

**Stellungnahme zur Anhörung des Ausschusses für Familie, Kinder und Jugend
zum Thema „Kinderschutz stärken - Interkollegialer Austausch von Kinderärzten
bei Verdacht auf Kindesmisshandlung ermöglichen“**

LANDTAG
NORDRHEIN-WESTFALEN
16. WAHLPERIODE

**STELLUNGNAHME
16/1082**

A04, A01

Das Dokument wurde erstellt von:

ISDSG – Institut für Sicherheit und Datenschutz im Gesundheitswesen

Westfalendamm 251 - 44141 Dortmund

Tel: 0231 4499599-91 | Fax: 0231 4499599-99

kontakt@isdsg.de | <https://www.isdsg.de>

Fingerprint: A554 551A D5F1 BEBB C552 A062 751F CD07 5A78 F82F

Ansprechpartner: Herr Magnus Welz (welz@isdsg.de)

Sofern möglich, haben sich die Autoren bemüht eine geschlechtergerechte Formulierung zu finden. Jedoch kann in diesem Dokument aus Gründen der besseren Lesbarkeit auch das generische Maskulinum verwandt worden sein, womit ausdrücklich Frauen und Männer gemeint sind.

Die in dieser Unterlage verwendeten Marken- und Handelsnamen oder Warenbezeichnungen sind, soweit nicht ausdrücklich anders angegeben, Eigentum bzw. eingetragene Markenzeichen des jeweiligen Herstellerunternehmens. Von der Nennung in diesem Dokument kann nicht auf eine grundsätzlich freie Nutzung geschlossen werden.

Version	Datum	Autor	Änderungsgrund/Bemerkungen
1.0	2013-09-20	Prof. Dr. Thomas Jäschke, Simon Hacks, Magnus Welz	Initiale Erstellung

Inhaltsverzeichnis

1	Ausgangslage.....	3
2	Beantwortung des Fragenkatalogs.....	4
2.1	Allgemeines.....	4
2.2	Frage 1.....	4
2.3	Frage 4.....	4
2.4	Frage 5.....	5
2.5	Frage 7.....	6
2.6	Frage 9.....	6
3	Stellungnahme.....	7

1 Ausgangslage

Betrachtungsgrundlage ist die Annahme, dass das Bundesland NRW die Einführung einer Softwarelösung plant, die dabei helfen soll den Austausch bei Verdacht auf Kindeswohlgefährdung bzw. -misshandlungen zwischen Kinderärzten zu vereinfachen. Bei Opfern von Kindesmisshandlungen müssen drei Gruppen von betroffenen Kindern unterschieden werden.

Zum einen gibt es Kinder, bei denen die Misshandlung zweifelsfrei diagnostizierbar ist und den Kinderärzten so der Weg zum Jugendamt oder anderen staatlichen Institutionen offen steht. In der zweiten Gruppe erfolgt die Misshandlung so subtil, dass sie unterhalb der Schwelle der Erkennung durch einen Arzt liegt. Für diese beiden Gruppen von Kindern bietet das geplante System keinen Schutz. Vielmehr soll für die Gruppen von Kindern, bei denen die behandelnden Ärzte sich nicht sicher sein können, ob die vorliegenden Symptome bei einem Kind „natürlichen“ Ursprungs sind oder durch eine Kindesmisshandlung zugefügt wurden, eine Lösung entwickelt werden. Insbesondere in den Fällen von Vernachlässigung oder aktiver Misshandlung erfolgt durch die Erziehungsberechtigten häufig ein regelmäßiger Arztwechsel, so dass der jeweils behandelnde Mediziner immer nur den akuten Ausschnitt der Behandlungshistorie sieht und keinen kompletten Überblick hat. Bedingt durch diesen eingeschränkten Fokus besteht möglicherweise der Verdacht auf eine Kindeswohlgefährdung, diese kann aber nicht definitiv festgestellt werden. Die zur Verifizierung oder Falsifizierung der Diagnose notwendigen Informationen liegen unter Umständen bei einem unbekanntem, ebenfalls das Kind mitbehandelnden Arzt vor. Die Lösung soll das Auffinden dieses Arztes unterstützen. Es soll mit dem System keine Zweitmeinung eines unbeteiligten Arztes eingeholt werden, sondern ein Arzt befragt werden, der das Kind bereits medizinisch versorgt hat und somit ein Behandlungskontext besteht.

Diese Stellungnahme beschäftigt sich mit den datenschutzbedingten Anforderungen einer solchen Software, die bereits in Duisburg und Umgebung eingesetzt wird.

2 Beantwortung des Fragenkatalogs

2.1 Allgemeines

Nachfolgend werden alle Fragen des Fragenkataloges beantwortet, die die fachliche Expertise des ISDSG berühren. Dies sind vor allem die Bereiche des Datenschutzes und der Informationstechnologie. Fragen, zu denen wir keinen fachlichen Bezug haben, werden nachfolgend nicht mit aufgeführt.

2.2 Frage 1

Welche landesrechtlichen, bundesrechtlichen oder sonstigen Maßnahmen erachten Sie zu einem besseren Schutz vor Kindeswohlgefährdung für notwendig?

Aus unserer Sicht sind für den Fall einer Einführung eines Systems, wie es RISKID darstellt, einige Gesetze zu beachten. Dies betrifft sowohl das Grundgesetz, mit seinem zusammengesetzten Grundrecht der informationellen Selbstbestimmung und der Erziehungshoheit der Eltern, als auch die Verfassung des Landes NRW (besonderer Schutz von Kindern). Das Bundeskinderschutzgesetz muss in diesem Rahmen ebenfalls betrachtet werden. Allerdings sind dort keine Regelungen enthalten, die den Austausch unter Ärzten oder die Datenerhebung bei Verdachtsfällen regeln. Ebenfalls von Belang für den Austausch zwischen Ärzten sind das Strafgesetzbuch, in dem die Schweigepflicht verhaftet ist, das Bundesdatenschutzgesetz und die Berufsordnung der entsprechenden Ärztekammer bzw. das Heilberufsgesetz NRW (HeilBerG). Sollte einer der Ärzte im Krankenhaus angestellt sein, gilt für diesen das Gesundheitsdatenschutzgesetz NRW und bei einer Einbindung von Krankenkassen müssen die Vorschriften der Sozialgesetzbücher und bei den Jugendämtern das NRW Datenschutzgesetz Berücksichtigung finden.

Ein Bruch der Schweigepflicht durch einen rechtfertigenden Notstand erscheint im Zusammenhang mit einer Datenerfassung für Verdachtsfälle nicht plausibel. Für den Fall, dass ein Arzt vom rechtfertigenden Notstand Gebrauch machen kann, scheint die Kindeswohlgefährdung insoweit gesichert zu sein, dass ein Einschalten des Jugendamtes dem Arzt offen steht und somit kein Eintrag in das System notwendig ist. Nach Ansicht des neuen Gutachtens zu RISKID erscheint die Pflege von Verdachtsmomenten in das System, mit dem Verweis auf die Delegation im Heilberufegesetz zur Berufsordnung, als erlaubter Austausch zwischen den Ärzten. Um definitive Klarheit zu schaffen, sollte dieser Austausch in einem Gesetz explizit erwünscht werden, um den Patienten und Betroffenen sowie den Ärzten Handlungssicherheit zu verschaffen. Eine Möglichkeit hierfür könnte ein eigenes Kinderschutzgesetz für NRW darstellen.

2.3 Frage 4

Inwieweit halten Sie den flächendeckenden Aufbau einer EDV-basierten Datenbanklösung zum interkollegialen Austausch von Kinderärzten, wie es beispielsweise in Duisburg und im westlichen Ruhrgebiet mit dem Projekt RISKID erfolgt ist, für zielführend und sinnvoll?

Ein Aufbau nach dem derzeitigen Modus Operandi erscheint eher nicht sinnvoll, da die Erziehungsberechtigten eine Schweigepflichtentbindung unterschreiben, um die Datenverarbeitung zu ermöglichen. Es erscheint wenig plausibel diese Entbindung zu unterschreiben, wenn hierdurch für die Person mögliche Konsequenzen zu erwarten sind. Zwar konnten bereits einige Fälle auf diese Weise entdeckt werden, jedoch erscheint es effektiver die Datenverarbeitung gesetzlich vorzuschreiben, damit alle Verdachtsfälle erfasst werden können. Durch eine gesetzliche Vorschrift wäre es somit nicht mehr notwendig eine Schweigepflichterklärung einzuholen und zwischen den Ärzten und den Betreibern der entsprechenden Plattform muss auch kein Vertrag zu Auftragsdatenverarbeitung geschlossen werden.

2.4 Frage 5

Welche Probleme bestehen aktuell bei einer solchen Datenbank? Gibt es Lösungsmöglichkeiten - wie kann das Spannungsfeld zwischen dem Schutzauftrag gegenüber den Kindern, der ärztlichen Schweigepflicht als schützenswertem Gut und dem Datenschutz für alle Beteiligten zufriedenstellend gelöst werden?

Derzeit wird im System bei einem Verdachtsfall der Vor- und der Nachname sowie das Geburtsdatum des Kindes eingetragen. Zusätzlich können die Ärzte optional die Art ihres Verdachts dokumentieren und in einem Freitextfeld weitere Anmerkungen erfassen. Wenn bei einem Arzt ein neues Kind vorstellig wird, kontrolliert der Arzt mit der Eingabe des Vor- und Nachnamen, sowie des Geburtsdatums, ob es zu dem Kind schon eine Eintragung verfügbar ist. In dem Fall bekommt der Arzt die Kontaktdaten des Arztes, der die Informationen über den Verdachtsfall des Kindes eingestellt hat. Im weiteren Verlauf besteht die Möglichkeit des Austausches der betroffenen Ärzte. Die Anzahl der eingepflegten Informationen sollte auf das Nötigste reduziert werden. Das Eintragen von Verdachtsdiagnosen oder weiteren Informationen ist unnötig, da diese Informationen nur dem Eintragenden zur Verfügung stehen und bei der Identifikation der Kinder nicht berücksichtigt werden. Alle medizinischen Informationen sind in der jeweiligen Primärdokumentation bzw. im Arztpraxisinformationssystem gespeichert.

Bei der Softwarelösung stellen sich einige Probleme dar: Das erste ist die Vorratsdatenspeicherung auf Verdacht, da momentan Daten ohne rechtliche Grundlage gesammelt werden. Momentan lässt sich dies mit der Schweigepflichtentbindung durch die Erziehungsberechtigten rechtfertigen. Sinnvoller erscheint eine gesetzliche Verordnung, sodass dies nicht mehr notwendig ist. Ein anderes Problem stellt die Klarspeicherung der Daten dar, so können Administratoren der Datenbank theoretisch die Namen der Kinder lesen (auch wenn es keinen Anlass zu vermuten gibt, dass es derzeit der Fall ist). Besser wäre eine Kombination aus einer Verschlüsselung der Daten durch ein Public-Key-Verfahren in Kombination mit einer Hash-Generierung. Der Hash sollte über die Pflichtangaben zu dem Kind erzeugt werden, sodass die Kinder durch andere Ärzte auffindbar bleiben und eine Zuordnung zu einem bestimmten Arzt noch möglich ist. Durch die verschlüsselte Ablage können die Hashes bestimmten Kindern zugeordnet werden und somit bei Zerschlagung des Verdachtes auch wieder aus der Datenbank entfernt. Eine noch nicht geklärte Frage in diesem Zusammenhang stellen die Lösfristen dar. Dabei sollten zwei Grenzen betrachtet werden. Zum einen können die Daten an das Alter des Kindes gebunden werden, sodass die Daten spätestens gelöscht werden wenn eine Volljährigkeit besteht. Eine weitergehende Überlegung ist, die Altersgrenze an die Erlangung der bedingten Geschäftsfähigkeit zu binden. Zum anderen sollten Kinder, zu denen über einen langen Zeitraum keine Eintragungen/Anfragen vorgenommen wurden, ebenfalls entfernt werden. Sinnvoll erscheint hierbei ein Zeitraum von drei bis fünf Jahren, in denen der Arzt erinnert werden soll, die Daten der Kinder selbst zu löschen. Momentan sollen die Ärzte bei jedem neuen Kind in ihrer Praxis nachschauen, ob schon eine Eintragung vorhanden ist. Es darf nur nach Kindern gesucht werden, wenn der Arzt einen Verdacht hat. Dies dürfte die Erkennungsquote nicht herabsetzen und neue Patienten würden nicht von Beginn an unter Verdacht gestellt werden. Gleichzeitig wird so auch verhindert, dass in den Protokollen Daten gesammelt werden, die zu Erstellung von Profilen genutzt werden könnten. In diesem Zusammenhang muss jede Suchanfrage dokumentiert werden (was schon der Fall ist) und jeder Mitarbeiter jeder Praxis einen personalisierten Zugang erhalten, damit durch die Protokollierung ein Missbrauch festgestellt werden kann. Möglicherweise ist es auch sinnvoll den Benutzerkreis insoweit weiter einzuschränken, dass Ärzte nur Daten von Kinder aus einer bestimmten Entfernung abfragen können. Die Stadtgrenzen stellen hierbei jedoch kein probates Mittel dar, weil vor allem in den Ballungszentren sehr schnell ein Arzt in einer anderen Stadt aufgesucht werden kann. Einen Radius um den Anfragenden zu ziehen ist eine andere Alternative, jedoch technisch sehr schwer bis gar nicht umzusetzen.

2.5 Frage 7

In welcher Form und Weise ist ein Einbezug der Krankenversicherer denkbar?

Eine Möglichkeit wäre, dass die Krankenkassen die Abrechnungsdaten der Ärzte zu einer Analyse nutzen, um die Wahrscheinlichkeit eines Missbrauchs zu ermitteln. Dies erscheint jedoch impraktikabel, da die Abrechnungsdaten nur quartalsweise an die Versicherer übertragen werden. Außerdem müsste ein Verfahren evaluiert werden, mit dem auf Basis der Konstellation bestimmter Diagnosen oder Verletzungsmuster ein Verdacht auf eine Kindeswohlgefährdung gefunden werden kann. Dies kann aber maximal ein Indiz darstellen. Des Weiteren erhalten die Kostenträger nur die Diagnoseinformationen und keine Begründungen für die einzelne Verschlüsselung. Es ist zu vermuten, dass ein solches Verfahren eine geringe Sensitivität bzw. Spezifität hätte und eine Analyse der Daten vermutlich zu viele Verdachtsfälle liefern würde. Dieses Vorgehen entspräche einer Rasterfahndung in den Daten und erscheint unverhältnismäßig. Für eine gesicherte Diagnose muss außerdem weiterhin ein Arzt verantwortlich sein.

2.6 Frage 9

Wie können Ärzte zum Wohl von Kindern sinnvoll in ein Netzwerk mit Schulen, Eltern, Jugendämtern und Betreuungsinstitutionen eingebunden werden? Gibt es Ihrer Meinung nach bereits sinnvolle und funktionierende Netzwerke, in denen Ärzte sinnvoll eingebunden sind?

Es bestünde die Möglichkeit in das System weitere Institutionen mit einzubinden. Davon sollte jedoch abgesehen werden, da durch eine reine Nutzung der Ärzte und ihrer Erfüllungsgehilfen alle Informationen bei Personen verbleiben, die der Schweigepflicht unterliegen. Eine Erweiterung des Nutzerkreises auf Personen, die nicht der Schweigepflicht unterliegen, könnte das Arzt-Patienten-Verhältnis stören. Daher sollte darauf verzichtet werden.

3 Stellungnahme

Derzeit nutzen 84 Ärzte aus 40 Einrichtungen in den Orten Moers, Krefeld und Duisburg RISKID. Diese Ärzte haben 384 Datensätze in die Datenbank eingetragen. Ziel soll es dabei sein durch den kollegialen Austausch Diagnosen zu sichern. Das heißt einen Verdacht auf Kindeswohlgefährdung zu bestätigen oder aber zu revidieren und im Anschluss daran den Datensatz aus der Datenbank zu löschen. Ist es der politische Wille eine solche Datenbank landesweit einzuführen, sollte diesem durch eine Gesetzgebung Ausdruck verliehen werden. Zwar bescheinigt das Gutachten der derzeitigen Lösung, dass eine Datenverarbeitung auch ohne die Entbindung von der Schweigepflicht zulässig sei, aber um den Ärzten Rechtssicherheit zu geben und die Formalismen einer Auftragsdatenverarbeitung zu vermeiden, deren Kontrollaufgaben durch Ärzte in der Regel nicht wahrgenommen werden können, sollte der Datenaustausch in einem Gesetz reglementiert werden.

Für eine technische Umsetzung einer landesweiten Datenbank kann RISKID als Vorbild dienen, da dort fast alle technischen Anforderungen, die wir aus Datenschutzsicht sehen, umgesetzt sind:

1. Die Benutzer der Datenbank müssen sich authentifizieren, bevor sie ein Zertifikat ausgestellt bekommen, mit dem sie sich mit dem Server verbinden können. Die Authentifizierung sollte hierbei durch einen Abgleich, beispielsweise mit der Kassenärztlichen Vereinigung, stattfinden.
2. Wenn ein Verbindungsaufbau zwischen Praxis und Server stattgefunden hat, sollte jeder Mitarbeiter, der mit dem System arbeitet, einen eigenen Benutzer erhalten, damit möglicher Missbrauch des Systems personenspezifisch dokumentiert werden kann. Um solchen Missbrauch nachweisen zu können muss jede Aktion im System protokolliert werden. Damit der Schutz der Mitarbeiter gewährleistet ist, sollte in die Protokolle nur im Vier-Augen-Prinzip und bei konkretem Verdacht Einsicht genommen werden.
3. Das Einpflegen von Informationen bei Verdachtsfällen muss auf das Nötigste beschränkt werden, also Vorname, Nachname und Geburtsdatum, sowie die Zugehörigkeit zu einem behandelnden Arzt, was durch den Einpflegenden implizit schon vorhanden ist. Weitere Informationen sollten im eigenen Arztinformationssystem hinterlegt sein, da die Übertragung der Daten zur Erfüllung des Zweckes des Kontaktaufbaus zwischen den beiden Ärzten nicht notwendig ist.
4. Um Erziehungsberechtigte nicht unnötig unter Verdacht zu stellen und anfallende Daten zu vermeiden, die einer Profilbildung dienen könnten, sollen Anfragen an das System nicht generell bei neuen Patienten gestellt werden, sondern nur dann, wenn der Arzt einen Anfangsverdacht hat. Die Regelung, dass dabei der Vorname, Nachname und der Geburtstag in die Suchmaske eingetragen wird und bei einem Treffer die Kontaktdaten des entsprechenden Arztes angezeigt werden, ist dabei schon gut umgesetzt.
5. Wenn nachträglich kein Verdacht auf Kindeswohlgefährdung besteht, muss der einstellende Arzt den Datensatz aus der Datenbank entfernen, sodass Datensätze von nicht betroffenen Kindern nicht in der Datenbank aufgeführt werden. Gleiches gilt für einen festzulegenden Zeitraum, über den zu einem Kind keine Anmerkungen mehr gemacht wurden. Hierbei empfiehlt es sich dem Arzt die letzte Entscheidung zu überlassen, ob er den Datensatz entfernt. Unabhängig davon sollten die Daten der Kinder spätestens dann gelöscht werden, wenn sie volljährig sind. Es ist zu überlegen, ob dies eventuell schon bei Kindern geschehen kann, die bedingt geschäftsfähig sind.
6. Aus technischer Sicht muss verhindert werden, dass der Administrator auf die Inhalte der Datenbank zugreifen kann. Dies kann dadurch erreicht werden, dass die Daten der Kinder mit einem Public-Key-Verfahren verschlüsselt abgespeichert werden. So können nur die behandelnden Ärzte auf die Klardaten zugreifen. Da die Daten in diesem Fall nicht mehr durchsuchbar sind, muss aus den Attributen, mit denen nach einem Kind gesucht wird, ein Hash erzeugt werden, aus dem sich die Daten des Kindes nicht herleiten lassen. Diese Funktionsweise wird bei der Speicherung von verschlüsselten Passwörtern genutzt. Auf diese Weise kann trotzdem nach den Kindern gesucht werden und technische Mitarbeiter können die Daten keiner konkreten Person mehr zuordnen. Sollten sich Angreifer von Außen, trotz der sicheren Architektur von RISKID, unerlaubten Zugriff auf die Daten verschaffen, können diese nicht mehr verwendet werden.
7. Vor einer landesweiten Einführung muss die Systemarchitektur hinsichtlich der zu erwartenden Lastanforderungen durch ein erhöhtes Anfrageaufkommen überprüft und ggf. angepasst werden.
8. Die Einbindung des Systems in das KVSafe.net, das sichere Netz zur Kommunikation zwischen Ärzten, sollte erwogen werden.

Wenn das Recht der Kinder auf Unversehrtheit höher angesehen wird, als das Recht der Kinder auf informationelle Selbstbestimmung (wahrgenommen durch die Erziehungsberechtigten) und die grundlegenden Einschränkungen einer Vorratsdatenspeicherung, dann ist die Lösung von RISKID, mit einigen notwendigen Änderungen, ein adäquates Mittel um dies –auch unter den Aspekten des Datenschutzes- umzusetzen. Dabei darf das System nur Ärzten zugänglich gemacht werden, damit die Informationen den Schutz der ärztlichen Schweigepflicht nicht verlassen.

Ihr Partner für Datenschutz im Gesundheitswesen!

Westfalendamm 251 - 44141 Dortmund

Tel: 0231 4499599-91 | Fax: 0231 4499599-99

kontakt@isdsg.de | <https://www.isdsg.de>

Fingerprint: A554 551A D5F1 BEBB C552 A062 751F CD07 5A78 F82F

Bitte übermitteln Sie uns vertrauliche Informationen ausschließlich mittels verschlüsselter Email an **info.pgp@isdsg.de**. Mehr zum Thema PGP Verschlüsselung, Tipps & Tricks zur Einrichtung und unseren öffentlichen PGP-Schlüssel finden Sie unter <https://www.isdsg.de>.

Das ISDSG – Institut für Sicherheit und Datenschutz im Gesundheitswesen in Dortmund beschäftigt sich mit allen Fragen zum Thema Informationssicherheit und Datenschutz mit Schwerpunkt auf die Akteure des Gesundheitswesens. Das Institut wurde vom Medizin-Wirtschaftsinformatiker Prof. Dr. rer. medic. Thomas Jäschke gegründet. Das Portfolio des ISDSG umfasst neben den frei zugänglichen Informationen und Dienstleistungen auch besonders ausgerichtete Angebote für Praxen und Unternehmen. Angetrieben wird das spezialisierte Team durch die fortschreitende Durchdringung der Digitalisierung in der Medizin, aufgrund der Potenziale neuer Informationstechnologien.