PaSIS

Patienten-Sicherheits-Informations-System

PaSIS-Startpaket

Formulare

zur Teilnahme am Incident Reporting System PaSIS

Formular 1:	**Checkliste PaSIS-Teilnahme**
Formular 2:	**Rahmenvereinbarung**
Formular 3:	**Mitarbeiter-Information**
Formular 4:	**Account-Antrag**
Formular 5:	**PaSIS-Beauftragte & Ansprechpartner**
Formular 6:	**Datenschutz, Erklärung und Merkblatt**
Formular 7:	**Aussageverweigerungsrecht**
Formular 8:	**Infoblatt PaSIS-Schulung**
Anhang:	**Bestellformular PaSIS-Schulungen**

PaSIS
c/o TüPASS
Tübinger Patientensicherheits-
und Simulationszentrum
Silcherstraße 5
72076 Tübingen

Tel. +49 (0)7071 / 29 86733
Fax: +49 (0)7071 / 29 4943
www.pasis.de

pasis

tüpass
Patientensicherheit und Simulation

PaSIS

Patienten-Sicherheits-Informations-System

Checkliste PaSIS-Teilnahme

Notwendige Schritte für Ihre Organisation

1. Informieren Sie die Leitungsebene und je nach Institution Betriebsrat und Datenschutzbeauftragte über die geplante Einführung von PaSIS. ☐

2. Fordern Sie die Vertragsunterlagen zur PaSIS-Teilnahme bei uns an (nicht über PaSIS-Homepage abrufbar). Lesen und unterzeichnen Sie die Vertragsunterlagen und die Rahmenvereinbarung **(Formular 2)**. ☐

3. Informieren Sie das Personal im Sinne des „internen Sanktionsschutzes“: Vertraulichkeit und Interesse an Verbesserungen zur Erhöhung der Patientensicherheit, nicht am Identifizieren von „Schuldigen“. Geben Sie allen Mitarbeitenden die schriftliche Zusicherung, dass keine negativen personellen Konsequenzen aus Berichten an PaSIS zu befürchten sind. Dafür verwenden Sie bitte die im Startpaket enthaltene Vorlage **(Formular 3).** ☐

4. Klären Sie vorab mit uns, wie Ihre Organisationsstruktur systemseitig dargestellt werden kann (Abbild der Organisation in PaSIS / Meldekreise / etc.). ☐

5. Beantragen Sie für jede teilnehmende Abteilung einen Account für PaSIS **(Formular 4)**. Bitte bewahren Sie eine Kopie an einem sicheren Ort auf. ☐

6. Benennen Sie einen PaSIS Hauptansprechpartner (Qualitätsmanagement), einen Ansprechpartner für Vertragliches und Rechnungen, sowie je nach Institutsgröße einen oder mehrere PaSIS-Beauftragte je Abteilung und Berufsgruppe **(Formular 5)**. ☐

7. Alle PaSIS-Beauftragten müssen einzeln nach §5 Datenschutzgesetz gegenüber dem Betreiber schriftlich verpflichtet werden **(Formular 6)** und über Ihr Aussageverweigerungsrecht informiert werden **(Formular 7)**. ☐

8. Die PaSIS-Beauftragten und evtl. weitere ärztliche und pflegerische Mitarbeiter sollten an einer PaSIS-Basis-Schulung teilnehmen **(Formular 8)**. Um Termine für Schulungen abzustimmen kommen Sie bitte auf uns zu. ☐

9. **Senden Sie die Vertragsunterlagen, sowie die Formulare 2, 4, 5 und 6 im Original unterzeichnet an untenstehende Adresse**. Bitte bewahren Sie Kopien für Ihre Unterlagen auf. ☐

10. Nach erfolgter Schulung der PaSIS-Beauftragten Ihrer Institution und Eingang aller Formulare erhalten Sie schriftlich Ihre endgültigen Logininformationen und die Information über die erfolgte Freischaltung Ihres Zuganges zu PaSIS. Die Abrechnung der anfallenden Gebühren **(Formular 9)** beginnt ab 1. des darauffolgenden Monats. ☐

PaSIS
c/o TüPASS
Tübinger Patientensicherheits-
und Simulationszentrum
Silcherstraße 5
72076 Tübingen

Tel. +49 (0)7071 / 29 86733
Fax +49 (0)7071 / 29 4943

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 Anonymitätszusicherung 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

pasis

tüpass
Patientensicherheit und Simulation

PaSIS

Patienten-Sicherheits-Informations-System

Information an alle Mitarbeiter

1) Zusicherung: Keine Nachteile durch Teilnahme an PaSIS

2) Hinweis auf Verpflichtung zum Wahrheitsgrundsatz bei Meldungen

Unsere Institution möchte zur Optimierung der Patientensicherheit am bundesweiten Incident Reporting System PaSIS teilnehmen. Durch eine möglichst zahlreiche und offene Darstellung abgelaufener Probleme oder kritischer Situationen soll die Patientensicherheit systematisch erhöht werden. Fallberichte werden anonym, sicher und verschlüsselt über das Internet an das zentral betriebene PaSIS-System gesendet.

Der Sinn des PaSIS ist die Erhöhung der Patientensicherheit. Es geht nicht darum „Schuldige“ zu finden.

Die Geschäftsführung sichert hiermit allen Mitarbeitern zu, dass:

- ✓ keine Anstrengungen unternommen werden, herauszufinden, wer einen speziellen Fall berichtet haben könnte
- ✓ selbst bei zufälliger Kenntnis der beteiligten Personen aus den Informationen im Fallbericht keine negativen Konsequenzen (Sanktionen / personalrechtliche / arbeitsrechtliche Folgen) für die Beteiligten getroffen werden
- ✓ immer versucht wird, systematische Ursachen für Probleme zu erkennen und zu verbessern, anstatt Einzelpersonen zur Verantwortung zu ziehen
- ✓ das Verfassen eines Berichtes für PaSIS als besonders motiviertes, verantwortungsvolles Verhalten gewertet wird und immer als besonders positiv betrachtet wird

Verpflichtung auf Wahrheitsgrundsatz: Unabhängig von obiger Zusage, bittet die Leitung darum, bei allen Meldungen den Wahrheitsgrundsatz einzuhalten. Das heißt, alle Meldungen sollen nach bestem Wissen der (zumindest subjektiv empfundenen) Wahrheit entsprechen. Dies ist für eine sinnvolle Funktion des Systems und aus juristischen Gründen notwendig.

_____

Ort, Datum

_____ _____

Unterschrift Institutionsleiter | Institution (Stempel/Siegel)

pasis

tüpass
Patientensicherheit und Simulation

PaSIS

Patienten-Sicherheits-Informations-System

Account-Antrag

Sie können hier einen Account für alle Mitarbeiter Ihrer Abteilung beantragen. Bitte halten Sie diese Accountdaten vertraulich. Bei Bedarf, z.B. wenn Sie den Verdacht haben, dass Ihr Account missbraucht wird, können Sie jederzeit über webmaster@pasis.de ein neues Passwort und / oder einen neuen Benutzernamen beantragen.

Wenn mehrere Abteilungen aus Ihrer Institution einen PaSIS-Account erhalten sollen, muss dieses Formular für jede Abteilung gesondert ausgefüllt werden.

Sie können hier ein Wunsch-Passwort angeben. Wünschen Sie kein spezielles Passwort, bekommen Sie ein zufälliges Passwort von TüPASS zugesandt.

Für die PaSIS-Beauftragten wird ein separater Account angelegt und ebenfalls auf dem Postweg zugestellt.

.....
Abteilung

.....
Institution

.....
Postadresse

.....
eMail

.....
Telefon

Optional:

Wunsch-Abteilungs-Passwort: .....

pasis

tüpass
Patientensicherheit und Simulation

PaSIS
Patienten-Sicherheits-Informations-System

Meldung: PaSIS Beauftragte

Institution: _____

Abteilung: _____

Wir empfehlen aus allen beteiligten Berufsgruppen Beauftragte zu benennen. Idealerweise sind dies freiwillige/gewählte Mitarbeiter mit eigenem Interesse an der Thematik. (Postadresse wegen Passwortzusendung notwendig)

PaSIS-Beauftragte(r)

Name, Vorname	Titel	Beruf	Adresse	Email	Telefon

Bitte beachten: Jeder involvierte PaSIS-Beauftragte muss eine Verpflichtung auf das Datengeheimnis nach §5 BDSG (Formular 6) unterzeichnen und an folgende Adresse schicken:

PaSIS
c/o TüPASS
Tübinger Patientensicherheits-
und Simulationszentrum
Silcherstraße 5
72076 Tübingen

Tel. +49 (0)7071 / 29 86733
Fax +49 (0)7071 / 29 4943

TüPASS
Tübinger Patienten-Sicherheits- und Simulations-Zentrum

PaSIS

Patientensicherheits- und Informationssystem

Meldung: PaSIS Ansprechpartner

Institution: _____

Abteilung: _____

PaSIS-Hauptansprechpartner

Name, Vorname	Titel	Beruf	Adresse	Email	Telefon

PaSIS-Ansprechpartner für Vertragliches und Rechnungen

Name, Vorname	Titel	Beruf	Adresse	Email	Telefon

Bitte beachten: Wir benötigen für jede teilnehmende Organisation einen Hauptansprechpartner und einen Ansprechpartner für Vertragliches und Rechnungen. Bitte senden sie das ausgefüllte Formular an folgende Adresse:

PaSIS
c/o TüPASS
Tübinger Patientensicherheits-
und Simulationszentrum
Silcherstraße 5
72076 Tübingen

Tel. +49 (0)7071 / 29 86733
Fax +49 (0)7071 / 29 4943

pasis

tüpass
Patientensicherheit und Simulation

PaSIS
Patienten-Sicherheits-Informations-System

Verpflichtung auf das Datengeheimnis

gemäß § 5 Bundesdatenschutzgesetz (BDSG), auf das Fernmeldegeheimnis gemäß § 88 Telekommunikationsgesetz (TKG) und auf Wahrung von Geschäftsgeheimnissen von Externen

Tübinger Patienten-Sicherheits- und Simulations-Zentrum (PaSIS-Betreiber)

Verpflichtender

Verpflichteter
(Name, Vorname, Institution)

1. Verpflichtung auf das Datengeheimnis nach § 5 BDSG
Aufgrund von § 5 BDSG ist mir untersagt, personenbezogene Daten oder Fallberichte, die mir im Rahmen meiner Tätigkeit für ***PaSIS*** bekannt werden, unbefugt zu erheben, zu verarbeiten oder zu nutzen. Dies gilt sowohl für die dienstliche Tätigkeit innerhalb wie auch außerhalb (z.B. bei Kunden und Interessenten) des Unternehmens/der Behörde. Die Pflicht zur Wahrung des Datengeheimnisses bleibt auch nach Beendigung meiner Tätigkeit bestehen.

2. Verpflichtung auf das Fernmeldegeheimnis
Aufgrund von § 88 Absatz 2 TKG bin ich zur Wahrung des Fernmeldegeheimnisses verpflichtet, soweit ich im Rahmen meiner Tätigkeit für ***PaSIS*** bei der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirke.

3. Verpflichtung auf Wahrung von Geschäftsgeheimnissen
Ich bestätige, dass ich die im Zusammenhang mit meiner Tätigkeit erlangten Unterlagen oder sonstige nicht allgemein zugängliche Informationen Dritten gegenüber vertraulich behandeln werde. Ich werde diese Unterlagen und Informationen ohne vorherige schriftliche Vereinbarung mit ***PaSIS*** auch nicht für eigene gewerbliche Zwecke oder andere Auftraggeber benutzen.

Von diesen Verpflichtungen habe ich Kenntnis genommen. Ich bin mir bewusst, dass ich mich bei Verletzungen des Datengeheimnisses, des Fernmeldegeheimnisses oder von Geschäftsgeheimnissen strafbar machen kann, insbesondere nach §§ 44, 43 Abs. 2 BDSG und § 206 Strafgesetzbuch (StGB). Das Merkblatt zur Verpflichtungserklärung mit den Abschriften der genannten Vorschriften habe ich erhalten.

Ort, Datum	Ort, Datum
Unterschrift Verpflichteter	Unterschrift Verpflichtender (TüPASS)

Muster nach Bundesdatenschutzgesetz.

PaSIS
Patienten-Sicherheits-Informations-System

Merkblatt zur Verpflichtungserklärung

§ 5 BDSG – Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nichtöffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 43 Absatz 2 BDSG – Bußgeldvorschriften

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,

5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder

6. entgegen § 30 Abs. 1 Satz 2 die in § 30 Abs. 1 Satz 1 bezeichneten Merkmale oder entgegen § 40 Abs. 2 Satz 3 die in § 40 Abs. 2 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt.

§ 44 BDSG – Strafvorschriften

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Aufsichtsbehörde.

§ 88 TKG Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

(4) Befindet sich die Telekommunikationsanlage an Bord eines Fahrzeugs für Seefahrt oder Luftfahrt, so besteht die Pflicht zur Wahrung des Geheimnisses nicht gegenüber der Person, die das Fahrzeug führt oder gegenüber ihrer Stellvertretung.

§ 206 StGB – Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekannt geworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder
3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,
2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder
3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekannt geworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

pasis

tüpass
Patientensicherheit und Simulation

PaSIS
Patienten-Sicherheits-Informations-System

Hinweise
im Falle eines Kontakts mit Strafverfolgungsbehörden

1) Aussageverweigerungsrecht für PaSIS-Beauftragte und Mitarbeiter

[Auszug aus dem juristischen Gutachten der Kanzlei Ulsenheimer vom 20.02.2006]

Das Zeugnisverweigerungsrecht ist ein Berufsrecht für Angehörige der zur Zeugnisverweigerung berechtigten Berufe. Mitglieder dieser Berufsgruppen müssen deshalb vor einer Vernehmung nicht extra auf ihr Zeugnisverweigerungsrecht hingewiesen werden.

§53 Abs. 1 Nr. 5 StPO erkennt „Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Druckwerken, Rundfunksendungen, Filmberichten oder der Unterrichtung oder Meinungsbildung dienenden Informations- und Kommunikationsdiensten berufsmäßig mitwirken oder mitgewirkt haben“, **ein weit reichendes Zeugnisverweigerungsrecht hinsichtlich der Person des Informanten, der in Hinblick auf ihre Tätigkeit gemachten Mitteilung, über deren Inhalt, den Inhalt selbst erarbeiteter Materialien und den Gegenstand berufsbezogener Wahrnehmungen an**.

PaSIS ist ein der Unterrichtung von Mitarbeitern im Gesundheitswesen dienender Informations- und Kommunikationsdienst [...]. Die redaktionell aufbereiteten Meldungen werden der (Fach-) Öffentlichkeit zum Zwecke der Diskussion und des Erkenntnisgewinns zur Verfügung gestellt. Der Dienst dient einer allgemein zugänglichen Unterrichtung und Meinungsbildung.

Der Zeuge ist mit der redaktionellen Aufbereitung der abrufbaren Informationen befasst. Er ist wiederkehrend für den Dienst tätig.
Das Zeugnisverweigerungsrecht bezieht sich auf sämtliche Arbeitsschritte einer Publikation von der Recherche über die inhaltliche, sprachliche und technische Gestaltung bis hin zur Veröffentlichung der Mitteilung. Folge ist ein Zeugnisverweigerungsrecht hinsichtlich der Person des Einsenders der Meldung sowie deren Inhalt.

2) Es besteht ein Beschlagnahmeverbot gemäß §97 Abs.5 StPO

hinsichtlich Schriftstücken, Ton-, Bild- und Datenträgern, die sich im Gewahrsam der Mitarbeiter oder der Redaktion befinden. Mindestens ist eine Versiegelung bis zur endgültigen Prüfung zu veranlassen.

pasis

tüpass
Patientensicherheit und Simulation

PaSIS Schulungsinhalte

Grundlagen für die Eingangsschulung von PaSIS-Beauftragten

- ✓ Einführung in das PaSIS System; Sensibilität der Aufgabe: Do's and Dont's beim Sammeln und Analysieren von Fällen
- ✓ Technische Aspekte der Dateneingabe und –Speicherung: Datensicherheit, physischer Speicherplatz, Zugriffsmöglichkeiten, Rechteverwaltung etc.
- ✓ Rechtliche Aspekte: Zwischenfall und Unfall-Meldepflichten etc. Wahrheitsgrundsatz und Wahrheitspflicht bei den Meldungen (formale „Verpflichtung zur Wahrheitsgemäßen Meldung").
- ✓ Zeugnisverweigerungsrecht und Datensicherheit bei PaSIS, Aufbewahrung von Unterlagen, Passwörtern etc
- ✓ Fehlerentstehung und –Prävention: Systemansatz, fehlerevozierende Handlungssituationen, grundlegende fehlerträchtige menschliche Eigenschaften
- ✓ Konsequenzen aus PaSIS: Sich aus Meldungen ergebende Aufgaben, Möglichkeiten der Umsetzung, Tipps für Unterstützung und Hilfe, rechtliche Konsequenzen für die nutzende Institution etc.
- ✓ Verfahren bei der Auswertung der Fälle: Anonymisierung / Deidentifizierung, Umgang mit den Freitexten; graphische Aufbereitungsmöglichkeiten etc., Überblick über den Ablauf der Fallbearbeitung im System, Tipps zur nachhaltigen Entwicklung und Umsetzung von Maßnahmen mit PaSIS
- ✓ Das PaSIS Startpaket mit Rahmenvereinbarung „Schritt-für-Schritt"
- ✓ Aktuelles, Fragen, lokale Probleme, Diskussion

Jeder Teilnehmer erhält über die PaSIS Plattform einen Zugang zu allen **Präsentationen (Powerpoint) in frei editierbarer Form** und zur Publikationssammlung (pdf). So kann die Idee des PaSIS intern weiter geschult und wiederholt werden (Schneeballsystem).

pasis

tüpass
Patientensicherheit und Simulation

PaSIS Kostenplan

(alle Angaben zzgl. MwSt.)

Einmalige Kosten zum Systemstart

Pos.	Bezeichnung	Menge	Einzelpreis	Betrag
1	Aufsetzen der Systemstruktur 1 Verbund 1 Klinik / Organisation 1 Meldekreis 1 Qualitätsmanagement-Account 1 Beauftragten-Account 1 Melder-Account	Pauschale	450,00 €	450,00 €
2	Schulung der Beauftragten Schulung der Beauftragten im Tüpass (3 Beauftragte, 150,00€ pro Person)	3	150,00 €	450,00 €
		Summe netto		900,00 €
		MwSt. 19%		171,00 €
		Gesamtbetrag		**1071,00 €**

Laufende monatliche Kosten

Pos.	Bezeichnung	Menge	Einzelpreis	Betrag
1	Teilnahmegebühren Rettungswagen 1 Rettungswagen (24h / 7d pro Woche)	1	203,00 €	203,00 €
2	Teilnahmegebühren Krankentransportwagen 1 Krankentransportwagen (24h / 1d pro Woche)	1	14,50 €	14,50 €
3	Software-Lizenzen PaSIS V5	Pauschale	0,00 €	0,00 €
4	Software-Updates PaSIS V5	Pauschale	0,00 €	0,00 €
5	Server-Wartung und –Administration	Pauschale	0,00 €	0,00 €
		Summe netto		217,50 €
		MwSt. 19%		41,33 €
		Gesamtbetrag		**258,83 €**

Kostenplan Details: Einmalige Kosten

Die Schulung der Beauftragten kann wahlweise im Tüpass oder vor Ort erfolgen.
Die Kosten für die Schulung der PaSIS-Beauftragten im Tüpass betragen 150,00 € pro teilnehmender Person.

Häufig vereinbaren wir eine Vor-Ort-Schulung und berechnen dafür pauschal 950,00 € pro Tag zzgl. Reisekosten für die Schulung der Beauftragten. So lässt sich auch eine größere Anzahl von Beauftragten effektiv und durch Wegfall der Reisekosten ihrer Mitarbeiter kostengünstig in die Benutzung des Systems einweisen.

Optional kann eine Einführungsveranstaltung für die Gesamtorganisation gebucht werden.
Die Einführungsveranstaltung kostet 450,00 € zzgl. Reisekosten (2 Personen) (bei Buchung in Kombination mit Vor-Ort-Schulung der Beauftragten, werden Reisekosten nur einmalig berechnet).

Bei der Einführung von PaSIS werden Ihnen Vorlagen für einige erforderliche Dokumente zur Verfügung gestellt (Sanktionsfreiheits-Erklärung, Schweigepflicht, Datenschutz etc.).

Für das Aufsetzen der Systemstruktur, die Eingabe der Kontaktdaten der PaSIS-Beauftragten und Einrichtung einer organisationsspezifischen Startseite wird eine einmalige Gebühr von 450,00 € berechnet.

Die Neuanlage eines Accounts (Standard-Benutzer / Beauftragter / Qualitätsmanager) in PaSIS kostet pauschal 25 Euro pro Account. Hierbei spielt es keine Rolle ob der Account in einer bereits existierenden Organisationseinheit angelegt wird, oder ob die Organisationseinheit ebenfalls neu angelegt werden muss.

Für den aktiven Betrieb von PaSIS wird die Benennung und Schulung von PaSIS-Beauftragten in jeder Abteilung / in jedem Meldekreis in ausreichender Anzahl empfohlen. Hierbei hat sich in der Praxis bewährt, das Team interprofessionell zusammenzustellen, um die Akzeptanz des Systems zu steigern.

Optional können vom TüPASS eine oder mehrere Einführungsveranstaltungen („Kick-Off“) für alle Mitarbeiter durchgeführt werden. Diese kann im Zusammenhang mit der Schulung oder unabhängig davon durchgeführt werden.

Die vom Tüpass durchgeführten PaSIS-Schulungen haben in der Regel eine Dauer von 6-7 Stunden und beinhalten die Grundlagen zum Verständnis und zum aktiven Arbeiten mit dem System (es wurden bereits über 300 Beauftragte geschult). Zusätzlich werden bei der PaSIS-Schulung frei veränderbare Präsentationen (Powerpoint-Dateien) zur internen Weiterschulung zur Verfügung gestellt.

Kostenplan Details: Laufende Kosten:

Tüpass übernimmt die Anonymisierung der eingehenden Ereignisse im 4-Augen-Prinzip (2 stufiges Verfahren, 2 Mitarbeiter unseres Teams anonymisieren die eingehenden Ereignisse unabhängig und asynchron).

Tüpass übernimmt die fachgerechte Analyse der gemeldeten Ereignisse. Die Beauftragten Ihrer Organisation stehen für Tüpass bei Rückfragen zur Analyse zur Verfügung.

Für die Anonymisierung nach 4-Augen-Prinzip und die Analyse der Ereignisse entstehen Ihrer Organisation keine weiteren Kosten. Diese werden durch die monatlichen Teilnahmegebühren gedeckt.

In den genannten Beträgen, adaptiert auf Ihre Größe, sind sämtliche laufende Kosten für den Betrieb von PaSIS eingeschlossen. Für die Nutzung der Software (Software-Lizenzen) fallen keine weiteren Gebühren an.
Ein Investitions- oder Softwareinstallationsaufwand ist nicht nötig, weder in Hardware noch in Software, ein gewöhnlicher Internetzugang ist die einzige Voraussetzung zur Teilnahme.
Das Hosting der PaSIS-Software übernimmt Tüpass, ebenso wird die Wartung und Administration des Servers von Tüpass unentgeltlich durchgeführt. Tüpass steht in üblichem Umfang kostenlos für Rückfragen (E-Mail / Telefon) kostenlos zur Verfügung.

Als Maßzahl für die erwartete mittlere Anzahl an Meldungen zur Anonymisierung und Analyse dient als einfache Berechnungsgrundlage die Anzahl der im Einsatz befindlichen Fahrzeuge für Rettung- und Transport.

Da bei Krankentransportwagen sowohl die zu erwartende Anzahl an Meldungen weniger ist, als auch die anzusetzende Analysetiefe und Komplexität der Ereignisse als geringer eingeschätzt wird, setzen wir hier nur 50% der üblichen Kosten für einen Rettungswagen / Notarzteinsatzfahrzeug / Ähnliches an.

Rettungswagen / Notarzteinsatzfahrzeug oder Ähnliches	203,00 € zzgl. MwSt. pro Monat
Krankentransportwagen oder Ähnliches	101,50 € zzgl. MwSt. pro Monat

Die PaSIS Plattform ist über eine verschlüsselte Verbindung jederzeit sowohl von der Klinik, wie auch von zu Hause aus, für Ereignismeldungen oder Fallbearbeitungen erreichbar.

Der Betrag für den Betrieb von PaSIS kann je nach Anzahl eingehender Meldung in gegenseitigem schriftlichen Einvernehmen alle 6 Monate nach oben oder unten korrigiert werden. Die Teilnahme an PaSIS ist jederzeit zum Monatsende von beiden Seiten kündbar.

pasis

tüpass
Patientensicherheit und Simulation

Bestellformular PaSIS-Schulungen

Mit diesem Formular können Sie Schulungen (Beauftragtenschulung / Einführungsveranstaltung) für die Mitarbeiter Ihrer Organisation bei TüPASS beantragen.

Kontakt für die Planung der Schulungen vor Ort

Name, Vorname	Titel	Beruf	Adresse	Email	Telefon

Angaben zu Ihren gewünschten Schulungen

Welche Schulung wollen sie buchen?	Örtlichkeit der Veranstaltung (Straße / Hausnummer / PLZ / Stadt / Land)	Wunschdatum (MM.JJJJ)
☐ Beauftragtenschulung ☐ Einführungsveranstaltung		
☐ Beauftragtenschulung ☐ Einführungsveranstaltung		

Beauftragtenschulung:
150 € pro Person oder als
Vor-Ort-Schulung pauschal 950 € zzgl. Reisekosten
(2 Personen)

Einführungsveranstaltung für die Gesamtorganisation:
450 € zzgl. Reisekosten (2 Personen)
(bei Buchung in Kombination mit Vor-Ort-Schulung der Beauftragten, werden Reisekosten nur einmalig berechnet)

Senden sie das ausgefüllte Formular bitte per Fax oder auf dem Postweg an TüPASS. Wir melden uns zur genauen Absprache der Schulungstermine bei Ihnen.

PaSIS
c/o TüPASS
Tübinger Patientensicherheits-
und Simulationszentrum
Silcherstraße 5
72076 Tübingen

Tel. +49 (0)7071 / 29 86733
Fax +49 (0)7071 / 29 4943

Hiermit beauftrage ich die Durchführung der oben aufgeführten Schulungen:

_____ _____

Ort, Datum Unterschrift