Giovanni Maglio. Cybersecurity: Preventing the Worst-Case Scenario. 22(6):317
https://iii.hm/1isp

Alexios Antoniou. Internet of Medical Things: Threats and Recommendations. 22(6): 322
https://iii.hm/1isr

HealthManagement.org

Promoting Management and Leadership