CISPA
HELMHOLTZ-ZENTRUM i. G.

CISPA | Stuhlsatzenhaus 5 | D-66123 Saarbrücken

Landtag des Saarlandes
Landtagsverwaltung z.H. Peter Schmolenzky

Franz-Josef-Röder Straße 7
66119 Saarbrücken

CISPA – Helmholtz-Zentrum (i. G). GmbH
Saarland Informatics Campus
Stuhlsatzenhaus 5
66123 Saarbrücken | Germany

TEL +49 681 302-71900
FAX +46 681 302-71942
E-MAIL office@cispa.saarland
WEB www.cispa.saarland

Saarbrücken, 20.09.2018

Stellungnahme zum Thema „Stand und Entwicklungsperspektiven der Telemedizin im Saarland“

Sehr geehrte Damen und Herren,

im Folgenden nehmen wir anlässlich der Einladung zur Anhörung des Ausschusses für Soziales, Gesundheit, Frauen und Familie zum Thema „Stand und Entwicklungsperspektiven der Telemedizin im Saarland“ Stellung. Wir beschränken uns dabei auf die Kernexpertise des CISPA, d.h. auf Fragestellungen mit Bezug zur IT-Sicherheit und Datenschutz.

Grundsätzlich sind wir der Meinung, dass ein verantwortungsvoller, sicherer und datenschutzfreundlicher Einsatz von Telemedizin mit dem heutigen Stand der Technik bereits realisierbar ist. Es gibt immer eine Abwägung zwischen Risiko und Nutzen, da eine 100% Absicherung, insbesondere bei der Berücksichtigung der menschlichen Komponente, nicht zu erreichen ist. Das gilt aber für nahezu alle Technologien, die bereits genutzt werden, auch für den Status Quo in der Präsenzmedizin. Wir sehen daher keine grundsätzlichen Ausschlussgründe im Bereich IT-Sicherheit bzw. Datenschutz, die ein Grund wären, Telemedizin nicht einzusetzen. Wir empfehlen hier die Erarbeitung branchenspezifischer Standards ähnlich wie beim IT-Sicherheitsgesetz bzw. dem BSI-Gesetz im Hinblick auf kritische Infrastrukturen. Mit Blick in die Zukunft sehen wir vor allem neue Entwicklungen in der Diagnostik, bei der datenschutzfreundliche Diagnose-Algorithmen neue Möglichkeiten bei der Erkennung von Krankheiten und telemedizingestützter Behandlung bieten. Dies wird aber eher das Feld der digitalisierten Medizin allgemein fortentwickeln, als dass es im Kern die Telemedizin betrifft.

Die Telemedizin stützt sich noch mehr auf digitale Technologien, als dies in der Präsenzmedizin heute bereits der Fall ist. Patientendaten liegen bei der Telemedizin in breiter Masse digital vor und werden über offene Netze (z.B. das Internet) kommuniziert. Das heißt aber auch, dass technische Fehler und Angriffe auf diese komplexen Systeme eine größere Anzahl von Nutzern und Patienten gleichzeitig betreffen können. Mit Blick auf die IT-Sicherheit und den Datenschutz im Kontext der Telemedizin sehen wir daher die größte Herausforderung in der Erstellung eines passenden Gesamtkonzeptes, der fehlerfreien Implementierung und Umsetzung für den Betrieb, um die Nutzung in diesem Anwendungsszenario entsprechend abzusichern. Hinzu kommt die Diskriminierungsfreiheit im Hinblick auf die technische Anbindung gerade in ländlichen Gebieten und die datengestützten automatisierten Einzelfallentscheidungen. Anknüpfungspunkte bzgl. der technischen IT-Sicherheit sehen wir beim Endgerät des Patienten, das für die Sensorik/Diagnostik und die Kommunikation mit dem Arzt verwendet wird, bei der Absicherung der Kommunikation mit dem Arzt selbst, der sicheren Speicherung und ggf. Aggregierung von Patientendaten (je nach Speicherort inkl. Absicherung weiterer Kommunikationskanäle) sowie der Sicherheit des Endgeräts für die Kommunikation beim Arzt. Sofern Daten vom Patienten oder Arzt noch an weitere Dritte weitergegeben werden (z.B. andere Ärzte, Krankenhäuser,

Apotheken, Versicherungen, etc.), ist erneut auf die Absicherung der Kommunikation und der Endgeräte bei diesen Parteien zu achten.

Beim Endgerät auf der Seite des Patienten ist die zentrale Frage, welche Geräte dort zum Einsatz kommen, ob das Gerät (Hardware und Software) als vertrauenswürdig angesehen wird, und wie weit man dort je nach Grad der Vertrauenswürdigkeit der Systeme Sicherheitskonzepte umsetzen kann. Sollten die Geräte konzeptuell und technisch stark durch Hersteller kontrolliert sein (wie z.B. bei vielen Smartphones heute üblich), sodass manche Lösungen nicht rein technisch umsetzbar sind, ist ggf. eine rechtliche Flankierung durch gesetzliche Anforderungen notwendig. Bei der Absicherung der Kommunikationskanäle gibt es diverse Möglichkeiten dies nach dem Stand der Technik umzusetzen. Bei der Speicherung von Daten auf dem Server sowie der Aggregierung und Zusammenführung von Daten etc. gibt es ebenfalls Lösungen, die auf sicheren kryptographischen Algorithmen aufbauen und damit eine sichere Infrastruktur für die Telemedizin darstellen können.

Sollten neuartige Entwicklungen (wie z.B. bei der Einbindung von Gesundheits- oder Fitness-Apps), die über die klassische Diagnose beim Arzt hinausgehen, nun in der Telemedizin umgesetzt werden, kann die Betrachtung im Hinblick auf IT-Sicherheit und Datenschutz anders aussehen. Dies hat in der Regel aber nichts mit der Telemedizin an sich, sondern mit neuartigen Diagnosemethoden zu tun. Werden zum Beispiel Datensätze von einer Vielzahl an Patienten für eine präzisere Diagnostik zentral zusammengeführt, ohne dass eine vollständige Anonymisierung möglich ist, so sind entsprechend neue Sicherheitskonzepte nötig. Dies gilt dann allerdings sowohl bei der Telemedizin, als auch bei der klassischen Anwendung der gleichen Diagnosemöglichkeit beim Arzt vor Ort.

Wir sehen gerade durch Innovationen in der IT-Sicherheit und beim Datenschutz Chancen zur interdisziplinären Zusammenarbeit mit der Medizin und im Ergebnis für Neuentwicklungen und die Fortentwicklung der IT-gestützten Diagnostik. Basierend auf neuen Algorithmen wird es möglich sein, eine präzisere Diagnose zu erreichen, die Privatsphäre von Patienten umfassend zu schützen und gleichzeitig neue Geschäftsmodelle durch datenschutzfreundliche Technologien zu entwickeln.

Im Hinblick auf den Datenschutz ist im Rahmen des Privacy by Design Grundsatzes ein Gesamtkonzept zur Erfüllung der gesetzlichen Anforderungen sowie eine Technikfolgenabschätzung zu erarbeiten. Es ist zu entscheiden, welche Daten erhoben werden müssen, wer die Verfügungsbefugnis über diese Daten inne hat, wo sie gespeichert werden und von wem sie zu welchem Zweck verarbeitet werden dürfen. Zusätzlich ist im Rahmen des Grundrechtsschutzes im Sinne der gesellschaftlichen Teilhabe sicher zu stellen, dass Patienten weder aufgrund ihrer IT-Ausstattung noch aufgrund durch Telemedizin erhobener Daten diskriminiert oder benachteiligt werden.

Autoren:

Dr.-Ing. Sebastian Gerling
Head of Scientific Strategy, CISPA

Ninja Marnau
Senior Researcher, CISPA

Prof. Dr. Christoph Sorge
juris-Stiftungsprofessur für Rechtsinformatik, Universität des Saarlandes