Int. Cybersecur. Law Rev. (2022) 3:247–254
https://doi.org/10.1365/s43439-022-00066-7

EDITORIAL

# Editorial

**Carsten Dochow**

Accepted: 18 September 2022 / Published online: 10 October 2022


## 1 Dear readers,

While healthcare experts in Germany are striving in extensive expert reports to put data protection into perspective and claim to have identified data protection as the—even deadly—cause for the backwardness in terms of digitization of the healthcare sector, the healthcare sector is gradually leading the sad statistics in terms of being the target of cyberattacks. According to a recent analysis of information technology (IT) security data, the risk of becoming the target of a cyberattack is particularly high for healthcare facilities. There have been 90% more attacks in the healthcare sector on a quarterly basis, with an increasing number of ransomware attacks in particular. Healthcare has a particular appeal to attackers for "ransomware" because of its vital services and confidential-sensitive content. The increasing attacks are predominantly due to known vulnerabilities. The "log4j" vulnerability also had an impact in the healthcare sector: for example, some services of the telematics infrastructure had to be disconnected from the Internet as a preventive measure at the end of 2021.

Against this backdrop, if drastic plasticity is required, inadequate precautions for cybersecurity in the healthcare sector are likely to potentially endanger human lives. Prominent in Germany was the case of the University Hospital in Düsseldorf, which became the target of a cyberattack. Although the death of a patient as a result of a transfer, which had become necessary, was not a proven consequence of the IT system failure, the case illustrates the worrying potential of such attacks on healthcare facilities. It is therefore all the more surprising that, when it comes to digitization in the healthcare sector, it is not cybersecurity which is currently under considerable threat that dictates the agenda, but rather pseudo-discussions about data protection.

Carsten Dochow (✉)
Bundesärztekammer, Berlin, Germany

After all, the changes in the wake of the coronavirus pandemic inevitably triggered certain processes toward digitization in the healthcare sector as well. Telemedicine with video telephony was now suddenly possible. After lengthy scientific development, e-health has gradually found its place in practice. However, ad hoc implementation always brings with it the risk of shortcomings. For example, chronic security flaws in e-health products have recently attracted attention: For the "fast-track" DiGAs—i.e., some health apps—the "zerforschung" initiative reported security gaps with "massive data leakage." So, has the speed of digitization recently taken precedence over cybersecurity?

Not at all, because in some cases there have been hasty reactions in the interest of security. For example, security vulnerabilities discovered by experts from the Chaos Computer Club (CCC) using open-source software and red watercolor paint in the video identification process caused the digital agency for the German healthcare system to stop the process, which was used to set up electronic patient records (ePA), altogether. The CCC had, indeed, partially questioned the video-based authentication of physical ID documents. But the flaws concerned a very specific case scenario. The reaction of a complete ban therefore seems excessive to some experts in view of the risk potential. Investigating and correcting the deficiency would have been sufficient. In contrast, it is entirely appropriate to stop using the procedure if it results in major damage. With currently empty electronic patient records, however, the risk of disclosing intimate health data is probably lower anyway.

During the introduction of the e-prescription, the CCC also examined the technology of the telematics infrastructure and claims to have discovered security deficiencies in the e-prescription. For example, inadequate encryption leads to medical health data being stored in plain text and availability requirements for critical infrastructures are not met. In a press release, gematik rejected the criticisms, citing stress tests that had been carried out and practicability requirements. The case shows that a concern with system security is inherent in the discussion about the development of a healthcare data infrastructure.

Nevertheless, sometimes the focus seems shifted: While in Germany the institutions primarily concerned with the security of the telematics infrastructure are still planning digitization and are primarily arguing about the replacement of hardware connectors because, according to controversial opinion, it is not possible to extend security certificates, security gaps in practice software have attracted greater attention. On August 11, 2022, significant defects in Doc Cirrus' "inSuite" practice management system became known. The "zerforschung" initiative had discovered several serious problems with the software, which had to be certified in accordance with the requirements of the German Association of Statutory Health Insurance Physicians ("Kassenärztliche Bundesvereinigung"), among others. This probably affected more than 60,000 patients from more than 270 doctors' surgeries. In this way, it was possible to gain access to e-mail accounts of the registered doctors' surgeries because the internal access data for sending e-mails could be obtained via the central access portal of Doc Cirrus. It was then possible to view e-mail communications between physicians and patients. In addition, due to programming errors in the software, personal data of patients could be accessed. In the process, sensitive

documents such as diagnoses, laboratory findings, blood values or certificates were accessible to third parties in an unsecured manner.

This is no longer a single incident. The "Medatixx" case had already occupied the healthcare sector last year: In November 2021, the IT service provider, which equips many doctors' surgeries with software, was affected by a ransomware attack. The infrastructures and IT systems of the doctors' surgeries were not directly affected. However, the potential for this may have existed and it was also not certain after all whether data had been stolen. Another case of a cyberattack involved "Compugroup Medical" (CGM), the market-leading manufacturer of practice-oriented management systems. This ransomware attack on the company's in-house systems did also not affect the "vast majority" of customers' systems. However, many details about the above-mentioned incidents remain in the dark. Further transparency rules could well be considered here.

By evaluating the introduced incidents, it can be pointed that in such cases the owners of the doctors' surgeries are obviously responsible for the IT security of their management systems; however the manufacturers—even according to statements by the German Federal Commissioner for Data Protection—have no direct obligation to do so instead. With it, cybersecurity in contract relationships is as a result addressed. This goes beyond the design of mere order processing agreements or contracts because not only the security of personal data, but the functionality of the IT systems as a whole may be affected. Cybersecurity is thus generally an important factor when drafting contracts with service providers.

However, healthcare and medical law have not yet comprehensively settled the risks of cyber hazards with regard to recently digitized processes. Specialised literature or judicial decisions specifically directed at cybersecurity law in healthcare are rare. Perhaps, the Flensburg Regional Court in Germany would have profoundly examined the failure to secure organizational precautions with the view to prevent unlawful access to patient data in a radiology program (PACS) and affirmed a claim for damages if the claim had not been time-barred.

Incidentally, the *International Cybersecurity Law Review (ICLR)* can contribute to a greater illumination of cybersecurity law in healthcare. Against this backdrop, I am pleased to present to you, in my role as Editor, the articles in the second *ICLR* issue of 2022:

*Tilmann Dittrich* and *Diana Nadeborn* appoint cybersecurity issues in healthcare. They address cybersecurity in hospitals in a two-part paper. The second part, which appears with this issue, looks at legal obligations and requirements for preventive measures to reduce cyber risks. It also highlights what to do in the event of a cybersecurity "emergency". Because critical infrastructures and thus also hospitals are increasingly becoming the target of ransomware attacks, the reader will gain practical knowledge with regard to the obligations to act.

On the occasion of the aforementioned "Medatixx" case and CMG, but also with a view to Doc Cirrus, *Ole Ziegler* deals in his article with cybersecurity in contract relationships in the healthcare sector. The subject is the need to design IT service contracts with a focus on owners of doctors' surgeries. Therefore, the possibilities of contract design with a view to the concerns of healthcare institutions, which have not yet received in-depth treatment in the literature, are examined in more detail.

Aspects of cybersecurity should be given special attention in contractual drafting. *Ziegler* proposes appropriate clauses for this purpose.

Beyond the health care sector, the other articles in issue 2/2022 of the *ICLR* will hopefully also meet with your interest: *Ben Chester Cheong* looks at avatars in the metaverse and their possible regulations. Furthermore, *Jukka Ruohonen* gives an overview of product safety regulations in the European Union.

*Roberto Carapeto* and *Ana Luíza Calil* take us to Latin America and shed light on cybersecurity in the context of 5G infrastructure tenders. *Sandra Schmitz-Bernd* and *Pier Giorgio Chiara* elucidate on Italian and German cybersecurity regulations in the context of the much-publicized proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (NIS2), which aims to strengthen cybersecurity and resilience in Europe.

Cybersecurity and compliance are closely related. *Roman Dickmann* therefore addresses vulnerability management as a compliance requirement in the Product Safety Regulation. "Cybersecurity reporting" as a way to prevent data breaches at publicly traded U.S. companies is addressed by *Glorin Sebastian*. *Alana Maurushat* and *Kathy Nguyen* elaborate in their article on the obligation of well-timed security patches and automatic updates, and, finally, the trust mechanism for digital intellectual property transactions is the subject of the paper by *Guilisse La Fortune Nkoua Nkuika* and *Xia Yiqun*.

I hope you enjoy reading the highly interesting articles from around the world!

With best wishes,

Dr. jur. Carsten Dochow, Berlin/Germany

## 2 Liebe Leserinnen, liebe Leser,

während sich in Deutschland Sachverständige des Gesundheitswesens in umfangreichen Gutachten um eine Relativierung des Datenschutzes bemühen, in welchem sie die – gar todbringende – Ursache für die Rückständigkeit in Sachen Digitalisierung des Gesundheitswesens ausgemacht haben wollen, führt der Gesundheitssektor nach und nach die traurigen Statistiken in Sachen Angriffsziel von Cyberangriffen an. Einer jüngeren Analyse von IT-Security-Daten zufolge ist das Risiko, Ziel eines Cyberangriffs zu werden, für Einrichtungen im Gesundheitswesen besonders hoch. Es sind im quartalsbezogenen Vergleich 90% mehr Angriffe im Gesundheitswesen und dabei vor allem eine steigende Zahl an Ransomware-Angriffen zu verzeichnen. Das Gesundheitswesen weist wegen der lebenswichtigen Dienste und vertraulich-sensiblen Inhalte für Angreifer eine besondere Attraktivität für „Lösegelder" auf. Die zunehmenden Angriffe sind dabei überwiegend auf bekannte Schwachstellen zurückzuführen. Die „log4j"-Schwachstelle hatte ebenfalls Auswirkungen im Gesundheitssektor: So mussten Ende 2021 einige Dienste der Telematikinfrastruktur präventiv vom Internet abgekoppelt werden.

Bedarf es also drastischer Plastizität, so werden vor diesem Hintergrund wohl eher ungenügende Vorkehrungen für die Cybersicherheit im Gesundheitswesen potenziell Menschenleben gefährden. Prominent war in Deutschland der Fall des Uniklinikums Düsseldorf, das Ziel einer Cyberattacke wurde. Wenngleich der Tod einer Patientin

infolge einer Verlegung nicht nachgewiesene Folge des Ausfalls der IT-Systeme war, so zeigt der Fall das besorgniserregende Potenzial von solchen Angriffen auf Einrichtungen des Gesundheitswesens. Umso überraschender ist es daher, dass in puncto Digitalisierung im Gesundheitswesen nicht etwa die gegenwärtig erheblich bedrohte Cybersicherheit die Agenda diktiert, sondern nebelkerzenartige Diskussionen um den Datenschutz geführt werden.

Die Zeit ist aber nicht stehen geblieben. Immerhin haben die Veränderungen im Zuge der Pandemie mit dem Coronavirus unweigerlich auch im Gesundheitswesen gewisse Prozesse zur Digitalisierung angestoßen. Telemedizin mit Videotelefonie war nun plötzlich möglich. E-Health hat nach längeren fachwissenschaftlichen Gärungsprozessen nach und nach in der Praxis ihren Platz gefunden. Allerdings bringt eine punktuelle Umsetzung im Ad-hoc-Tempo freilich auch immer das Risiko von Mängeln mit sich. So erregen in jüngerer Zeit chronische Sicherheitsmängel bei E-Health-Produkten die Aufmerksamkeit: Für die „Fast-Track"-DiGA – also einige Gesundheitsapps – meldete zum Beispiel die Initiative „zerforschung" Sicherheitslücken mit „massivem Datenabfluss". Genießt neuerdings die Geschwindigkeit bei der Digitalisierung also Vorrang vor der Cybersicherheit?

Mitnichten, denn zum Teil folgen durchaus eilfertige Reaktionen im Interesse der Sicherheit. So veranlassten Sicherheitslücken, die Experten vom Chaos Computer Club mit Open-Source-Software und roter Aquarellfarbe beim Video-Ident-Verfahren aufgedeckt hatten, die Digitalagentur für das deutsche Gesundheitswesen dazu, das Verfahren, das zur Ersteinrichtung elektronischer Patientenakten (ePA) eingesetzt wurde, gleich ganz zu stoppen. Der CCC hatte die videobasierte Echtheitsprüfung physischer ID-Dokumente zwar teilweise infrage gestellt. Die Mängel betrafen aber ein ganz bestimmtes Fallszenario. Die Reaktion der vollständigen Untersagung erscheint einigen Experten in Ansehung des Risikopotenzials daher überzogen. Die Ergründung und Behebung des Mangels hätte genügt. Demgegenüber ist es durchaus sachgemäß, das Verfahren nicht mehr einzusetzen, wenn daraus größere Schäden resultieren. Bei derzeit leeren elektronischen Patientenakten ist das Risiko einer Offenbarung intimster Gesundheitsdaten indes wohl sowieso eher geringer.

Der CCC hatte sich anlässlich der Einführung des E-Rezepts ferner mit der Technik der sog. Telematikinfrastruktur auseinandergesetzt und will beim E-Rezept ebenfalls Sicherheitsmängel entdeckt haben. Beispielsweise sollen durch unzureichende Verschlüsselung medizinische Gesundheitsdaten im Klartext gespeichert sein und Verfügbarkeitsanforderungen für KRITIS nicht erfüllt werden. Die *gematik* wies die Kritikpunkte unter Hinweis auf durchgeführte Stresstests und Praktikabilität in einer Pressemitteilung zurück. Der Fall zeigt, dass der Diskussion um die Entwicklung einer Dateninfrastruktur des Gesundheitswesens eine Befassung mit der Systemsicherheit inhärent ist.

Dennoch scheint manchmal der Fokus verschoben: Während in Deutschland die maßgeblich mit der Sicherheit der Telematikinfrastruktur befassten Institutionen einerseits immer noch die Digitalisierung planen und sich andererseits vornehmlich über den Austausch von Hardware-Konnektoren streiten, weil eine Verlängerung von Sicherheitszertifikaten nach umstrittener Auffassung nicht möglich sei, erregten in der Praxis Sicherheitslücken in Praxissoftware größere Aufmerksamkeit: Am 11.08.2022 sind erhebliche Mängel im Praxisverwaltungssystem „inSuite" von Doc

Cirrus bekannt geworden. Die Initiative „zerforschung“ hatte mehrere gravierende Probleme in der, unter anderem nach Maßgaben der Kassenärztlichen Bundesvereinigung zu zertifizierenden, Software entdeckt. Davon waren wohl mehr als 60.000 Patienten von mehr als 270 Praxen betroffen. Dabei war ein Zugang zu E-Mail-Konten der registrierten Arztpraxen möglich, weil über das zentrale Zugangsportal von Doc Cirrus die internen Zugangsdaten zum Versenden von E-Mails erlangt werden konnten. Es war dann möglich, die E-Mail-Kommunikation zwischen den Ärzten und Patienten einzusehen. Zudem konnten aufgrund der Programmierfehler in der Software persönliche Daten von Patienten abgegriffen werden. Dabei waren sensible Dokumente wie Diagnosen, Laborbefunde, Blutwerte oder Atteste für Dritte ungesichert zugänglich.

Das ist längst kein Einzelereignis mehr. Schon im letzten Jahr hat der Fall „medatixx“ das Gesundheitswesen beschäftigt: Im November 2021 war der IT-Dienstleister, der viele Arztpraxen mit Software ausstattet, von einer Ransomware-Attacke betroffen. Zwar waren die Infrastrukturen oder IT-Systeme der Praxen nicht direkt tangiert. Allerdings dürfte das Potenzial hierzu bestanden haben und es war auch nicht sicher, ob beim Dienstleister gespeicherte Daten entwendet worden sind. Ein weiterer Fall eines Cyberangriffs betraf „Compugroup Medical“ (CGM), den marktführenden Hersteller für Praxisverwaltungssysteme. Auch dieser Ransomware-Angriff auf die firmeninternen Systeme soll wohl die „überwiegende Mehrheit“ der Systeme der Kunden nicht betroffen haben. Viele Einzelheiten zu den Vorfällen blieben aber im Dunkeln. Hier könnte durchaus über weitere Transparenzregeln nachgedacht werden.

Interessant an den Vorfällen ist aber auch, dass die Praxisinhaber für die IT-Sicherheit der bei ihnen eingesetzten Praxisverwaltungssysteme verantwortlich sind und die Hersteller – auch nach Aussagen des Bundesbeauftragten für den Datenschutz – hierfür keine direkte Verpflichtung trifft. Damit ist die Cybersicherheit in Auftragsverhältnissen angesprochen. Das geht über die Gestaltung von bloßen Auftragsverarbeitungsvereinbarungen hinaus, weil nicht nur die Sicherheit von personenbezogenen Daten, sondern die Funktionsfähigkeit der IT-Systeme insgesamt betroffen sein kann. Cybersicherheit ist damit generell ein wichtiger Faktor bei der Vertragsgestaltung mit Dienstleistern.

Das Gesundheits- und Medizinrecht hat sich mit den Risiken der Cybergefahren für die neuerdings digitalisierten Prozesse aber noch nicht umfassend auseinandergesetzt. Das speziell auf das Cybersicherheitsrecht im Gesundheitswesen gerichtete Schrifttum und gerichtliche Entscheidungen sind rar. Vielleicht hätte das LG Flensburg das Unterlassen organisatorischer Vorkehrungen zur Vermeidung unrechtmäßiger Zugriffe auf Patientendaten in einem Radiologieprogramm (PACS) geprüft und einen Schadensersatzanspruch bejaht, wenn der Anspruch nicht verjährt gewesen wäre.

Im Übrigen kann die Zeitschrift *International Cybersecurity Law Review (ICLR)* zu einer stärkeren Beleuchtung des Cybersicherheitsrechts im Gesundheitswesen beitragen. Ich freue mich vor diesem Hintergrund, Ihnen in meiner Rolle als Mitherausgeber im Rahmen dieser zweiten Ausgabe der ICLR für das Jahr 2022 die Beiträge vorstellen zu dürfen:

Zu einer weiteren Akzentuierung von Cybersicherheitsthemen im Gesundheitsbereich tragen *Tilmann Dittrich* und *Diana Nadeborn* bei. Sie befassen sich in einem zweiteiligen Beitrag mit der Cybersicherheit in Krankenhäusern. In dem mit dieser Ausgabe erscheinenden zweiten Teil werden zum einen Rechtspflichten und Anforderungen für präventive Maßnahmen zur Verringerung von Cyberrisiken betrachtet. Zum anderen wird beleuchtet, was im Cybersicherheits-„Notfall" zu tun ist. Weil kritische Infrastrukturen und damit auch Krankenhäuser vermehrt Ziel von Ransomware-Attacken werden, verspricht die Lektüre praktischen Nutzen mit Blick auf die Handlungspflichten.

Anlässlich der erwähnten Fälle „medatixx" und CMG, aber auch mit Blick auf Doc Cirrus befasst sich *Dr. Ole Ziegler* in dieser Ausgabe mit der Cybersicherheit in Auftragsverhältnissen im Gesundheitswesen. Gegenstand ist der Gestaltungsbedarf für IT-Dienstleistungsverträge mit Fokus auf Arztpraxisinhaber. Näher beleuchtet werden daher die Möglichkeiten der Vertragsgestaltung mit Blick auf Belange von Einrichtungen des Gesundheitswesens, die bisher noch keine vertiefte Behandlung im Schrifttum erfahren haben. Aspekten der Cybersicherheit sollte bei der vertraglichen Gestaltung besondere Aufmerksamkeit geschenkt werden. *Ziegler* bietet dafür konkrete Klauselvorschläge an.

Jenseits des Gesundheitswesens treffen hoffentlich nicht minder die weiteren Beiträge in der Ausgabe 2/2022 der *ICLR* auf Ihr Interesse: So befasst sich *Ben Chester Cheong* mit Avataren im Metaversum und möglichen Regulierungen. Einen Überblick über die Produktsicherheitsvorschriften in der Europäischen Union gibt überdies *Jukka Ruohonen.*

*Roberto Carapeto* und *Ana Luíza Calil* entführen uns nach Lateinamerika und beleuchten „cyber security" im Zusammenhang mit Ausschreibungen für die 5G-Infrastruktur. *Sandra Schmitz-Bernd* und *Pier Giorgio Chiara* betrachten im Kontext der vielbeachteten NIS2-Richtlinie, die zu einer Stärkung der Cybersicherheit und Resilienz in Europa führen soll, in einer Gegenüberstellung die italienischen und deutschen Cybersicherheitsregelungen.

Cybersicherheit und Compliance stehen in einem engen Zusammenhang. *Roman Dickmann* befasst sich daher mit dem Schwachstellenmanagement als Compliance-Anforderung in der Produktsicherheitsverordnung. Die „Cybersicherheitsberichterstattung" als Möglichkeit, Datenschutzverletzungen bei börsennotierten US-Unternehmen zu verhindern, behandelt *Glorin Sebastian*. Zur Verpflichtung zu rechtzeitigen Sicherheitspatches und automatischen Updates führen *Alana Maurushat* und *Kathy Nguyen* in ihrem Beitrag aus, und um den Vertrauensmechanismus für Transaktionen mit digitalem geistigem Eigentum dreht sich der Aufsatz von *Guilisse La Fortune Nkoua Nkuika* und *Xia Yiqun*.

Bei der Lektüre der hoch interessanten Beiträge aus aller Welt wünsche ich viel Vergnügen!

Mit den besten Wünschen
Dr. jur. Carsten Dochow, Berlin

**Carsten Dochow**