Dienstvereinbarung

zwischen dem

Universitätsklinikum Heidelberg („Klinikum“)

und

dem Gesamtpersonalrat

des Universitätsklinikums Heidelberg („Gesamtpersonalrat“)

über den

Einsatz des SAP Security Monitors und die Protokollierung des Zugriffs auf den Patientenorganizer in IS-H/i.s.h.med

Präambel

Der Einsatz von Protokollierungen der Zugriffe auf Patientendaten im SAP-System IS-H/i.s.h.med im Universitätsklinikum Heidelberg dient der Umsetzung datenschutzrechtlicher Anforderungen, der Gewährleistung schutzwürdiger Belange der Beschäftigten und Dritter wie z.B. Patienten sowie der Wahrung berechtigter Interessen des Universitätsklinikums.

Es ist erklärtes Ziel beider Vertragspartner, dass die Möglichkeiten der Überwachung der Systemnutzung durch Beschäftigte und Geschäftspartner[1] des Klinikums ausschließlich dazu dienen sollen, Verstöße gegen datenschutzrechtliche Regelungen zu verhindern und festzustellen, insbesondere unzulässige Zugriffe auf Patientendaten. Die Rechte der Beschäftigten/Nutzer des o.g. Systems bleiben durch die Protokollierungen und Auswertungen gewahrt; ein Eingriff erfolgt nicht ohne sachlichen Grund.

Ein weiteres Ziel ist es, auch Beschäftigten, die sich als Patienten in das Klinikum begeben, einen erweiterten Schutz zu gewähren. Dies geschieht insbesondere durch die Möglichkeit der Protokollierung und Auswertung von Zugriffen, die nicht im Behandlungskontext stattfinden und die allgemeine Bekanntgabe dieser Möglichkeit.

Beide Parteien wirken durch diese Dienstvereinbarung darauf hin, dass dem Schutz des allgemeinen Persönlichkeitsrechts Betroffener in allen Belangen Rechnung getragen wird.

Soweit möglich werden im Folgenden geschlechtsneutrale Formulierungen verwendet; wo dies nicht geschah dient dies der besseren Lesbarkeit der Regelungen, ist aber bitte geschlechtsneutral zu lesen.

[1] Z.B. durch Servicefirmen oder Kooperationspartner

§ 1 Begriffsbestimmungen

(1) Der SAP Security Monitor („Security Monitor“) im Sinne dieser Dienstvereinbarung ist eine Anwendungssoftware zur Protokollierung und Überwachung der Nutzungsvorgänge in SAP-Systemen (hier: IS-H/i.s.h.med). Das Programm protokolliert die Nutzung von SAP-Modulen an der Schnittstelle des User-Interfaces.

(2) Der Patientenorganizer ist die zentrale Transaktion der Klinischen Dokumentation im SAP-System IS-H/i.s.h.med. Er stellt nahezu alle verfügbaren klinischen und administrativen Informationen zu einem Patienten bereit. Protokolliert werden dabei Zugriffe, bei denen systemseitig zum Zeitpunkt des Zugriffs eine aktuelle Beteiligung der Fachabteilung des Nutzers an der Versorgung des Patienten nicht festgestellt werden kann, der Nutzer aber die dienstliche Erforderlichkeit des Zugriffs durch Auswahl bzw. Eingabe einer Begründung in einem PopUp-Fenster bestätigt.

(3) Datenschutzteam: Der Datenschutzbeauftragte und seine unmittelbare Mitarbeiterin im Klinikum.

(4) Datenschutzkontrolle im Sinne dieser Dienstvereinbarung sind die Maßnahmen zur Feststellung und Prävention unzulässiger Zugriffe auf Patientendaten.

(5) Betroffene im Sinne dieser Dienstvereinbarung sind Personen, deren Daten im System SAP IS-H/i.s.h.med verarbeitet werden.

§ 2 Gegenstand und Geltungsbereich

Diese Dienstvereinbarung gilt für die Einführung und den Betrieb des SAP Security Monitors im System SAP IS-H/i.s.h.med, die Nutzung der Protokollierung der Zugriffe auf den Patientenorganizer im System IS-H/i.s.h.med im Universitätsklinikum Heidelberg und für die Zugriffe aller Beschäftigten und sonstigen Nutzer, die im Bereich des Universitätsklinikums Heidelberg tätig sind, auf diese Systeme.

§ 3 Zulässigkeit und gesetzliche Anforderungen

(1) Bei den Protokollierungen handelt es sich um Daten zur Datenschutzkontrolle. Sie dürfen damit nach § 15 Abs.1 des Landesdatenschutzgesetzes („zulässig zur Aufgabenerfüllung“) i.V.m § 15 Abs.3 Landesdatenschutzgesetz („Wahrnehmung von Kontrollbefugnissen“) gespeichert und genutzt werden.

(2) Personenbezogene Daten der Nutzer zu Zwecken der Datenschutzkontrolle dürfen nach § 15 Abs.4 Landesdatenschutzgesetz (LDSG) „nur für diesen Zweck und hiermit in Zusammenhang stehende Maßnahmen gegenüber Bediensteten genutzt werden.“

(3) Beschäftigte, die als Patient im Klinikum versorgt werden, sollen erfahren dürfen, welche andere Beschäftigten unzulässigerweise auf ihre medizinischen Daten in SAP IS-H/i.s.h.med zugegriffen haben. Diese Dienstvereinbarung stellt hierfür die Rechtsgrundlage dar (im Sinne von § 36 Abs.1 LDSG, („vorgesehen durch eine Dienstvereinbarung“).

(4) Die Landesbeauftragten für den Datenschutz fordern heute schon eine Protokollierung aller Zugriffe auf Patientendaten[2] sowie deren stichproben- und anlassbezogene Auswertung. Damit sollen unrechtmäßige Zugriffe/Datenmissbrauch im Sinne von Datengeheimnis und Schweigepflicht festgestellt und verfolgt werden können. Allerdings fordern sie auch, dass die Protokollierung auf das erforderliche Maß eingeschränkt wird.

(5) Nach § 9 Abs. 3 Nr. 5 LDSG muss sichergestellt werden, dass Nutzer nur aufgabengerecht auf Patientendaten zugreifen können („Zugriffskontrolle“). Wo der Zugriff auf Patienten potenziell möglich sein muss (z.B. wegen Konsilen, Notfällen oder Sonderaufgaben) und daher der Zugriff nicht komplett verwehrt werden muss eine Absicherung des Zugriffs durch eine Protokollierung erfolgen.

(6) Nach einem Gerichtsurteil des Europäischen Gerichtshofs für Menschenrechte liegt in der fehlenden Protokollierung von lesenden Zugriffen auf medizinische Daten ein Verstoß gegen Artikel 8 der Europäischen Menschenrechtskonvention vor.[3]

§ 4 Grundsätze

(1) Neben dieser Vereinbarung sind sonstige datenschutzrechtliche Regelungen, sowie gesetzliche Verschwiegenheitsverpflichtungen zu beachten.

(2) Zweckbestimmung, Zweckbindung: Der Einsatz des Security Monitors und die Nutzung der Protokollierung beim Zugriff auf den Patientenorganizer dienen ausschließlich der Datenschutzkontrolle und der rechtskonformen Nutzung des System SAP IS-H/ i.s.h.med. Ausdrücklich ausgeschlossene Zwecke:

   a. Leistungskontrolle oder sonstige Verhaltenskontrolle der Beschäftigten.

   b. Der Betrieb wird auf keine weiteren Module ausgedehnt.

§ 5 Verarbeitete Beschäftigtendaten

Die erhobenen und gespeicherten Daten werden - soweit es der Zweck der Zugriffskontrolle erlaubt und es technisch möglich ist - in ihrem Umfang so weit wie möglich eingeschränkt.

§ 6 Speicherung und Auswertung

(1) Speicherung: Die Speicherung protokollierter Daten erfolgt ausschließlich zum Erreichen eines der in § 4 Abs. 2 genannten Zwecke.

(2) Auswertung:

   a. Der vereinbarte Prozess der Auswertungen durch das Datenschutzteam ist in der Prozessbeschreibung in Anlage 1 dokumentiert.

   b. Bei Auftreten von technischen Problemen können Service-Techniker der systembetreuenden (externen) Firmen hinzugezogen werden. Diese müs-

[2] Siehe Orientierungshilfe zu Zugriffsrechten in Klinischen Informationssystemen der Bundes-/Landesbeauftragten (März 2011)

[3] ECHR, Application No. 20511/03 v. 17.10.2008. – Case of I v. Finland

sen auf das Datengeheimnis und einzuhaltenden Datenschutzmaßnahmen bei diesen Wartungsarbeiten verpflichtet sein.

c. Alle Zugriffe auf die Daten sind in einem Protokoll mit Begründung zu dokumentieren (siehe Muster in Anlage 2).

§ 7 Technische und organisatorische Maßnahmen

(1) Zugriffsregelungen: Zugriff auf die Protokolldaten erhalten durch entsprechende Systemeinstellung ausschließlich

a. das Datenschutzteam des Klinikums,

b. die zuständigen eingewiesenen Systembetreuer (Basis und Applikation) des ZIM.

(2) Diese Personen werden auf die Einhaltung der Festlegungen dieser Dienstvereinbarung sowie auf die Einhaltung der datenschutzrechtlichen Vorschriften schriftlich verpflichtet.

(3) Löschfristen:

a. Die Protokolldaten sind grundsätzlich im 13. Monat nach ihrem Entstehen zu löschen. Evtl. länger verfügbare Daten aus Sicherungskopien gelten als gesperrt und dürfen nicht über den Zeitraum nach Satz 1 hinaus genutzt werden.

b. Ausnahmen zu Punkt a. sind Protokolldaten, die Gegenstand des Klärungs- und –Verfolgungsprozesses in Zusammenhang mit einem vermuteten und dokumentierten Verstoß sind. Diese dürfen aufbewahrt werden soweit dies für Klärung und Verfolgung und Nachweis eines Verstoßes erforderlich ist oder gesetzliche Aufbewahrungsfristen dies erfordern.

§ 9 Rechte Beschäftigter als Systemnutzer

Betroffene Nutzer haben stets das Recht, Auskunft über die zu ihrer Person als Nutzer gespeicherten Daten Auskunft oder Einsicht zu erhalten.

§ 10 Verfahren bei vermuteten Verstößen

(1) Soweit das Datenschutzteam aufgrund seiner Prüfungserkenntnisse einen Verstoß gegen Regelungen des Datenschutzrechts, der Schweigepflicht oder verbindlichen Klinikumsregelungen für wahrscheinlich hält, kann es diese Fälle an den dafür zuständigen Ansprechpartner in der Personalabteilung mit den relevanten Protokolldaten und vorhandenen Informationen zum Fall weitergeben.

(2) Der zuständige Ansprechpartner in der Personalabteilung beruft einen Arbeitskreis ein, der aus folgenden Personen besteht:

a. der zuständige Ansprechpartner in der Personalabteilung bzw. dessen Stellvertreter und

b. ein/e Vertreter/in des Gesamtpersonalrats und

c. der Datenschutzbeauftragte oder seine Stellvertretung sowie

d. der Rechtsabteilung, Bereich Arbeitsrecht.

(3) Dieser Arbeitskreis erörtert unter Berücksichtigung aller Fakten den Fall. Soweit aufgrund der Begleitumstände des Falles ein eindeutiger Entlastungsnachweis des Nutzers durch gespeicherte Daten, Dokumentation oder Zeugenaussagen nicht möglich ist gilt der Grundsatz in „dubio pro reo“; in diesem Fall wird der Vorgang nicht weiter verfolgt.

(4) Soweit sich Hinweise auf einen Verstoß verdichten kann der betroffene Nutzer vorgeladen und befragt werden. Zur Befragung sowie zur weiteren Erörterung kann der Vorgesetzte des betroffenen Nutzers hinzugezogen werden soweit dies der Arbeitskreis mehrheitlich (einfache Mehrheit) für erforderlich oder sinnvoll hält.

(5) Nach Anhörung des betroffenen Nutzers beschließt der Arbeitskreis mehrheitlich (einfache Mehrheit) ob der festgestellte Sachverhalt an die Personalverwaltung weitergeleitet wird um ggf. disziplinarische bzw. arbeitsrechtliche Maßnahmen (wie etwa Ermahnung, Abmahnung oder Kündigung) einzuleiten. Der Arbeitskreis kann dies mit einer Empfehlung verbinden.

§ 11 Weitere Rechte des Gesamtpersonalrates

(1) Der Gesamtpersonalrat hat das Recht, die Einhaltung dieser Dienstvereinbarung zu überprüfen. Er hat dazu insbesondere das Recht die Dokumentation der getätigten Zugriffe auf die Protokolldaten einzusehen.

(2) Der Gesamtpersonalrat wird rechtzeitig vor wesentlichen Änderungen am Programm oder Einsatz des Security Monitors sowie der Protokollierung beim Zugriff auf den Patientenorganizer informiert.

(3) Rechtzeitig i.S.d. Abs. 2 bedeutet, dass die Information zu einem Zeitpunkt erfolgt, zu dem der Arbeitgeber intern und Dritten gegenüber noch keine bindenden Festlegungen getroffen hat, so dass die Vorschläge und Anregungen des Gesamtpersonalrates noch eingearbeitet werden können. In der Regel wird dem Gesamtpersonalrat eine Anhörungsfrist vom Zeitpunkt der Information an von 4 Wochen eingeräumt werden.

§ 12 Bekanntmachung der Dienstvereinbarung und der Prozesse

(1) Die Protokollierungs- und Auswertungsvorgänge sind klinikumsweit allgemein bekannt zu machen. Ebenso in einer regelmäßigen Meldung für die Systemnutzer. Hiermit soll eine Sensibilisierung bezüglich unzulässiger Zugriffe insbesondere auf Daten von Kolleginnen und Kollegen erreicht werden.

(2) Die Dienstvereinbarung ist allen betroffenen Beschäftigten zugänglich zu machen.

§ 13 Personalmaßnahmen

Maßnahmen gegen Beschäftigte, die unter Verstoß oder Umgehung gegen die Regelungen dieser Dienstvereinbarung getroffen werden, sind unzulässig.

§ 14 Salvatorische Klausel

Sollten Bestimmungen dieser Dienstvereinbarung ganz oder teilweise unwirksam sein oder werden, so wird dadurch die Wirksamkeit der Dienstvereinbarung im Übrigen nicht berührt. Die Parteien werden eine unwirksame Bestimmung durch eine Bestimmung ersetzen, die der unwirksamen Bestimmung am ehesten entspricht. Kommt hierüber keine Einigung zustande, so gilt diejenige wirksame Bestimmung als vereinbart, die dem Sinn und Zweck der unwirksamen Bestimmung am nächsten kommt.

§ 15 Änderungen der Dienstvereinbarung

(1) Ergeben sich aus der Anwendung dieser Vereinbarung neue Regelungsbedarfe oder wird die Verletzungen von Regelungen dieser Vereinbarung festgestellt, so werden auf Antrag einer Vertragspartei Verhandlungen aufgenommen mit dem Ziel einer einvernehmlichen Regelung.

(2) Änderungen und Ergänzungen dieser Dienstvereinbarung bedürfen zu ihrer Rechtswirksamkeit der Schriftform.

§ 16 Inkrafttreten, Geltungsdauer, Kündigung

(1) Diese Dienstvereinbarung tritt mit Wirkung vom **01.01.2014** in Kraft. Sie wird auf unbestimmte Zeit beschlossen.

(2) Fristgerechte Kündigung: Die Dienstvereinbarung kann von jeder Vertragspartei mit einer Frist von 3 Monaten zum Ende eines Kalenderhalbjahres gekündigt werden. Bis zum Abschluss einer neuen Dienstvereinbarung gilt die bisherige Dienstvereinbarung weiter, soweit nicht Rechtsvorschriften entgegenstehen oder sich die Vertragsparteien auf eine vorläufige Regelung einigen.

Heidelberg, tt.mm.2013

Irmtraut Gürkan	Helmut Beck
Kaufmännische Direktorin	Vorsitzender Gesamtpersonalrat

Anlage 1

Auswertungsprozess Datenschutzteam

1. Übersicht über die verschiedenen Auswertungsverfahren:

(1) **Kriterienverfahren**

(2) **Stichprobeverfahren**

(3) **Patientenschutzverfahren** (Bei Nachfrage von Patienten bezüglich des Zugriffes auf ihre Daten)

2. Kriterienverfahren

(1) Das Kriterienverfahren ist ein Verfahren, in dem über den verfügbaren (noch nicht gelöschten) Gesamtprotokollbestand hinweg anhand von Kriterien (siehe dazu Abs. 2) die Rechtmäßigkeit und Plausibilität von Zugriffen geprüft wird.

(2) Das Datenschutzteam darf den Protokollgesamtdatenbestand oder Auszüge daraus auf datenschutzrelevante Auffälligkeiten hin prüfen, insbesondere in folgenden Fällen:

a. Unplausible Fachrichtungszugriffe (z.B. Neurochirurgie auf Frauenklinik)

b. Fälle auffällig häufiger fachabteilungsübergreifender Zugriffe durch einen Nutzer (Sortierung nach der Anzahl der Zugriffe im Prüfzeitraum)

c. Fälle nicht sachgemäßer Eingaben bei der Begründung des Zugriffs auf den Patientenorganizer (z.B. sinnlose Buchstabenfolgen, Quatsch, Flüche).

(3) Das Datenschutzteam kann die betroffenen Nutzer um Stellungnahme bitten. Diese haben die Anfragen zu beantworten.

(4) Soweit die Ursache für auffällige Zugriffe in der nicht korrekten Zuweisung der Zugriffsrechte liegt, wirkt das Datenschutzteam auf eine entsprechende Anpassung der Einräumung der Zugriffsrechte hin.

3. Stichprobeverfahren

(1) Das Stichprobeverfahren findet bis zu 5 Mal im Jahr statt.

(2) Das Datenschutzteam wählt bei diesem Verfahren 5 zufällige Einträge aus.

(3) Es informiert die betroffenen Nutzer über die Auswahl.

(4) Es informiert die Fachabteilung, auf deren Daten zugegriffen wurde über den Zugriff eines (nicht namentlich genannten) Nutzers.

(5) Die betroffene Fachabteilung kann bei Bedarf vermutete unzulässige Zugriffe zurückmelden. Diese werden nach den Maßgaben dieser Dienstvereinbarung weiter verfolgt.

(6) Die Stichprobenfälle liegen bei Anfrage an die Betroffenen maximal 3Tage zurück.

4. Anfrage von Patienten (auch Beschäftigten als Patienten)

(1) Das Datenschutzteam wertet die vorhandenen Zugriffe auf die Patientendaten der betreffenden Person (bzw. der von ihr gesetzlich Vertretenen, z.B. Kinder oder Betreute) aus.

(2) Es prüft soweit möglich die Plausibilität des Behandlungszusammenhangs der zugreifenden Nutzer und ihrer Fachabteilungen.

(3) Es fordert bei Bedarf beim betroffenen Nutzer eine Stellungnahme an.

(4) Es informiert den Anfrager, ob ein möglicherweise unzulässiger Zugriff festgestellt wurde oder nicht, sowie ggf., dass der Verstoß klinikumsintern verfolgt wird.

(5) Beschäftigte als Patienten werden informiert, dass Sie nach Abschluss des Verfahrens gemäß Dienstvereinbarung § 10 Abs. 5 über das Ergebnis sowie bei einem erwiesenen Verstoß über die Identität des Nutzers informiert werden.

6. Anfrage sonstiger Stellen oder Personen

Das Datenschutzteam kann gemäß Nr.4 und Nr. 6 auch auf Hinweis oder Nachfrage anderer Stellen oder Beschäftigter des Klinikums oder auch Externer tätig werden. Eine Information dieser Stellen über die Erkenntnisse erfolgt aber nicht.

7. Nachweis durch Nutzer

(1) Nutzer können die Erforderlichkeit und Zulässigkeit ihres Zugriffs bzw. ihren Behandlungsauftrag durch schriftliche oder digitale Dokumentation zum betreffenden Patienten sowie Einträge in der Dienstplanung nachweisen.

(2) Soweit ein Nachweis aufgrund einer Dokumentation nicht möglich ist hat der Nutzer eine Begründung in Textform (Brief oder Mail) abzugeben.

Anlage 2

Zugriffe Protokollierung - Dokumentation		
Datum	<tt.mm.20nn>	Namen
Zugriff durch (Name, Bereich)	❑ Zugriffsberechtigte der ZIM-Systembetreuung ❑ Datenschutzteam ❑ Hinzugezogene externe Servicetechniker	
Anlass/Zweck kurz	❑ Routineprüfung ❑ Anfrage eines Betroffenen ❑ Anfrage anderer Personen/Stellen ❑ Sonstiges: _____	
Ergänzende Informationen zu Anlass/Zweck		
Vorgehen gem. Dienstvereinbarung	❑ Kriterienverfahren ❑ Stichprobeverfahren ❑ Patientenschutzverfahren	
Zugriffsumfang (Kurzbeschreibung)	<Geprüfter Zeitraum und Datenumfang grob, z.B. Alle Zugriffe für Kriteriensortierung oder Stichprobe 5 Zugriffe oder Alle Zugriffe auf Fälle des Anfragers. >	

Heidelberg, tt.mm.20nn

<z.B. Schurer, DSB>

Dokumentierende Person
Name, Bereich, Funktion Klartext

1. z.d.A. DSB-Verzeichnis Audit\Zugriffskontrollen