Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Gesundheitspolitik

Formular für Stellungnahme zur Anhörung Ausführungsrecht zum Bundesgesetz über das elektronische Patientendossier EPDG

Stellungnahme von

Name / Kanton / Firma / Organisation	: **Information Security Society Switzerland**
Abkürzung der Firma / Organisation	: **ISSS**
Adresse, Ort	: Bollwerk 21, 3011 Bern
Kontaktperson	: Dr. Ursula Widmer, Rechtsanwältin, Past President ISSS / Leitung ISSS Task Force Ausführungsvorschriften EPDG
Telefon	: +41 31 351 66 33 / +41 79 300 32 38
E-Mail	: ursula.widmer@widmer.ch
Datum	: 28. Juni 2016

Hinweise

1. Bitte dieses Deckblatt mit Ihren Angaben ausfüllen.
2. Bitte für jede Verordnung das entsprechende Formular verwenden.
3. Pro Artikel der Verordnung eine eigene Zeile verwenden
4. Ihre elektronische Stellungnahme senden Sie bitte als Word-Dokument bis am **29. Juni 2016** an eHealth@bag.admin.ch

1 Ausführungsrecht zum Bundesgesetz über das elektronische Patientendossier EPDG

Allgemeine Bemerkungen zu den Erlasstexten

Sehr geehrte Damen und Herren

ISSS bedankt sich für die Gelegenheit, im Rahmen der Vernehmlassung für das Ausführungsrecht zum Bundesgesetz über das elektronische Patientendossier Stellung nehmen zu können.

Die Information Security Society Switzerland (ISSS; http://www.isss.ch) ist der führende Fachverband in der Schweiz auf dem Gebiet der ICT-Sicherheit, welchem heute mehr als 1100 Einzel- und Firmenmitglieder aus Wirtschaft, Verwaltung und Wissenschaft angehören. ISSS setzt sich mit den technischen, wirtschaftlichen, regulatorischen und gesellschaftspolitischen Aspekten von ICT-Sicherheit und Informationsschutz auseinander. ISSS ist offizieller ICT Security Fachpartner von SwissICT.

Die ISSS Stellungnahme beschränkt sich auf diejenigen Punkte der Entwürfe des Ausführungsrechts zum Bundesgesetz über das elektronische Patientendossier, welche im Zusammenhang mit der ICT-Sicherheit und dem Datenschutz stehen. ISSS äussert sich daher nur zur EPDV und TOZ.

Der ICT-Sicherheit und dem Datenschutz kommen für den Erfolg des ePatientendossiers entscheidende Bedeutung zu. Dies gilt umso mehr, als die Nutzung des ePatientendossiers sowohl für die Patienten als auch für die Gesundheitsfachpersonen (ausgenommen Spitäler und Heime) freiwillig ist.

Es ist jedoch bei den Detailregelungen auf der Ebene der Ausführungsvorschriften darauf zu achten, dass es zu keiner Überregulierung kommt, welche einen zu grossen technischen und organisatorischen Aufwand erfordert und welche die Gesundheitsfachpersonen bzw. deren Gemeinschaften sowie die Patienten in der praktischen Handhabung des ePatientendossiers zu stark behindert und praktikable Lösungen unnötig erschweren würde. Das wäre nicht nur generell der verbreiteten Nutzung des ePatientendossiers abträglich, sondern wäre auch für die Sicherstellung der ICT-Sicherheit nicht förderlich, da eine zu grosse Komplexität immer auch mit Sicherheitsrisiken verbunden ist.

Wir hoffen, dass wir mit unserer Stellungnahme einen Beitrag zur Förderung der ICT-Sicherheit und dem Informationsschutz im Medizinalbereich der Schweiz leisten können und danken Ihnen für die Berücksichtigung unserer Anträge, welche wir Ihnen, wenn immer möglich, zu Ihrer Unterstützung gleich als ausformulierte Textvorlage mit dazugehöriger Begründung einreichen.

An der ISSS Stellungnahme haben folgende ISSS Mitglieder mitgearbeitet (in alphabetischer Reihenfolge):

Konrad Bähler, Dr. Widmer & Partner, Rechtsanwälte
Petra Breitling, Spital Thurgau AG
Philine Brinkmann, Swisscom (Schweiz) AG
Dr. Daniel Burgwinkel, Kompetenzzentrum Records Management GmbH
Robert De Brot, Arvernus Consulting
Dr. Peter E. Fischer, Institut für Wirtschaftsinformatik Hochschule Luzern
Hans Herriger
Beat Lehmann, Alcan Holding Switzerland AG
Doron Moritz, Tessaris Integrated Security AG
Peter Nussbaumer, MediatorIT
Thomas Reich, Post AG
Fridel Rickenbacher, MIT-Group
Carl Rosenast, QuoVadis Trustlink Schweiz AG
Simon Schneiter, NTT Com Security
Thomas Selzam, Berner Fachhochschule
Steven Stalder, Redguard AG
Dr. Ursula Widmer, Dr. Widmer & Partner, Rechtsanwälte

Freundliche Grüsse

Dr. Ursula Widmer, Rechtsanwältin, Past President ISSS / Leitung ISSS Task Force Ausführungsvorschriften EPDG

Allgemeine Bemerkungen zu den Erläuterungen

Keine Kommentare

2 BR: Verordnung über die Finanzhilfen für das elektronische Patientendossier EPDFV

Allgemeine Bemerkungen

Keine Kommentare

Bemerkungen zu einzelnen Artikeln

Artikel	Kommentar	Änderungsantrag

Bemerkungen zu den Erläuterungen

Seite / Artikel	Kommentar	Änderungsantrag

3 BR: Verordnung über das elektronische Patientendossier EPDV

Allgemeine Bemerkungen

Es werden von ISSS nur Kommentare und Anträge mit direktem oder indirektem Bezug zu ICT-Sicherheit / Datenschutz gemacht,

Bemerkungen zu einzelnen Artikeln

Artikel	Kommentar	Änderungsantrag
Art. 2 Abs. 2	Im Hinblick darauf, dass der Patient die Möglichkeiten zur Zuweisung von Zugriffsrechten an Gruppen von Gesundheitsfachpersonen bzw. den Ausschluss einzelner Gesundheitsfachpersonen (einer Gruppe) praktisch wahrnehmen kann, ist ihm von den Gemeinschaften jeweils eine Liste der in Frage kommenden Gesundheitsfachpersonen vorzulegen.	Neuer Absatz 2 (die bisherigen Absätze 2-5 werden zu Absatz 3-6): Patienten muss auf Verlangen von den Gemeinschaften eine Personalliste vorgelegt werden, damit Patienten über die Zuweisung von Zugriffsrechten an Gesundheitsfachpersonen oder Gruppen von Gesundheitsfachpersonen sowie über den Ausschluss einzelner Gesundheitsfachpersonen vom Zugriff entscheiden können.
Art. 9 Abs. 1 lit. d (neu)	Artikel 9 führt aus: „1 Gemeinschaften müssen sicherstellen, dass (c). Daten des elektronischen Patientendossiers nur in Ablagen gespeichert werden, die ausschliesslich dafür vorgesehen sind.“ Es werden keine Anforderung an die ordnungsgemässe Datenhaltung bzw. ein Nachweis der Integrität gefordert. Dies sollte mit aufgenommen werden, da andere Gesetze konkrete Vorgaben machen (z.B. GeBüV Art. 3). Auf Seite 16 der Erläuterungen wird hervorgehoben, dass das Patientendossier „Kopien“ enthält und die „Originale“ in den Archivsystemen der Primärsysteme gespeichert werden.	d. Daten des elektronischen Patientendossiers so aufbewahrt werden, dass ein Nachweis der Integrität möglich ist, d.h. eine nachträgliche Änderung der Daten lässt sich feststellen (z.B. durch Benutzer oder durch technische Fehlfunktionen oder Missbrauch/Cyberangriffe).

Bemerkungen zu einzelnen Artikeln		
Artikel	**Kommentar**	**Änderungsantrag**
	Aus Sicht der zukünftigen Prüfer ist deshalb der Nachweis der Integrität aus zwei Aspekten wichtig: (a) Nachweis, dass Integrität der Daten im Dossier gewährleistet ist (regelmässige Überprüfung) (b) Nachweis, dass Daten im Dossier mit Daten im Primärsystem übereinstimmen. In Ziff. 4.17.1 des Anhangs 2 zur EPDV-EDI wird nur von "besonders schützenswerten Daten“ gesprochen, die (a) verschlüsselt und (b) integritätsgeschützt werden müssen («4.17.1 Besonders schützenswerte Daten des elektronischen Patientendossiers müssen mit geeigneten und dem Stand der Technik entsprechenden kryptographischen Massnahmen verschlüsselt und integritätsgeschützt gespeichert werden.") • Es muss jedoch für alle Daten im Dossier der Nachweis der Integrität erfolgen, auch wenn nur ein Teil der Daten „besonders schützenswert“ ist und verschlüsselt wird. • Wenn nur ein Teil der Daten verschlüsselt und integritätsgeschützt gespeichert wird, kann nicht die Integrität des gesamten Dossiers nachgewiesen werden. • Andere Länder haben in ihrem eHealth System den Integritätsnachweis aller Daten umgesetzt (z.B. Estland, wo eHealth Dokumente mit Blockchaintechnologie abgesichert werden). Auch durch die in Ziff. 2.10 des Anhangs 2 zur EPDV-EDI vorgesehene Protokollierung der Bearbeitung der Daten im Dossier ist die Integrität nicht vollständig sichergestellt, z.B. dann nicht, wenn Daten aufgrund technischer Fehlfunktionen verändert werden.	

Bemerkungen zu einzelnen Artikeln		
Artikel	**Kommentar**	**Änderungsantrag**
Art. 11 Abs. 1 lit. b	Präzisierungsvorschlag	b. Ein System zur proaktiven Erkennung von und zum Umgang mit ~~Sicherheitsvorfällen~~Vorfällen im Bereich Angriffssicherheit und Betriebsausfallsicherheit;
Art. 11 Abs. 1 lit. c	Präzisierungsvorschlag	c. Ein Verzeichnis der Datenablagen, Berechtigungen und Prozesse zur Datensicherung und sicheren Aufbewahrung;
Art. 11 Abs. 1 lit. d	Präzisierungsvorschlag	d. Ein Verzeichnis der angeschlossenen Primärsysteme, welche direkten oder indirekten Zugang zu den Daten / Kommunikation haben oder erlangen können;
Art. 11 Abs. 3	Vorschlag auf Ergänzung durch die Anforderung der Anpassung an die Entwicklung der Bedrohungslage	Das EDI legt die Anforderungen in Bezug auf Datenschutz und Datensicherheit und deren Anpassung an die Entwicklung der Bedrohungslage fest.
Art. 11 Abs. 4	Präzisierungsvorschlag	[4] Die Datenleitungen, Datenverbindungen, Datenübermittlung, Datenspeicherung und Datenverarbeitung müssen sich in der Schweiz befinden und dem Schweizer Recht unterstehen.
Kap. 4 Überschrift	Korrekterweise müsste hier von einem elektronischen oder digitalen Identifikationsmittel die Rede sein.	4. Kapitel: Elektronisches Identifikationsmittel Art. 22: Anforderungen an das elektronische Identifikationsmittel

Art. 22 lit. a	Bei den elektronischen Identifikationsmitteln muss gewährleistet sein, dass diese von den Herausgebern zeitgerecht und in der geforderten Qualität und Menge zur Verfügung gestellt werden können. Dies ist dann möglich, wenn bereits heute bestehende anerkannte und zertifizierte Identifikationsmittel eingesetzt werden (**HPC, SuisseID, Mobile ID**) und nicht nach einem anderen Standard (ISO/IEC29115) neue Identifikationsmittel von den Herstellern gefordert werden. Dazu fehlt Zeit und Geld. Nebst den bereits existierenden elektronischen Identifikationsmitteln stehen in der Schweiz und in Europa die folgenden Mittel für eine sichere Authentisierung zur Verfügung: - **geregelte Zertifikate gemäss ZertES** - die abgeschlossene Totalrevision des Schweizerischen Signaturgesetzes (ZertES) beinhaltet neu geregelte Zertifikate, sowohl für natürliche Personen wie auch für Organisationen (Siegel). Diese geregelten Zertifikate wurden vorwiegend zum Zweck der Authentifizierung geschaffen. Diese Zertifikate werden ab Januar 2017 zur Verfügung stehen. - **eID** – das vorliegende Konzept von fedpol beinhaltet eine sichere Möglichkeit der Identifizierung/Authentifizierung auf Basis einer staatlich anerkannten elektronischen Identität. Von einer flächendeckenden Verbreitung der eID kann ausgegangen werden. Die Einführung der eID ist im 2020 geplant. - **eIDAS** – in allen europäischen Ländern gilt seit Juli 2014 die Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen. Bestandteil dieser gesetzlichen Regelung ist auch die Definition und Umsetzung der elektronischen Identifizierung.	a. Das Identifikationsmittel muss einer der folgenden Normen oder Vorschriften entsprechen: - Qualitätsstufe 3 der eCH-0170 Norm; - geregeltes Zertifikat gemäss ZertES; - SuisseID Authentisierungs-Zertifikat gemäss eCH-0113 Spezifikation - eIDAS

Bemerkungen zu einzelnen Artikeln		
Artikel	**Kommentar**	**Änderungsantrag**
	Alle diese existierenden und künftigen Identifikationsmittel richten sich nicht oder nur sehr bedingt nach der ISO/IEC29115 Norm. Wichtig zu erwähnen ist zudem, dass seit Juni 2014 der schweizerische eCH-Standard für den Umgang mit elektronischen Identitäten (eCH-0170 Qualitätsmodell für elektronische Identitäten) existiert. Dieser Standard wurde massgeblich für die Bereiche eGovernment und eHealth entwickelt. Sollte der eCH Standard den Ansprüchen des EPD nicht genügen, so muss mit eCH die Zusammenarbeit gesucht und entsprechende Änderungsanträge gestellt werden. eCH-0170 befindet sich derzeit in der Überarbeitung (Zusammenarbeit von eCH, BFH, IAM Bund, IDV Schweiz). Aus diesen Gründen sollten in erster Linie bestehende und bereits definierte elektronische Identifikationsmittel zur Anwendung kommen. Zusätzlich sollte der eCH Standard für die Definition von weiteren Identifikationsmittel massgeblich sein.	
Art. 23 Abs. 1	Die Definition der Anforderungen an die Identitätsprüfung sind Bestandteil der jeweiligen Norm/Regelung (eCH-0170, eCH-0113, ZertES, eIDAS).	[1] Der Herausgeber des elektronischen Identifikationsmittels muss die Identität der antragstellenden Person gemäss der jeweiligen Norm, unter der das Identifikationsmittel herausgegeben wird, überprüfen. Diese muss …
Art. 30 Abs. 1 lit. b	Präzisierungsvorschlag	b. sicherstellen, dass das Personal über die erforderlichen Fachkenntnisse, Erfahrungen, ~~und~~ Qualifikationen und anerkannte Zertifizierungen verfügt;

Bemerkungen zu einzelnen Artikeln		
Artikel	**Kommentar**	**Änderungsantrag**
Art. 30 Abs. 1 lit. c	Präzisierungsvorschlag in Ergänzung zu Art. 11 Abs. 4.	c. Informatiksysteme und -produkte verwenden, die vertrauenswürdig sind und zuverlässig in der Schweiz betrieben werden;
Bemerkungen zu den Erläuterungen		
Seite / Artikel	**Kommentar**	**Änderungsantrag**

4 EDI: Verordnung des EDI über das elektronische Patientendossier EPDV-EDI

Allgemeine Bemerkungen

Keine Kommentare

Bemerkungen zu einzelnen Artikeln

Artikel	Kommentar	Änderungsantrag

Bemerkungen zu den Erläuterungen

Seite / Artikel	Kommentar	Änderungsantrag

5 EDI: EPDV-EDI Anhang 1: Kontrollzifferprüfung

Allgemeine Bemerkungen

Keine Kommentare

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag

6 EDI: EPDV-EDI Anhang 2: Technische und Organisatorische Zertifizierungsvoraussetzungen (TOZ)

Allgemeine Bemerkungen

Es werden von ISSS nur Kommentare und Anträge mit direktem oder indirektem Bezug zu ICT-Sicherheit / Datenschutz gemacht.

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag
2.1	Hier ist die Rede von «Daten müssen vernichtet werden». Es ist unklar, was dies konkret bedeutet. Reicht z.B. das (elektronische) Löschen aus? Es ist daher zu präzisieren, nach welchen Vorgaben die Daten «vernichtet» werden müssen.	2.1.1.3 durch das in Ziff. 2.1.1.1-2.1.1.2 erwähnte Vernichten müssen die Daten kontrolliert und dokumentiert vollständig und unwiderruflich gemäss aktuellen Best Practice Regeln gelöscht werden.
2.6.1.2	Wie sollen diese Notfallzugriffe vor Missbrauch geschützt werden? Wie sieht hier die genannte manuelle Interaktion genau aus? Gibt es eine Art Notfall-Übersteuerung der Zugriffskontrolle und was sind die Anforderungen an diese?	Prozess detaillierter formulieren.
4.2.2.3	Via 4.2.2.3.1 und 4.2.2.3.2 und 4.2.2.3.3 und 4.2.2.3.5 sollten bewusst auch die Komponenten für die ICT-Fachdisziplinen wie Angriffssicherheit, Betriebsausfallsicherheit und System- und Daten-Backup abverlangt werden zur Awareness und Grundlage für Management Review / Auditierungen / Zertifizierungen	4.2.2.3 ein aktuell gehaltenes Inventar der folgenden Betriebsmittel (vgl. Kap. 4.8): 4.2.2.3.1 Hardware (Inventar der Datenspeicher, Server, Backup-Systeme, Sicherheitsfunktionen); 4.2.2.3.2 Software (Inventar von Betriebs- und EPD-Anwendungssystem, Endpoint Protection, Backup, Monitoring, Update- und Patch-Management); 4.2.2.3.3 Datenbestände (Beschrieb zu Datenhaltung, Datenorganisation, Datensicherheit, Berechtigungen)

Bemerkungen zu einzelnen Ziffern		
Ziffer	**Kommentar**	**Änderungsantrag**
		4.2.2.3.4 Aufbauorganisation; 4.2.2.3.5 Prozesse (zu Datenschutz- und Datensicherheitsmanagementsystem, insbesondere auch zu Ausfallszenarien, Recovery, Tests, Audits, Verantwortlichkeiten).
4.4	Im Hinblick auf die praktische Umsetzung ist vorzusehen, dass die beauftragten Personen eine Schulung / Kurs / Attest absolvieren müssen.	4.4.1.3 sicherstellen, dass Datenschutz- und Datensicherheitsereignisse angemessen organisatorisch und technisch gemäss Kap. 4.5 adressiert werden. Speziell sind mittels Sensibilisierungsmassnahmen, Schulungen oder Erfahrungsaustausch mit anderen Verantwortlichen die beauftragten Personen innerhalb der Gemeinschaft angemessen und wiederkehrend zu unterstützen.
4.5.1.1	Ergänzung. Grund: Konformität zur EU DSGVO (siehe dazu auch Ziff. 4.13).	4.5.1.1 Verfahren für das unverzügliche Melden von Datenschutz- und/~~oder~~ Datensicherheitsereignissen an die vorgegebenen Stellen und für die Eskalation (Meldung an BAG und Zertifizerungsstelle nach Art. 11 Abs. 2) definiert haben sowie deren Einhaltung einfordern und kontrollieren; formale Verfahren für das Melden von Datenschutz- und Datensicherheitsereignissen an die betroffenen Patienten gemäss Ziff. 4.13 definiert haben.
4.7.4 (neu)	Zusatzanforderung	4.7.4 Gemeinschaften müssen zur Unterstützung des Sicherheitsschwachstellenmanagements mindestens vierteljährlich automatisierte Schwachstellen-Scans durchführen.
4.7.5 (neu)	Zusatzanforderung	4.7.5 Gemeinschaften müssen zur Unterstützung des Sicherheitsschwachstellenmanagements mindestens jährlich einen Penetration-Test durch einen unabhängigen Anbieter durchführen lassen.

Bemerkungen zu einzelnen Ziffern		
Ziffer	**Kommentar**	**Änderungsantrag**
4.9.2	Präzisierungsvorschlag mit Beispielkatalog	4.9.2 Gemeinschaften verpflichten die angeschlossenen Gesundheitseinrichtungen dazu, eine sichere Konfiguration derjenigen Endgeräte sicherzustellen (z.B. auch speziell eingeschränkt für Internet-Nutzung, Visual- oder Audio-Aufnahmen, Datentransfers, Synchronisationen), die von den Gesundheitsfachpersonen für den Zugriff auf das elektronische Patientendossier genutzt werden.
4.10.2.3	Ist hier z.B. für die Systemadministratoren eines Lieferanten ein NDA ausreichend? Falls ja, Präzisierungsvorschlag.	4.10.2.3 …Personen, die Zugang zu Daten des elektronischen Patientendossiers erlangen könnten, einer der ärztlichen Schweigepflicht analogen Verpflichtungen (wie z.B. einer vertraglichen Geheimhaltungspflicht) unterliegen;
4.10.3.2	Muss die PSP nur initial durchlaufen werden? Oder sollte diese regelmässig wiederholt werden?	4.10.3.2 diese Personen vor Aufnahme ihrer Tätigkeit und in begründeten Fällen auch während ihrer Tätigkeit eine Personensicherheitsprüfung (PSP) nach Militärgesetz durchlaufen haben;
4.13	Entsprechend den Vorgaben in anderen Zusammenhängen, z.B. der EU Datenschutzgrundverordnung, hat die Information über sicherheitsrelevante Vorgänge auch gegenüber den betroffenen Patienten zu erfolgen, wenn für diese voraussichtlich ein hohe Risiko besteht.	4.13.1 …. und kontrollieren. Zudem müssen Gemeinschaften formale Verfahren für das unverzügliche Melden von Vorfällen an die betroffenen Patienten, durch welche die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten dieser Patienten zur Folge hat, definiert haben.

Bemerkungen zu einzelnen Ziffern		
Ziffer	**Kommentar**	**Änderungsantrag**
4.14.1.2.3	Dies ist praxisfern. Wenn der Lieferant die Infrastruktur und somit auch deren fortlaufenden Betrieb sicherstellen muss, dann können Zugriffe nicht erst "bei Bedarf" aktiviert werden. SLAs können so nicht eingehalten werden (vgl. 4.23.1.2).	Streichen
4.14.1.4	Präzisierungsvorschlag	4.14.1.4 vollständige Backups gemacht werden und dass diese verschlüsselt, örtlich getrennt und sicher aufbewahrt sind;
4.14.1.5	Es ist unklar, was mit dieser Regelung bzw. dem 4-Augenprinzip gemeint ist. Vermutlich darf das Passwort nicht nur einer Person bekannt sein. Aber wie dies technisch aussehen soll, müsste man unbedingt erläutern. Ansonsten streichen.	Streichen
4.14.1.7	Sofern ein Lieferant den Betrieb der IT Infrastruktur übernimmt und dort regelmässig entsprechende Backups erstellt werden, so geschieht dies automatisiert. Eine Trennung des Speichers vom Netzwerk ist somit unrealistisch, da dies manuelle Tätigkeiten bedeuten würde.	Streichen.
4.14.1.11	Es ist eine Präzisierung bezüglich der Löschmethode erforderlich, analog oben zu Ziff. 2.1.	4.14.1.11 … vorgängig alle Daten kontrolliert und dokumentiert, vollständig und unwiderruflich gemäss aktuellen Best Practice Regeln gelöscht werden.

Bemerkungen zu einzelnen Ziffern		
Ziffer	**Kommentar**	**Änderungsantrag**
4.14.2.5	Von allen anderen Systemen des Betreibers? Braucht es wirklich für alle Systeme dedizierte Komponenten in einer separaten Netzwerkzone? Vorschlag: Mittels geeigneter Trennung (so werden logische Massnahmen wie VLAN, Virtualisierung etc. nicht ausgeschlossen).	4.14.2 Die Produktivumgebung der gemeinschaftsinternen Informatikinfrastruktur des elektronischen Patientendossiers muss: 4.14.2.5 von anderen Systemen des Betreibers mittels geeigneter Trennung~~eigener Netzwerkzonierung~~ isoliert sein (bei Trennung auf nicht physischer Basis sind weitergehende und detailliert dokumentierte Sicherheits- und Kontroll-Massnahmen zwingend erforderlich);
4.19.1.4 (neu)	Zusatzanforderung, evt. bereits (teilweise) in 4.19.1.2 abgedeckt, je nach Interpretation.	4.19.1.4 nicht-autorisierte WLAN-Zugriffspunkte erkannt und identifiziert werden.
4.20.1.1.6 (neu)	Zusatzanforderung bzgl. Systemhärtung	4.20.1.1.6 ausschliesslich die für die Systemfunktion notwendigen Dienste, Protokolle und Daemons aktiviert sind;
4.20.2.1	Das Wort „separiert“ lässt viel Interpretationsspielraum zu (virtuell, logisch, physisch…). Daher der folgende präzisierende Ergänzungsvorschlag.	4.20.2.1 …. aufweisen. Bei Trennung auf nicht physischer Basis sind weitergehende und detailliert dokumentierte Sicherheits- und Kontroll-Massnahmen zwingend erforderlich;

Bemerkungen zu einzelnen Ziffern		
Ziffer	**Kommentar**	**Änderungsantrag**
4.21 / 4.21.1 / 4.21.2	Es ist zwar richtig, dass ein Ablauf der Sitzung stattfinden soll, allerdings wäre dieser sinnvollerweise anderswo zu definieren und hier darauf zu verweisen. Es sollte nicht der ganze Anhang angepasst werden müssen, wenn eine Anpassung der Ablaufzeit stattfindet. Ausserdem wäre es womöglich passender, generell von Sitzungen zu sprechen (und nicht von Netzwerk-Sitzungen), da die gleichen Grundsätze auch für offline-Arbeitsplätze gelten können.	4.21 **Ablauf von Netzwerk-Sitzungen («*Session timeout*») (Abs. 3)** 4.21.1 Inaktive Netzwerk-Sitzungen müssen nach einer definierten Inaktivitätsperiode ~~(20 Minuten bei Patienten 2 Stunden bei Gesundheitsfachpersonen)~~ automatisch beendet werden. 4.21.2 Die Authentisierung auf den Zugangsportalen und Endgeräten muss vor dem nächsten Zugriff erneut durchgeführt werden, wenn während ~~20 Minuten bei Patienten, beziehungsweise 2 Stunden bei Gesundheitsfachpersonen~~ der Inaktivitätsperiode keine Interaktion des Benutzers mit dem elektronischen Patientendossier stattfand.
4.23.1.2	Eine „vertraglich vereinbarte Verfügbarkeit über die Zeit von mindestens 98%“ ist eine ungenügende Formulierung. Wird ein Jahr als Massstab genommen, entspräche das 7 Tage Ausfall. Eine Formulierung über einen bestimmten Zeitraum und/oder mittels absolut definierter Ausfalldauer ist vorzuziehen.	4.23.1.2 die exponierten technischen Dienste der Informatikinfrastruktur eine vertraglich vereinbarte Verfügbarkeit über die Zeit von mindestens 98%, sowie unter Last aufweisen, wobei die maximale Ausfalldauer am Stück 48h nicht überschreiten darf;
4.25 (neu)	Zusatzanforderung, damit sichergestellt ist, dass Patientendaten nicht nach deren Vernichtung in alle Ewigkeit in Datensicherungen fortbestehen.	**4.25 Datensicherung (Backups)** Datensicherungen sind spätestens nach zwei Jahren zu vernichten, sofern keine gesetzlichen oder regulatorischen Anforderungen etwas Anderes verlangen. Im Falle belegbar betrieblicher Notwendigkeit kann diese Dauer auf maximal 3 Jahre ausgedehnt werden.

7 EDI: EPDV-EDI Anhang 3: Metadaten

Allgemeine Bemerkungen

Keine Kommentare

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag

8 EDI: EPDV-EDI Anhang 5: Integrationsprofile

Allgemeine Bemerkungen

Keine Kommentare

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag

9 EDI: EPDV-EDI Anhang 5: Integrationsprofile - Nationale Anpassungen der Integrationsprofile

Allgemeine Bemerkungen

Keine Kommentare

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag

10 EDI: EPDV-EDI Anhang 5: Integrationsprofile - Nationale Integrationsprofile

Allgemeine Bemerkungen

Keine Kommentare

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag

11 EDI: EPDV-EDI Anhang 6: Kennzahlen für die Evaluation

Allgemeine Bemerkungen

Keine Kommentare

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag

12 EDI: EPDV-EDI Anhang 7: Mindestanforderungen an die Qualifikation der Angestellten der Zertifizierungsstellen

Allgemeine Bemerkungen

Keine Kommentare

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag

13 EDI: EPDV-EDI Anhang 8: Vorgaben für den Schutz der Identifikationsmittel

Allgemeine Bemerkungen

Keine Kommentare

Bemerkungen zu einzelnen Ziffern

Ziffer	Kommentar	Änderungsantrag