

PaSIS

Patientensicherheits- Informationssystem

Rahmenvereinbarung

zur Teilnahme am Incident Reporting System PaSIS

Hintergrund

Das Incident Reporting System PaSIS dient der anonymen Erfassung und Verbreitung von sicherheitsrelevanten Ereignissen in Klinik und Praxis und wird vom Tübinger Patientensicherheits- und Simulationszentrum TüPASS betrieben. Als „sicherheitsrelevante Ereignisse“ werden alle Abweichungen vom regelhaften Verlauf, Fehler, kritische Ereignisse und Beinahe-Zwischenfälle bezeichnet, welche die Patientensicherheit gefährdet haben oder haben könnten. Das Incident Reporting System (IRS) ist anonym und internetbasiert aufgebaut.

Zahlreiche Informationsunterlagen sind unter www.pasis.de im Bereich „Downloads“ verfügbar, darunter einige Publikationen sowie das Startpaket inklusive dieser Rahmenvereinbarung und entsprechender Vordrucke und Mustervorlagen.

Für den Erfolg des Incident Reporting Systems PaSIS in Deutschland und damit für die Patientensicherheit ist die sachgerechte Nutzung des Werkzeugs PaSIS entscheidend.

Wird PaSIS entgegen seiner Bestimmung gebraucht, wird also z.B. einmal die Anonymitätsgarantie verletzt, so kann der Schaden sehr leicht über die lokale Institution hinausgehen und sich möglicherweise unwiderruflich negativ auf die Gesamtidee des Incident Reporting in Deutschland auswirken. Als Folge würden unter Umständen keine Berichte mehr eingetragen, wenn die Nutzer das Vertrauen in das System verloren haben. Aus diesem Grunde ist es essentiell, dass sich die beteiligten Institutionen bzw. die PaSIS-Verantwortlichen vor Ort der Bedeutung und Verantwortung ihrer Arbeit bewusst sind.

Hintergründe PaSIS

Seit 2005 besteht PaSIS als Projekt des Tübinger Patienten-Sicherheits- und Simulations-Zentrum (TüPASS) am Universitätsklinikum Tübingen. Das TüPASS-Team um Dr. med. Silke Reddersen hat sich in den letzten Jahren mit sicherheitsbezogenen Simulationstrainings und Projekten zur systematischen Erhöhung der Patientensicherheit beschäftigt. Seit 2004 betreibt TüPASS das Incident Reporting System PaSIS, welches zu Beginn auch als Grundlage für das ehemalige Incident Reporting System der DGAI (PaSOS) verwendet wurde. Die Unterschiede der beiden Systeme sind so minimal, dass für sie dieselben gesetzlichen Rahmenbedingungen gelten. Aus diesem Grunde haben die Aussagen des juristischen Gutachtens und des Datenschutzgutachtens zum PaSOS der DGAI und des BDA auch für PaSIS Gültigkeit.

Juristisches Gutachten zum Incident Reporting im Auftrag DGAI/BDA

Um Klarheit über rechtliche Aspekte rund um die Thematik Incident Reporting zu bekommen, wurde von der Sozietät Ulsenheimer & Friederich im Auftrag von DGAI/BDA im Februar 2006 ein juristisches Gutachten erstellt. In enger Kooperation mit der AG Incident Reporting von DGAI/BDA wurden alle relevanten Fragen aus juristischer Sicht beantwortet. Auch die Rahmenvereinbarung und sämtliche Unterlagen inklusive des Meldebogens wurden einer juristischen Prüfung unterzogen und entsprechend angepasst. Vor allem wurde deutlich, dass externe, zentrale Reporting Systeme wie PaSIS deutliche Sicherheitsvorteile gegenüber lokalen Systemen haben. Außerdem wurde auf die wichtigen Vorteile der externen Anonymisierung und De-Identifizierung durch PaSIS im Vergleich zur lokalen Anonymisierung hingewiesen (s. Formular 7 zu Schutz vor Vernehmungen, Zeugnisverweigerungsrecht und Schutz vor Beschlagnahme der Unterlagen). Dies führte dazu, dass die Teilnahme an PaSIS aus Sicherheitsgründen nur noch mit (kostenpflichtiger) externer Anonymisierung & De-Identifizierung möglich ist. Gleichzeitig kommt für alle Fälle eine zentrale Verschlagwortung zum Einsatz, welche eine attraktive Suchfunktion für den Fallpool zur Verfügung stellt.

Wird das PaSIS-Tool entgegen seiner Bestimmung gebraucht, wird also z.B. einmal die Anonymitätszusicherung verletzt, so kann der Schaden sehr leicht über die lokale Institution hinaus gehen und sich möglicherweise unwiderruflich auf das gesamte Incident Reporting in Deutschland negativ auswirken. Als Folge würden u.U. keine Berichte mehr eingetragen, wenn die Nutzer das Vertrauen in das System verloren hätten. Aus diesem Grunde ist es essentiell, dass sich die beteiligten Institutionen bzw. die PaSIS-Beauftragten vor Ort der Bedeutung und Verantwortung ihrer Arbeit bewusst sind

Um die Sicherheit für die Nutzer und die Effektivität des Systems zu optimieren, wird mit den Beteiligten die folgende Rahmenvereinbarung schriftlich geschlossen.

Rahmenvereinbarung

für die Nutzung von PaSIS

Die hier genannten Rahmenbedingungen für die Nutzung des PaSIS haben verpflichtenden Charakter und werden schriftlich vereinbart. Nichtbeachtung kann zum Ausschluss von der Teilnahme und ggf. Schadensersatzforderungen führen.

- 1) Vor der Einführung von PaSIS informiert die Leitung der Institution/Abteilung die Mitarbeitenden über die Einführung des PaSIS. Die Information eines etwa vorhandenen Personal- oder Betriebsrates wird vor Beginn empfohlen. Analog wird die Information und Zustimmung der Einrichtungsleitung empfohlen. Datenschutzbeauftragte sollten ebenso eingebunden werden. Durch die zugesicherte Sanktionsfreiheit und Anonymität des PaSIS-Systems wird die Zustimmung im Allgemeinen kein Problem darstellen.

- 2) Die Institutionsleitung sichert ihren Mitarbeitern die **Vertraulichkeit** der gemeldeten Daten zu. Ein Formular zur Aushändigung an alle Mitarbeiter hierfür liegt bei (Formular 3). Es wird zugesichert, dass aufgrund eines Berichtes keine negativen (z.B. personalrechtlichen) Konsequenzen für den Mitarbeiter abgeleitet werden. Nach dem Eingang von Meldungen wird von allen Leitungspersonen nicht versucht herauszufinden „Wer war das?“. Der Sinn von PaSIS ist die Erhöhung der Patientensicherheit. Es geht nicht darum „Schuldige“ zu finden.

- 3) Die Institutsleitung benennt mindestens einen **PaSIS-Beauftragten** (Aufgaben des Beauftragten s.u.). Dieser wird schriftlich mit Kontaktdaten (Telefon, Email, Anschrift) an PaSIS gemeldet (s. Formular 5). Es wird empfohlen für alle Berufsgruppen (Ärzte, Pflegekräfte, Rettungsassistenten u.a.) jeweils mindestens einen Beauftragten je Organisationseinheit zu benennen und die Anzahl der Abteilungsgröße anzupassen. Beispiel: Intensivstation: 2 Ärzte, 2 Pflegekräfte; OP: 2 Ärzte, 2 Pflegekräfte; Normalstation: 1 Arzt, 1-2 Pflegekräfte etc.

Aufgaben der PaSIS-Beauftragten sind:

- Klärung von Problemen vor Ort und Ansprechpartner für PaSIS
- Anregung der Mitarbeiter, Fälle zu berichten und ggf. dabei zu helfen.
- Interne Mitwirkung an der Bearbeitung der Fälle. Die Analyse und Ableitung von möglichen Verbesserungsmaßnahmen erfolgen in Kooperation zwischen TüPASS und den Beauftragten. Dabei ist immer die enge Koordination mit der Abteilungsleitung und dem zentralen Risiko- bzw. Qualitätsmanagement anzustreben. Für diese Funktion wird für die PaSIS-Beauftragten ein eigener Account angelegt (interne Diskussions- und Bearbeitungsfelder).
- Teilnahme an einer von TüPASS durchgeführten speziellen Schulung in der Anwendung von PaSIS

Die PaSIS-Beauftragten sollen für ihre Aufgaben in ausreichendem Umfang freigestellt werden.

- 4) Jeder PaSIS-Beauftragte der teilnehmenden Organisation wird **schriftlich nach §5 Datenschutzgesetz auf Verschwiegenheit verpflichtet** (s. Formular 6). Dies soll die hohe Bedeutung des Datenschutzes, sowie der Schweigepflicht nach intern und extern in Bezug auf meldende und / oder betroffene Personen (Mitarbeiter, Patienten) gewährleisten und unterstreichen. Erst nach Vorliegen dieser Verpflichtungen kann das System in Betrieb gehen.

Werden innerhalb des teilnehmenden Instituts neue PaSIS-Beauftragte benannt oder scheidet ein PaSIS-Beauftragter aus dem System aus, ist das Institut dazu verpflichtet diese Änderungen anzuzeigen.

Neu berufene PaSIS-Beauftragte sind ebenso mit Hilfe der entsprechenden Formulare auf Datenschutz zu verpflichten. Die Originale der unterschriebenen Verpflichtungserklärungen sind bei TüPASS vorzulegen.

- 5) Die Fälle jeder Abteilung werden in anonymer Form der bundesweiten Datenbank des PaSIS-Systems zur Verfügung gestellt. Vor der Freigabe findet eine Anonymisierung der eingegebenen Daten durch Mitarbeiter des TüPASS statt. Die ano-

nymisierten Daten werden dann, ohne dass andere eine Zuordnung zu einer Institution vornehmen könnten, auf dem allgemeinen, bundesweiten PaSIS-System bearbeitet. Eingehende IP-Adressen werden nicht datensatzbezogen gespeichert. Über den **abteilungsbezogenen Account** können die anonymisierten Fälle der eigenen Einrichtung selektiv eingesehen werden. So **ersetzt PaSIS ein lokales Incident Reporting System**, mit dem Vorteil der zentralen Datenspeicherung und externen Anonymisierung. **Nach Aussage eines Rechtsgutachtens sind die Daten im zentralen System des PaSIS mit hoher Sicherheit für juristische Belange nach Presserecht geschützt.** Durch die Speicherung im zentralen Informationsdienst von PaSIS besteht ein Zeugnisverweigerungsrecht, welches sich sowohl auf die Daten, als auch die zentralen PaSIS-Mitarbeiter (z.B. für Anonymisierung) erstreckt. Dies ist ein enormer Vorteil im Vergleich zu allen lokalen Systemen, deren Daten prinzipiell jederzeit beschlagnahmt und eingesehen werden können.

- 6) **Kosten:** Da es sich bei PaSIS um ein Internetbasiertes System handelt, muss in der Klinik keine Software installiert werden. Auch die Bedienung des Systems zur Eingabe von Berichten ist einfach und meist ohne spezielle Einweisung nutzbar. Die Kosten, die sich im Wesentlichen auf die fallbezogenen Arbeiten (Anonymisierung und Analyse, sowie Rückmeldung an Beauftragte) beziehen, sind im Kostenplan als Bestandteil dieses Vertrages aufgeführt.

- 7) Um die optimale Nutzung von PaSIS zu gewährleisten, bedarf es einer entsprechenden Expertise der Verantwortlichen aus den sich beteiligenden Institutionen. Alle PaSIS-Beauftragten sollen an einer **Basisschulung im Umgang mit PaSIS** teilnehmen. Die Schulungen werden von Mitarbeitern des TüPASS durchgeführt. Ziel der Schulung ist, die PaSIS-Beauftragten in Sicherheit und Nutzung von PaSIS, sowie in der Darstellung möglicher Maßnahmen zur Analyse und zum Feedback eingegangener Meldungen zu unterrichten. Den Schulungsteilnehmern wird ein **Zugang zu allen Präsentationen (Powerpoint) in frei editierbarer Form und zur Publikationssammlung (pdf)** nach der Schulung zur Verfügung gestellt. So kann PaSIS intern weiter geschult (Schneeballsystem) und neue Mitarbeiter können entsprechend eingewiesen werden.

8) Das **PaSIS stellt in keiner Weise einen Ersatz für anderweitig vorgeschriebene interne oder externe Meldungen von Zwischenfällen dar**. Haftungsrechtlich oder gesetzlich vorgeschriebene Meldungen (z.B. Arzneimittelnebenwirkungen, MPG-Meldungen etc.) werden durch PaSIS nicht ersetzt, ebenso wenig die Information des Patienten oder der Angehörigen. Durch die Anonymität der Meldungen kann ein Incident Reporting System wie PaSIS bzw. dessen Beauftragte diese Funktion nicht leisten. Da es PaSIS auch ermöglicht, Fälle mit Patientenschäden zu melden, sind die Mitarbeiter initial und regelmäßig auf diesen Umstand hinzuweisen. Zur Klärung straf- und zivilrechtlich relevanter Vorkommnisse kann PaSIS aufgrund der Anonymisierung der Fälle nicht herangezogen werden.

9) **Haftungsausschluss**: Schutz- und Verbesserungsmaßnahmen müssen immer lokal vor Ort getroffen werden. PaSIS kann aufgrund der Freiwilligkeit und Anonymisierung keinerlei Gewähr für wichtige Warn- oder Verbesserungsmeldungen übernehmen. Die Meldungen in PaSIS stammen von anonymen Meldern, die im Prinzip Mitarbeiter an jeder beliebigen Institution sein können. Damit kann für die Verbindlichkeit von Aussagen in PaSIS keinerlei Gewähr übernommen werden. Alle genannten Empfehlungen müssen kritisch bewertet und im Einzelfall von kompetentem Fachpersonal auf Anwendbarkeit, Sinnhaftigkeit und Sicherheit überprüft werden. Eine Haftung für direkte oder indirekte Schäden (Rufschädigung etc), die sich aus Meldungen an PaSIS oder den Betrieb von PaSIS ergeben, auch solche durch unzureichende Anonymisierung, ist explizit ausgeschlossen, sofern nicht grobe Fahrlässigkeit oder Vorsatz auf Seiten von PaSIS nachgewiesen werden kann.

Vorstehender Haftungsausschluss gilt nicht für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer fahrlässigen Pflichtverletzung beruhen, sowie für sonstige Schäden, die auf einer grob fahrlässigen Pflichtverletzung oder Vorsatz beruhen.

10) Die **Teilnahme an PaSIS ist freiwillig** und kann jederzeit von beiden Seiten (PaSIS-Betreiber und Nutzer) innerhalb der vertraglichen Fristen gekündigt werden.

Ich habe die Punkte der PaSIS-Rahmenvereinbarung zur Kenntnis genommen und versichere gegenüber dem TüPASS (Betreiber von PaSIS) die Umsetzung und Einhaltung dieser Rahmenbedingungen.

(Ihre unterzeichnete Vereinbarung bekommen Sie gegengezeichnet als Kopie für Ihre Akten zurückgesendet.)

Institutionsleiter (Titel / Vorname / Name)

Ort, Datum

Unterschrift

[Stempel / Siegel der Institution]

Für den Betreiber des PaSIS, vertreten durch den Leiter des Tübinger Patienten-Sicherheits- und Simulations-Zentrums (TüPASS): Dr. med. Silke Reddersen

Tübingen, den _____

Dr. med. Silke Reddersen