



# *4<sup>th</sup> European Hospital Conference*

## *Conclusions*

by

**Dr. med. Erich Theo Merholz, AEMH/VLK**

**Vice-President AEMH**

**Ärztlicher Direktor/Medical COO &  
Chefarzt/Head of the Dept. of Maxillo-Facial Surgery**

**St. Lukas Hospital  
DE-42697 Solingen / Germany**



## ***Conclusion A***

**In Europa werden immer mehr eHealth-Services als reguläres System implementiert und umfassen z. B.:**

- ePatientenakte/ePatientenkarte**
- Telemedizin**
- fitness tracker**

**In Europe more and more eHealth-Services are being implemented as regular systems covering e. g.:**

- epatient file/ehealth-ID-card,**
- telemedicine/mHealth,**
- fitness trackers.**



## ***Conclusion B***

**Die bereits bestehenden eHealth-Lösungen haben die Zustimmung von Ärzten, Kliniken, Patienten und Krankenversicherungsunternehmen, d. h. es gibt eine breite Akzeptanz durch die Stakeholder.**

**The already existing eHealth-solutions have support from physicians, hospitals, patients and health-insurance companies, i. e. there is a widespread acceptance among the stakeholders.**



## ***Conclusion C***

**Von den bestehenden eHealth-Lösungen wird erwartet, dass sie**

- alle relevanten Informationen/Daten ad hoc liefern,**
- somit eine klare Service-Verbesserung bewirken,**
- zu klaren Zeit- und Kosteneinsparungen führen.**

**Expectation is that the existing eHealth solutions can give rise to**

- ad hoc-delivery of relevant information/data,**
- a significant improvement of service quality,**
- substantial savings of time and costs.**



## ***Conclusion D***

**Für die routinemäßige Nutzung von eHealth sind Maßnahmen notwendig, die Sicherheit bieten gegen**

- Hackerangriffe aus dem Internet, z.B. Datendiebstahl,**
- Malware, die Datensätze teilweise oder gänzlich unter externe Kontrolle bringen oder gar löschen kann,**
- versehentliches Löschen.**

**For the routine use of eHealth some measures are pivotal in order to protect against**

- cybercrime-type hacking, e. g. data theft,**
- malware/ransomware which can exert external control over datasets in part or totally or can delete data,**
- inadvertent erasing of data.**



## *Conclusion E*

Das zentrale eHealth-Tool in Europa ist eine **ePatienten-karte/-App**, die den Zugang zu möglichst aktuellen Daten geben sollte, damit eine Klinik bei einem eingelieferten Notfall sofort z. B. Allergien/Unverträglichkeiten berücksichtigen kann.

Key eHealth-Tool in Europe is an **eHealth-ID-card/-App** giving access to patient data as up-to-date as possible so that a hospital gets an overview on e. g. allergies/intolerances of an emergency patient.



# *Conclusion F1*

Um die grenzüberschreitende Behandlung von Patienten zu ermöglichen, sollte ein **Interoperability-Tool** für die Patientenkarte verfügbar sein, das zum Lesen der Patientendaten

- multilingual ist,
- verschiedene Datenbankformate in Europa verarbeiten kann.

Durch die Kenntnis der “Patientengeschichte” können Kliniken dann Notfallpatienten optimal behandeln.

To facilitate the “cross-border” treatment of patients, an **Interoperability-Tool** for the patient card should be available which

- is multilingual,
- is fitted to read the various database formats in Europe.

Knowing the “health history” would enable hospitals to optimally treat emergency patients.



## *Conclusion F2*

Idealerweise sollten die Patientendaten gänzlich gem. ICD-10-CM+PCS kodiert sein. Da aber demnächst die Version ICD-11-CM+PCS gelten wird, sollte den nationalen eHealth-Systemen/Stakeholders ein **Konversions-Modul** für die Konvertierung aller Daten von Version 10 in die dann gültige Version 11 verfügbar sein.

Ideally, patient data should be coded according to ICD-10-CM+PCS. Since version ICD-11-CM+PCS is about to be implemented, European eHealth-systems/stakeholders should have a **conversion module** to transform all version-10 data into version-11 data.





## ***Conclusion G***

**Qualitätsanforderungen an obligatorische Aktualisierungen von Firmware für Geräte z. B. implantierte Herzschrittmacher oder Defibrillatoren sollten klar definiert sein, um unerlaubte externe Manipulationen von vornherein zu unterbinden (s. frühere Geräte eines US-Herzschrittmacherherstellers).**

**Quality assurance requirements for obligatory firmware updates of e. g. implantable cardiac pacemakers or fibrillators should be clearly defined in order to *ab initio* exclude illegal external manipulations (cf. previous issue with *US-cardiac devices*).**



## ***Conclusion H***

**Ebenso sind Qualitätsanforderungen an Services in den Bereichen Telemedizin und mHealth (Health-Apps) zu definieren im Hinblick auf z. B.**

- medizinische Zuverlässigkeit (z. B. Info, Messdaten),**
- keine Weitergabe von Nutzerdaten an Dritte,**

**Similarly, quality assurance requirements of services in telemedicine and mHealth (Health-Apps) are to be defined with regard to**

- reliability of medical service (e.g.info,measurements)**
- protection of medical data, “no leak to 3rd parties”.**



## ***Conclusion I***

**Viele Klinikgeräte wie z. B. Röntgengeräte speisen die Daten online in das Klinik-Netzwerk ein. Auch bei diesen Geräten sind regelmäßige Firmware-Updates notwendig, um “cybersecurity” im Klinik-Netzwerk zu gewährleisten.**

**Several types of equipment like e. g. X-ray equipment forward their data directly into the hospital network. That means that for such equipment regular firmware-updates are essential to maintain “cybersecurity” in the hospital network.**



## ***Conclusion J***

**Viele andere Klinikhilfsgeräte wie z. B. Sterilisatoren sind online über das Internet steuerbar und sind dann Teil des “*Internet of things (IoT)*”. Auch bei diesen Geräten sind regelmäßige Firmware-Updates notwendig, um die ungewollte externe Steuerung zu unterbinden. Die Lieferanten sind auch hier in der Pflicht.**

**Several types of auxiliary equipment like sterilisers can be accessed and programmed via Internet as part of “*Internet of things (IoT)*”. In order to prevent involuntary external control/supervision regular updates are needed - the suppliers must deliver updates!**



## ***Conclusion K***

**Auch Software für die neuen Hardware-Anwendungen von “*Augmented Reality (AR)*” und “*Virtual Reality (VR)*” bei Operationen oder deren Vorbereitung bedarf genauer Qualitätsvorgaben und ständiger Aktualisierungen mit besonderer Sorgfalt, um externe Eingriffe auszuschließen.**

**Software for novel hardware applications like “*Augmented Reality (AR)*” and “*Virtual Reality (VR)*” for operations/their preparation must have defined quality requirements and regular updates worked out with due diligence in order to exclude external invasions.**



## ***Conclusion L - Challenges 1***

**a) Der Schutz von Kliniken und Arztpraxen vor Cybercrime/Malware ist oberste Priorität, da sie sonst nicht ihre Aufgabe ausüben können: nämlich Leben retten!**

**It must be of highest priority to protect hospitals and medical practices against cybercrime/malware - otherwise they cannot carry out their obligation: saving human life!**

**b) Auch die eKommunikation zwischen den eHealth-Stakeholders braucht einen gut funktionierenden Datenschutz für die Patientendaten.**

**eCommunication among eHealth-stakeholders needs well-functioning data protection of patient data.**



## **Conclusion L - Challenges 2**

**c) Wissenschaftlicher medizinischer Fortschritt darf nicht durch fehlerhafte Software/Firmware für medizinische Hardware blockiert werden.**

**Scientific advancement in the medical profession must not be blocked by faulty software/firmware for medical hardware.**

**d) Qualitätsvorgaben für jede medizinische Software/Firmware für medizinische Geräte aller Art und deren Update-Zyklen sind zu definieren und von den Lieferanten verbindlich zu garantieren zum Wohl des Patienten.**

**Quality assurance requirements for each and every medical software/firmware for all types of medical equipment/device as well as their update-cycles have to be pre-defined and must be guaranteed in a binding manner by the supplier for the sake of patients' health.**



## **Conclusion L - Challenges 3**

e) **“Big Data”-artige Auswertungen von Patientendaten dürfen nur in anonymisierter Form erfolgen, da ansonsten in “Big Brother”-Manier der gläserne Patient erzeugt wird, dem dadurch ein wichtiger Teil seiner Privatsphäre und seiner Identität genommen wird. “Big Data” darf niemals zum neuen Kollegen von “Big Brother” werden.**

**“Big Data”-type evaluations of patient data may only be executed in anonymised form since otherwise the transparent patient would be created in a “Big Brother”-like manner who, thereby, would be deprived of an important part of his private sphere and identity.**

**“Big Data” may never become the new colleague of “Big Brother”.**