Schutz von SHV-relevanten Daten unter der Lupe

Der Schweizerische Hebammenverband hat seine internen Prozesse analysiert und wo nötig der künftig in Kraft tretenden Revision des Schweizerischen Bundesgesetzes über den Datenschutz angepasst. Wie schützt die Zürcher Hochschule für Angewandte Wissenschaften die Daten bei der Auswertung der Statistik der frei praktizierenden Hebammen? Und wie verfahren die Anbieter der Softwares MoonCare und Artemis Hebamme?

TEXT:
ANDREA WEBER-KÄSER,
SUSANNE GRYLKA,
JEAN-MARC FILLISTORF,
THOMAS A. KAUFMANN

Unter dem Aspekt der neuen europäischen Datenschutz-Grundverordnung und der zu erwartenden Revision des Schweizerischen Bundesgesetzes über den Datenschutz hat der Schweizerische Hebammenverband (SHV) seine internen Prozesse, die in Bezug zum Datenschutz stehen, analysiert und – wo nötig – angepasst und verbessert.

iStockphoto 638236868, blossomstar

Wieso informiert der SHV über dieses Thema?

Einerseits trat die Europäische Datenschutz-Grundverordnung, die einen Quantensprung im Datenschutz darstellt, am 25. Mai 2018 in Kraft, und andererseits haben wir die verbandseigene Website komplett überarbeitet, womit der Datenschutz automatisch zum Thema wird. In Anbetracht der zu erwartenden Revision des Schweizerischen Datenschutzgesetzes wollten wir diesbezüglich auf dem neusten Stand sein und darüber berichten.

Was brachte die erwähnte Analyse der internen Prozesse zutage?

Grundsätzlich ist es unabdingbar, dass man sich von einer Fachperson, die auf dem Gebiet des Datenschutzes spezialisiert ist, beraten lässt. Die Analyse zeigte, dass wir einzelne Abläufe optimieren mussten, was wir getan haben. So ist das Team der Geschäftsstelle seit Neuestem in Besitz einer E-Mail-Adresse, die einen verschlüsselten E-Mail-Verkehr zulässt. Das ist aus der Sicht des Verbandes z. B. insbesondere für das Beantworten und datenschutzkonforme Weiterleiten von schriftlich eingesandten Beschwerden von Klientinnen an die Sektionspräsidentinnen und andererseits für das vertraglich geregelte Versenden von Daten von Mitgliedern an die verschiedenen Branchenverbände der Krankenkassen nötig. Weiter war es wichtig, eine Datenschutzerklärung zu erstellen, die alle verbandsinternen Themen zum Datenschutz aufzeigt, damit sich jedes Mitglied informieren kann, welche Daten mit welchen Analysetools und zu welchem Verarbeitungsweck registriert, gesammelt und ausgewertet werden. Diese Erklärung muss zudem aufzeigen, wer innerhalb des Verbandes für den Datenschutz zuständig ist und wo man sich melden kann, wenn man seine Rechte in Bezug auf den Datenschutz ausüben möchte, z. B. Recht auf Auskunft, Recht auf Einschränkung der Verarbeitung.

Welches waren die Stolpersteine bei der Optimierung der internen Prozesse?

Der Teufel steckt – wie meistens – im Detail. Einerseits mussten wir uns ein enormes Wissen aneignen. Andererseits mussten wir jahrelang bestehende Abläufe bzgl. Datenschutzkonformität untersuchen und falls nötig anpassen, was sowohl zeitintensiv (mehrere Personen involviert) und/oder technisch aufwendig war. So darf z. B. ein Newsletter nur als Newsletter bezeichnet werden, wenn vorab informiert wird, dass man ihn als Mitglied erhält und jederzeit selber abbestellen kann. Um diesen Anforderungen gerecht zu werden, haben wir nun ein neues Newslettertool programmieren lassen, das im Dezember in die neue Website implementiert werden wird. Somit wurde die Möglichkeit zur Abbestellung umgesetzt. Ein weiterer Knackpunkt ist die «Weitergabe von Daten an Dritte». Dies musste genau geprüft und die nötigen Schweigepflichtserklärungen mussten erneuert werden.

Als kleiner Verband mit knappen Ressourcen müssen wir in der Thematik Datenschutz Schwerpunkte setzen. Das haben wir gemacht. Wir legten den Fokus auf die Erstellung der Datenschutzerklärung, die alle relevanten Punkte aufzeigt und jedem Mitglied Klarheit bringen soll, sowie auf die Möglichkeit des verschlüsselten E-Mail-Verkehrs. ⊙

«So ist das Team der Geschäftsstelle seit Neuestem in Besitz einer E-Mail-Adresse, die einen verschlüsselten E-Mail-Verkehr zulässt.»

AUTORIN

Andrea Weber-Käser,
Geschäftsführerin Schweizerischer Hebammenverband.

Quellen

Der Bundesrat (1992) Schweizerisches Bundesgesetz über den Datenschutz. www.admin.ch

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (2018) Datenschutz Grundverordnung der Europäischen Union. www.edoeb.admin.ch

Grüter, U. (2018) Folgen der EU-Datenschutzverordnung für Verbände. «Fachzeitschrift für Verbands- und Nonprofit-Management», 2/2018, 50ff.

Datenablage bei der Zürcher Hochschule für Angewandte Wissenschaften

Die Auswertung der Statistik der frei praktizierenden Hebammen wird von der Forschungsstelle Hebammenwissenschaft der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) durchgeführt. Die Daten werden deshalb von den Softwareanbietern der ZHAW übermittelt, dort bereinigt, ausgewertet und auf dem Server der Hochschule archiviert.

Wo befindet sich der Server der ZHAW?

Die ZHAW betreibt ein eigenes Rechenzentrum, das in der Schweiz liegt.

Wo werden die regelmässig durchgeführten Backups von Daten und Dokumenten gespeichert?

Die Backups werden ebenfalls im Rechenzentrum der ZHAW gespeichert. Die Administratoren des Rechenzentrums können Daten wiederherstellen, haben jedoch keine Einsicht in Ordner und Dateien, die verschlüsselt sind.

Werden die Daten auf dem ZHAW-Server geschützt aufbewahrt und wer hat Zugang zu den Daten?

Die Daten werden angemessen geschützt und gesichert aufbewahrt. Der Zugriff auf die Daten ist ferner wie folgt beschränkt: Die Projektleiterin der Statistik der frei praktizierenden Hebammen sowie die Leiterin der Forschungsstelle Hebammenwissenschaft haben Administratorenrechte, um die Zugriffe auf den gesicherten Ordner zu regeln. Die Zugangsrechte sind beschränkt auf die beiden Administratoren des Ordners sowie auf eine wissenschaftliche Mitarbeiterin, die im Projekt mitwirkt. Die weiteren Mitarbeiter/innen der ZHAW haben weder Zugang zu den Daten noch zu den Analysecodes.

Sind sensible Daten, die der ZHAW übermittelt werden, geschützt?

Ja, die ZHAW verwendet angemessene Schutzmassnahmen (inkl. Anonymisierung), um den datenschutzrechtlichen Anforderungen gerecht zu werden. Die Statistik beinhaltet keine Namen von Müttern, sondern deren AHV-Nummern. Diese sind zufällig generierte Nummern, aus denen keine Rückschlüsse auf die dahinterstehenden Personen gezogen werden können (telefonische Auskunft des Sozialversicherungsamtes, SVA, Zürich, vom 20. September 2018). Einzig das SVA besitzt Kenntnisse darüber, welche Nummer welcher Person zugeordnet werden kann. Die Angestellten der ZHAW haben keine Möglichkeit, AHV-Nummern und Personen zu verlinken. Auf Wunsch von Hebammen und einzelnen Softwareanbietern werden die AHV-Nummern zudem verschlüsselt. Damit wird eine zusätzliche Sicherheit eingebaut, damit Mütter nicht identifiziert werden können.

Werden im Rahmen der Statistik der frei praktizierenden Hebammen der Datenschutz und ethische Grundsätze beachtet?

Ja, die gegebenen und anwendbaren datenschutzrechtlichen Anforderungen werden beachtet, da die Daten anonymisiert übermittelt, ausgewertet und verschriftlicht sowie sicher aufbewahrt werden. Die Forschungsstelle Hebammenwissenschaft der ZHAW wird demnächst bei der Ethikkommission des Kantons Zürich eine Zuständigkeitsabklärung beantragen. Diese wird beurteilen, ob die Statistik der frei praktizierenden Hebammen in den Geltungsbereich des Humanforschungsgesetz fällt, und falls dies der Fall wäre, ob die Vorgaben des Gesetzes eingehalten werden. Eine Nichtzuständigkeit der Ethikkommission oder eine Ethikbewilligung wird die Unbedenklichkeit der Statistik bestätigen.

Leitet die ZHAW Daten an Dritte weiter?

Nein, die Daten gehören dem SHV, und die ZHAW ist nicht berechtigt, Daten an Dritte weiterzuleiten. Einzig der SHV ist dazu befugt. ⊙

«Die Administratoren des Rechenzentrums können Daten wiederherstellen, haben jedoch keine Einsicht in Ordner und Dateien, die verschlüsselt sind.»

AUTORIN

Susanne Grylka,
stellvertretende Leiterin und Dozentin an der Forschungsstelle Hebammenwissenschaft, Institut für Hebammen, Zürcher Hochschule für Angewandte Wissenschaften, Winterthur.

Sicherheit der Software MoonCare

Die Sicherheit ist ein fundamentales Anliegen von Gammadia AG, denn die Anwendungen, die wir entwickeln, enthalten heikle Daten. Die Sicherheit umfasst mehrere Aspekte, die wir ständig weiterbearbeiten.

Sind meine Daten in MoonCare sicher?

MoonCare basiert auf einer SaaS-Web-Plattform («Software as a Service»), auf der die Kundendaten mittels Kontrollen auf allen Ebenen – von der Hardware bis zu den Applikationen – geschützt sind. Die physische Infrastruktur von MoonCare befindet sich ausschliesslich in der Schweiz und wird von einem der wichtigsten Hosting Provider fernverwaltet, mit Backups an zwei getrennten Standorten. Die Kommunikation zwischen den Nutzerinnen von MoonCare und unseren Servern ist verschlüsselt und basiert auf einer starken Authentifizierung (256-bit «Secure Socket Layer», SSL), die mit der Note A bewertet ist (die Qualität der Verschlüsselung kann online getestet werden, bspw. auf SSL Labs). Alle unsere Systeme werden permanent aktualisiert (Sicherheits-Patches), um jegliche Risiken eines externen Angriffes zu vermeiden.

Die einzige Verantwortung der Hebamme: die regelmässige Aktualisierung des Betriebssystems und des Browers ihres Computers/Tablets/Smartphones.

Ist mein Passwort sicher?

Die Passwörter unserer Nutzerinnen sind fragmentiert und werden nie im Textformat gespeichert. Die Zugänge zu den Daten sind durch einen Kontrollmechanismus geschützt. Dieser verbietet einer Nutzerin den Zugang zu Daten, die ihr nicht gehören.

Die einzige Verantwortung der Hebamme: Wahl eines genügend langen Passworts (bspw. eines Satzes) und dessen Speicherung. Es sollte nirgends aufgeschrieben werden.

Muss ich Datenverluste befürchten?

Alle MoonCare-Daten werden jede Stunde vollständig neu gesichert. Das geschieht automatisch, ohne Mitwirkung der Nutzerinnen. Die Backups sind an zwei getrennten Standorten gespeichert. Alle Daten werden, wie gesetzlich vorgeschrieben, mindestens sechs Jahre lang gespeichert. Falls eine Hebamme dies wünscht, kann sie eine PDF-Kopie des Dossiers auf der Festplatte ihres Computers speichern.

Kann ich jederzeit auf MoonCare zugreifen?

Es ist wichtig, dass die Hebammen jederzeit und ohne Unterbruch oder Datenverlust auf MoonCare zugreifen können. Zur optimalen Bekämpfung möglicher Schwachstellen investieren wir die notwendigen Mittel, damit jedes Element unserer Infrastruktur verdoppelt werden kann:

- Unsere Rechenzentren verfügen über mehrere Internetverbindungen und mehrere elektrische Anschlüsse.
- Die Produktivdaten werden simultan auf mehreren Servern an getrennten Standorten gespeichert.
- Ausserdem werden die Backups auf einer zusätzlichen externen Site gespeichert.

Die Nutzerinnen werden über E-Mail rechtzeitig informiert, wenn aus Gründen des Unterhalts Unterbrüche nötig sind. Bei einem unvorhergesehenen Unterbruch wird unverzüglich unser 24-Stunden-Pikettdienst benachrichtigt, der an 365 Tagen pro Jahr tagsüber und nachts sofort reagieren kann. So bleiben die Daten jederzeit verfügbar.

Die einzige Verantwortung der Hebamme: Sie muss über eine normal funktionierende Internetverbindung verfügen.

Wie kann ich sicher sein, dass nur ich Zugang zu meinen Daten habe?

Der Aufbau von MoonCare gewährleistet die totale Abschirmung jedes einzelnen Nutzerinnenkontos. Alle Aktionen auf der Datenbank werden gesichert und kontrolliert, damit ausschliesslich jene Hebamme die Daten lesen oder eintragen kann, die Zugang zu diesem Dossier hat. Zusätzlich hat nur die Applikation MoonCare Zugang zu diesen Daten.

Alle Angestellten von Gammadia AG unterstehen vertraglich dem Berufsgeheimnis. Es haben lediglich jene Zugang zur Produktionsinfrastruktur, die eine entsprechende Bewilligung haben, wobei die Zugänge klar identifiziert sind. Der Zugang zu den Daten unserer Nutzerinnen erfolgt nur bei Bedarf und stets im Einvernehmen mit der Nutzerin (z. B. für den Support oder den Unterhalt). Der Zugang zu den geteilten Dossiers ist auf die Nutzerinnen beschränkt, die eine Einladung für dieses spezifische Dossier haben.

Die einzige Verantwortung der Hebamme: Bevor sie ein Dossier teilt, muss sie die Mutter um eine Bewilligung ersuchen (über das Dokument, das im Tab «Dokumente» von MoonCare verfügbar ist).

Welche Informationen werden statistisch ausgewertet?

Nur die in MoonCare klar gekennzeichneten Bereiche werden statistisch ausgewertet. Die an den Statistikdienst weitergeleiteten Daten sind anonymisiert. Ab 2019 wird die AHV-Nummer ebenfalls verschlüsselt, sodass es definitiv nicht mehr möglich sein wird, die Mutter zu identifizieren.

Die einzige Verantwortung der Hebamme: Sie muss bei der elektronischen Rechnungsstellung entscheiden, ob sie den Versicherungen gewisse heikle Daten schicken soll oder nicht (bspw. bei Schwangerschaftskontrollen im Falle eines Risikos oder beim Fetalmonitoring).

Dank unserer Bemühungen auf diesen verschiedenen Gebieten der Sicherheitskontrolle können wir mit Stolz sagen, dass

- wir nie irgendwelche Daten verloren haben,
- keine Person ohne Autorisierung je Zugang zu heiklen Daten hatte,
- wir eine speziell hohe Verfügbarkeitsrate bieten (>99,9 %). ⊙

AUTOR

Jean-Marc Fillistorf,
Generaldirektor, Gammadia AG.
www.gammadia.ch

Sicherheit bei der Software Artemis Hebamme

Die Software Artemis Hebamme (eInvoice) ist ein effektives und einfach bedienbares Statistik- und Abrechnungstool. Einer seiner zahlreichen Vorteile bildet die Datensicherheit. Im Unterschied zu ähnlichen Lösungen, die Cloud-basierte Systeme einsetzen, geht es bei Artemis um eine App, die ausschliesslich lokale Daten verwendet und den höchsten Wert auf die Datensicherheit legt. Sämtliche Datenoperationen – Dateneingabe, -speicherung, -bearbeitung und -übertragung – werden in der App mittels eines mehrstufigen Verfahrens geschützt. Auch die Datenlöschung in der App findet datenschutzgesetzkonform statt, indem nach dem Ablauf der gesetzlichen Aufbewahrungspflicht das System eine automatische Anonymisierungsfunktion bietet, mit der die Patientendaten entkoppelt bzw. gelöscht werden.

Daten nur über verschlüsselte Verbindungen übertragen

Das Einloggen ins System wird ab Mitte 2019 zusätzlich zum Passwort über eine Handy-App mit einer 2-Faktor-Authentifizierung abgesichert. Da es bei Patientendaten um besonders sensible Daten geht, werden diese ausschliesslich auf dem persönlichen PC bzw. im persönlichen Onlinebackup – einem sicheren webbasierten Datenspeicher – gespeichert. Aus Sicherheitsgründen wird eine Einspielung (Restore) auf einem anderen Gerät durch den Support bereitgestellt.

Die gesamte Datenübertragung findet lediglich über verschlüsselte Verbindungen statt. Ausserdem sind sämtliche Daten mit einer Punkt-zu-Punkt-Verschlüsselung gesichert und von Daten bzw. Anwendungen anderer Kundinnen isoliert. Dies geschieht zum einen physisch bei der Appinstallation, zum anderen über die Datenablegung in persönlichen Konten und die Datenverwaltung in unterschiedlichen Datenspeichern.

Da sich die gesamte Serverinfrastruktur der App in der Schweiz befindet, erfolgt die Datenverwaltung bei der kaSoft GmbH gemäss den entsprechenden gesetzlichen Grundlagen. Sämtliche Datenschutzdokumente sind im Serviceportal der App zu finden.

Externe Experten überwachen die Datensicherheit

Alle beteiligten Mitarbeiter der kaSoft GmbH sind als Hilfspersonen der Hebamme bzw. der Hebammenpraxis definiert und unterstehen demgemäss der ärztlichen Schweigepflicht. Den Zugriff auf die Server haben ausschliesslich speziell ausgebildete Mitarbeiter der kaSoft GmbH, die eine zusätzliche Geheimhaltungsvereinbarung unterzeichnet haben. Zusätzlich sollen diese zertifizierten Mitarbeiter jährlich an einer Sicherheitsweiterbildung teilnehmen.

«Die Software Artemis bietet sowohl den Hebammen als auch ihren Kundinnen die Möglichkeit an, eine Liste von Personen mit dem Datenzugriff anzufordern.»

Die Software Artemis bietet sowohl den Hebammen als auch ihren Kundinnen die Möglichkeit an, eine Liste von Personen mit dem Datenzugriff anzufordern. Auf solche Weise kann die Datensicherheit seitens der Appnutzerinnen kontrolliert werden.

Die Überwachung der Systeme seitens der kaSoft GmbH als Anbieter findet in regelmässigen Abständen mit dem Einbezug von externen Experten statt. Relevante Prüfberichte werden ausschliesslich nach der Behebung von entdeckten Fehlern bzw. Schwachstellen veröffentlicht. Bei kritischen Vorfällen werden die Appnutzerinnen sofort per E-Mail informiert. Ein solches mehrstufiges Datensicherungsverfahren schützt die Privatsphäre der Kundinnen und garantiert die Wahrung des Berufsgeheimnisses der Appnutzerinnen.

Bei allen Fragen steht die kaSoft GmbH als zuständiger Ansprechpartner gerne zur Verfügung. ⊙

AUTOR

Thomas A. Kaufmann,
Inhaber und Systementwickler kaSoft GmbH.
www.kasoft.ch