Datenschutzkonzepte für eine elektronische Patientenakte im Klinischen Krebsregister Schleswig-Holstein (KKR-SH)

C. Krauss (1), A. Höpken (2), P. Boll (3), B. Kremer (1)
(1) Klinisches Krebsregister Schleswig-Holstein e. V., Kiel
(2) Externer Datenschutzbeauftragter, KKR-SH e. V., Kiel
(3) Universitätsklinikum Schleswig-Holstein, Campus Kiel

Einleitung

Eine besondere Bedeutung im Aufbau eines flächendeckenden Klinischen Krebsregisters in Schleswig-Holstein kommt der datenschutzkonformen Ausgestaltung des Verfahrens zu. Einerseits müssen die Patientendaten nach dem neuesten Stand der Technik vor Angriffen und Missbrauch jeglicher Art geschützt werden, andererseits sollen die Behandlungsdaten in der Datenbank den Ärzten und Kliniken im Behandlungszusammenhang als onkologische Patientenakte online zur Verfügung stehen. Dabei müssen, je nach Rechtsform der beteiligten Einrichtungen, gesetzliche Regelungen wie z.B. das Landesdatenschutzgesetz oder das Bundesdatenschutzgesetz neben weiteren spezifischen Gesetzen beachtet werden.

Material und Methoden

Zweck des KKR-SH ist es, die klinische Krebsregistrierung des Landes Schleswig-Holstein aufzubauen und weiterzuentwickeln. Unter klinischer Krebsregistrierung ist die Erfassung der klinischen Befunde und der Verlaufsdaten der in Schleswig-Holstein behandelnden Krebspatientinnen und -patienten und die Auswertung der erhobenen Daten zum Zwecke der Qualitätssicherung der onkologischen Versorgung zu verstehen.

Wichtige Regelungen sind bei der Einführung und dem Betrieb des Verfahrens zu beachten wie z. B. die Ärztliche Berufsordnung (insbesondere § 9 Schweigepflicht und § 10 Abs. 5 Sicherheit von ärztlicher Dokumentation auf Datenträgern), das Strafgesetzbuch (insbesondere § 203 „Verletzung von Privatgeheimnissen“, § 202 a „Ausspähen von Daten“, § 202 b „Abfangen von Daten“, § 202 c „Vorbereitung des Ausspähens und Abfangens von Daten“) oder auch das Bundesdatenschutzgesetz. Aufgrund der Rechtsform des KKR-SH, gilt für diesen Verein insbesondere das Bundesdatenschutzgesetz (BDSG) und nicht das Landesdatenschutzgesetz Schleswig-Holstein. Um den Betrieb einer solchen Online-Datenbank datenschutzkonform und rechtssicher zu betreiben, wurden folgende Punkte bearbeitet und detailliert mit der Datenschutzaufsichtsbehörde (ULD) abgestimmt:

Punkt 1: Rechtssichere Speicherung der Daten durch Einwilligungserklärung der Patienten

Für die Eingabe der Klinischen Krebsregisterdokumentation wird eine Einwilligungserklärung vom Patienten eingeholt. Diese wurde mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) und dem Ministerium für Soziales, Gesundheit, Familie und Gleichstellung (MSGFG) abgestimmt. Die jeweilige Institution/Klinik hat das Vorliegen einer wirksamen Einverständniserklärung vor Eingabe in der Online-Datenbank zu dokumentieren.

Punkt 2: Vertragliche Regelung zwischen Melder (Krankenhaus / Arzt) und Verein

Die medizinisch tätigen Mitglieder verpflichten sich, die zur Verfügung gestellte Online-Datenbank ordnungsgemäß, mit äußerster Sorgfalt und entsprechend den Vorgaben des

Vereins zu nutzen und sicherzustellen Die Pflichten und Rechte sowie die Verwendung der im Klinischen Krebsregister gespeicherten Daten sind über einen Vertrag zwischen dem Verein und den Mitgliedern geregelt.

Punkt 3: Sicherheitsmaßnahmen der Online-Datenbank

Aufgrund des Online-Zugriffs auf die Daten müssen besondere Sicherheitsmaßnahmen für das Hosting und den Betrieb der Datenbank vorgesehen werden. Hierfür wurden zwei Server eingerichtet, welche den Online-Zugriff regeln: Der erste Server ist ein Token Management Server (TMS) für die sichere Anmeldung durch Zweifaktorauthentisierung. Nach erfolgreicher Anmeldung mit dem OTP-Token und Passwort wird eine verschlüsselte Verbindung (per Reverse Proxy) zu dem zweiten Server, dem Applikations-Web-Server aufgebaut.

Auch innerhalb der Online-Datenbank wurde für eine ausreichende Sicherheit gesorgt: Grundsätzlich orientiert sich die Online-Datenbank an den Vorgaben von „Sicherheit von Webanwendungen. Maßnahmenkatalog und Best Practices“ des Bundesamtes für Sicherheit in der Informationstechnik[1] sowie an „GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems“ [2]. Datenfelder in der Online-Datenbank sind per AES 256Bit verschlüsselt und können nur von der Applikation gelesen werden. Auch die Backups der Datenbank werden verschlüsselt gespeichert. Über das interne Audit Trail sind alle Änderungen in der Datenbank nachvollziehbar. Die strikte Mandantentrennung stellt sicher, dass nur befugte Personen die entsprechenden Daten einsehen und ggf. bearbeiten dürfen.

Ergebnisse

Das Verfahren der Bereitstellung einer Online-Dokumention ist zwar aufwendig, jedoch die Akzeptanz ist bei den dokumentierenden Stellen trotzdem sehr hoch. Die Benutzer schätzen die ständige Verfügbarkeit der Eingabemasken sowie der onkologischen Patientenakte. Im Ergebnis konnte eine datenschutzkonforme Lösung mit hoher Akzeptanz bei den Nutzern gefunden und etabliert werden.

Diskussion

Das vorliegende Verfahren zeigt einen Weg, wie klinische Krebsregistrierung und der Zugriff auf eine gemeinsame onkologische Patientenakte über neue Online-Technologien datenschutzkonform funktionieren können. Das Management des Online-Zugriffs über die OTP-Zugriffstoken und der Mandantentrennung ist zwar aufwendig, aber dennoch gut geeignet für die Dokumentation im Klinischen Krebsregister im Bereich der Krankenhäuser und großen Schwerpunktpraxen.

Literatur

[1] https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/websec/index_htm.html
[2] http://www.ispe.org/gamp-5

Dr. Christian Krauss
Klinisches Krebsregister Schleswig-Holstein e.V.
Holtenauer Str. 94
24105 Kiel

Tel.: 0431/260 92 260, E-Mail: christian.krauss@kkr-sh.de