Information Security in Healthcare

Praxistipps im Umgang mit Zugriffsinformationen im EPD und bei verteilten Systemen

Christoph Knöpfel / Thomas Akermann, CSP AG

Agenda

Information Security in Healthcare

Agenda

Information Security in Healthcare

Ausgangslage

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Information Security in Healthcare

EPDG

Ziele

- Stärkung der Qualität
- Prozessoptimierungen
- Erhöhung der Patientensicherheit
- Effizienzsteigerung in der Behandlung
- Stärkung der Gesundheitskompetenz der Patientinnen und Patienten

Kantonales Recht

- Aktualisierung von kantonalem Recht
- Zuständig für die Überwachung der Gesundheits-einrichtungen
- Mitarbeit in der Ausgestaltung des Ausführungsrecht

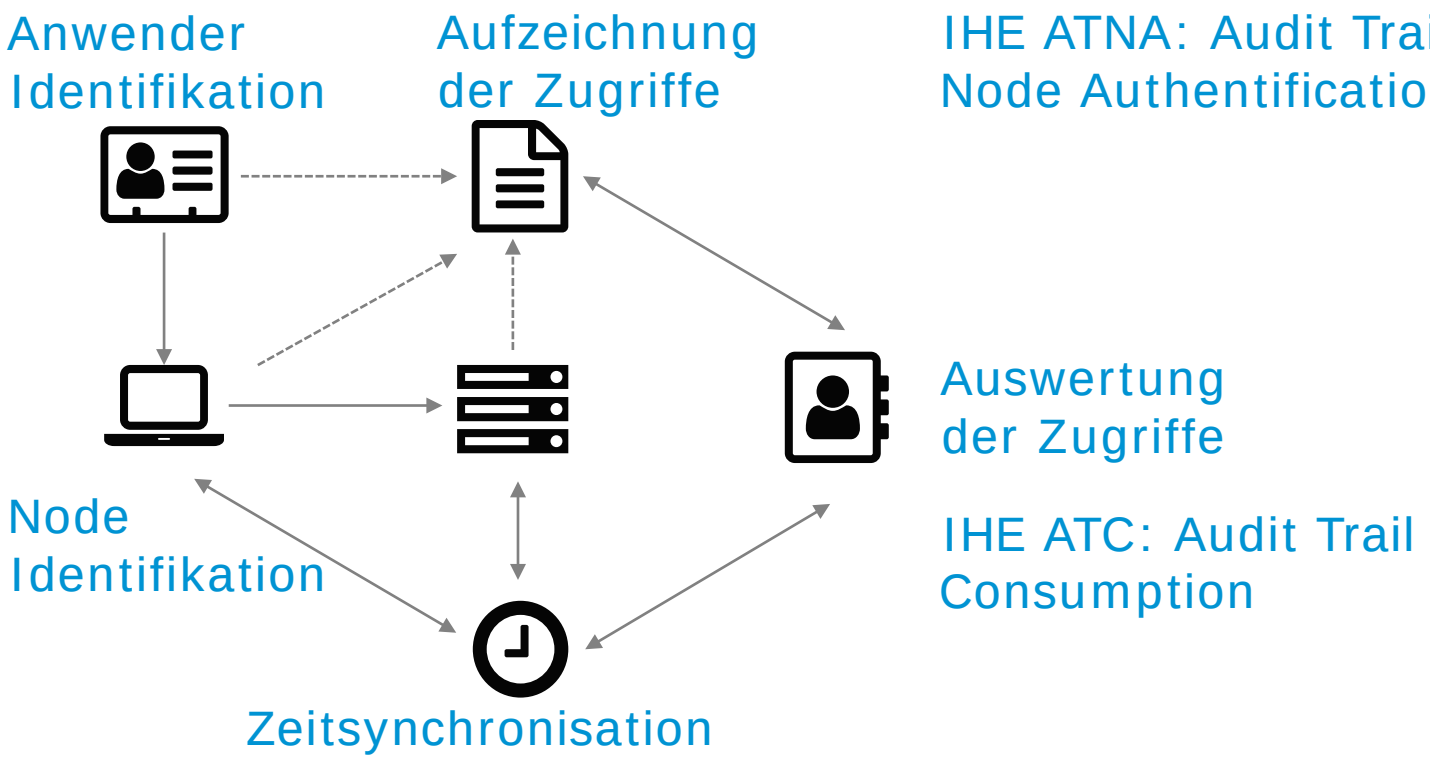
Ausführungsrecht

- Verordnung zu Finanzhilfen
- Verordnung zum EPD
  - Departements-verordnungen mit diversen Anhängen
- Anhang 2: TOZ (Technische und Organisatorische Zertifizierungs-voraussetzungen)
- Anhang 5: Vorgaben zu den Integrationsprofilen

Ausgangslage

Information Security in Healthcare

So schreibt der Anhang 2 der Verordnung des EDI vom 22. März 2017 über das elektronische Patientendossier («TOZ») in Ziffern 4.6.2 Buchstaben d vor, dass in jeder Gemeinschaft Systeme und Datenspeicher für die Protokolldaten (IHE-Akteure *Audit Repository*, und *Patient Audit Record Repository*) vorhanden sein müssen.

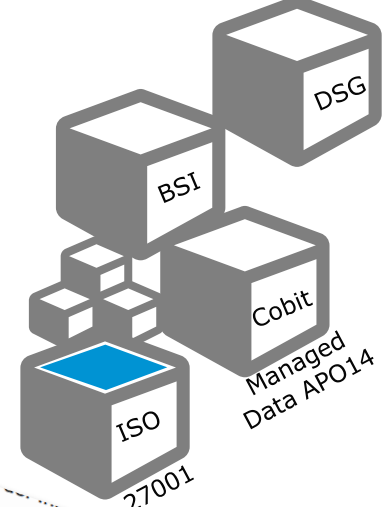


Agenda

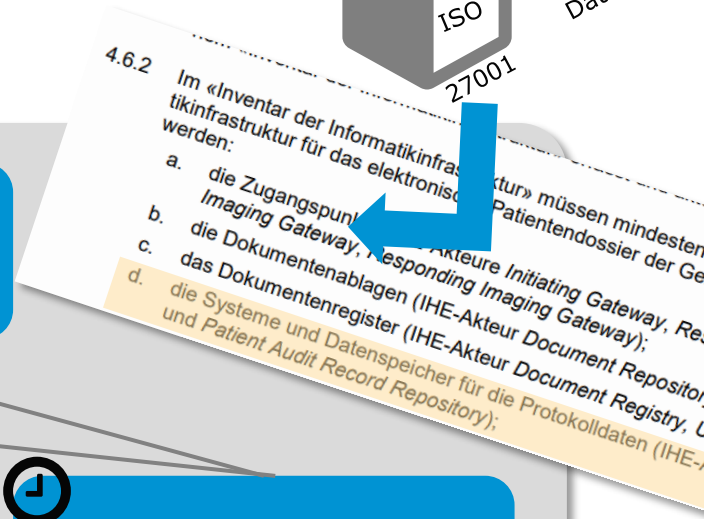
Information Security in Healthcare

Aufzeichnung von Datenzugriffen

Information Security in Healthcare



Frameworks / Vorgaben…



ISO 27001, Anhang 12.4

Datenzugriff

Ereignisse sind aufgezeichnet A12.4

Nachweise sind erzeugt A12.4

Ereignisprotokollierung A12.4.1

Schutz der Protokollinformationen A12.4.2

Administratoren- und Bedienerprotokolle A12.4.3

Uhrensynchronisation A12.4.4

Wer wertet unsere Protokolle überhaupt aus? Sind die Überprüfungen von Protokollen intern geregelt?

Wo sind meine Protokolle und sind die vor Veränderbarkeit geschützt?

Werden Administratorenrechte periodisch überprüft?

Laufen meine Systeme synchron, dass ich auch eine entsprechende Vergleichbarkeit der Protokolle garantieren kann?

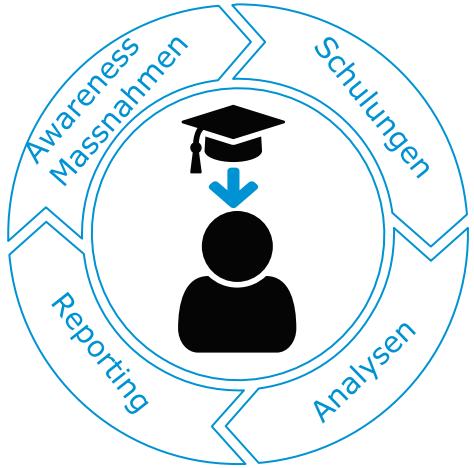
Ziele der Aufzeichnung von Datenzugriffen

Information Security in Healthcare

Wieso zeichnen wir eigentlich auf?

- Der Umgang mit Informationssicherheitsvorfällen ist ein wichtiger Bestandteil der Informationssicherheit.
- Sicherheitsvorfälle kommen immer wieder vor → In einem solchen Fall ist es wichtig, den Quellen und Ursachen auf den Grund gehen zu können (Analyse und Recovery).
- Ziel präventiv Vorfälle zu entdecken → dazu werden ein zentrales Log Management und Analyse sowie die notwendigen Ressourcen (bspw. ein Sicherheitsbeauftragter oder im besten Fallen ein Security Operations Center SOC) benötigt.

In den meisten Fällen ist die Quelle eine Person,
die unbeabsichtigt oder beabsichtigt einen Vorfall auslöst.

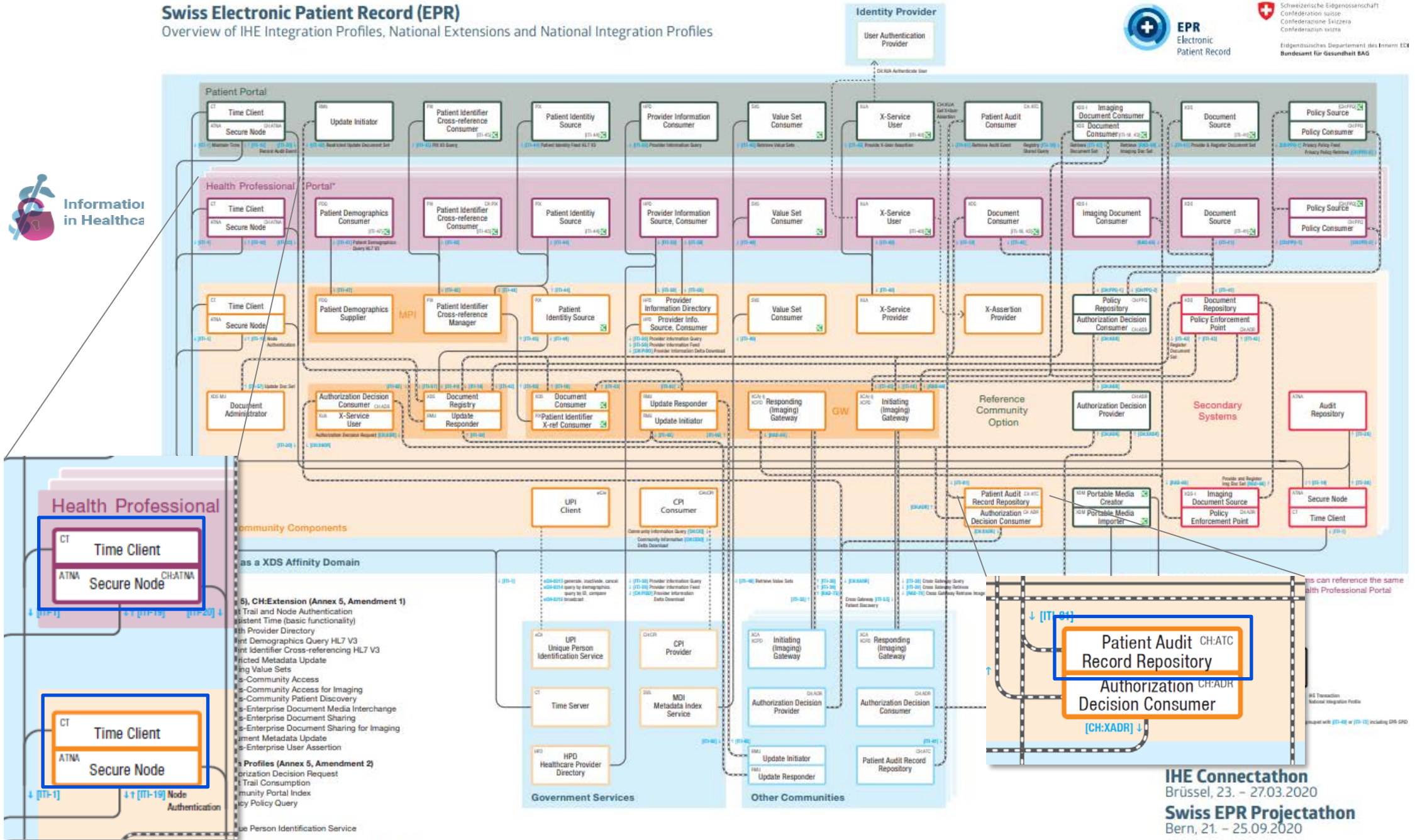


Agenda

Information Security in Healthcare

Swiss Electronic Patient Record (EPR)

Overview of IHE Integration Profiles, National Extensions and National Integration Profiles



IHE Connectathon
Brüssel, 23. – 27.03.2020

Swiss EPR Projectathon
Bern, 21. – 25.09.2020

Agenda

Information Security in Healthcare

Woran sollten wir bei Aufzeichnungen speziell denken?

Information Security in Healthcare

Aufzeichnungen und deren Auswertungen sind «Good Practice». Dies gilt nicht nur für das EPD/Gesundheitswesen.

Rechtliche Vorgaben definieren für den erhöhten Schutzbedarf (Patientendaten, besondere Personendaten) -> daraus ergeben sich weitere Vorgaben

Die Stammgemeinschaft verfügt über einen zentraler Logserver (Audit Repository).

- Ein Notfallzugriff löst immer einen Alarm aus.
- Unberechtigte und abgewiesene Zugriffsversuche müssen regelmässig ausgewertet werden.

Tipps im Umgang mit Datenzugriffen auf das EPD

Information Security in Healthcare

Was bedeutet dies nun im EPD Kontext:

- Sämtliche Datenzugriffe können durch den Besitzer des EPD eingesehen werden
- Unerlaubte Zugriffe werden gemeldet
- Notfallzugriffe werden dem Besitzer des EPDs nicht nur angezeigt, sondern mittels einer Nachricht speziell hervorgehoben

Bitte machen Sie das Ihren GFPs (Gesundheitsfachpersonen) und HIPs (Hilfspersonen) bewusst!

Agenda

Information Security in Healthcare

Tipps zur Nutzung der Datenzugriffe in der Gesundheitseinrichtung

Information Security in Healthcare

Die Aufzeichnungen der Datenzugriffe können auch einen Mehrwert innerhalb einer Gesundheitseinrichtung ermöglichen.

Kennen Sie folgende Situationen?

- Es ist nicht mehr eindeutig nachvollziehbar welcher Anwender welche Informationen erstellt, verändert oder gelöscht hat
- Es steht die Behauptung im Raum, dass ein Anwender unbefugt auf Informationen zugegriffen hat
- Als Gesundheitseinrichtung sind Sie mit einem Haftpflichtfall konfrontiert und die Rechtsabteilung muss den Ablauf rekonstruieren
- Ein Patient beansprucht die Auskunftspflicht und will alle Informationen bezüglich wer welche Behandlungsinformationen erstellt, verändert oder gelöscht hat

Nutzen wir doch das Konzept des EPDs!

Tipps zur Nutzung der Datenzugriffe in der Gesundheitseinrichtung

Information Security in Healthcare

Was braucht es dazu?

- Einteilung der zu involvierenden IT Systeme wie KIS, PACS, PDMS, LIS, eArchiv, Pathologie Archiv, „EPD Viewer“
- Audit Record Repository zum Beispiel als Ergänzung zum eArchiv
- Einheitliche Konfiguration des Time Servers
- Einheitliche Anbindung des Active Directory zur Nutzung der Benutzer Identifikationen
- Aktualisierung der IT Nutzungsreglemente
- Vorlagen für Beschaffungen

Tipps zur Nutzung der Datenzugriffe in der Gesundheitseinrichtung

Information Security in Healthcare

Mögliches Vorgehen für die Umsetzung

- Aktivierung des Audit Record Repository in einem vorhandenen eArchiv oder einer Integrationsplattform und dem Zugang zu einem Audit Consumer
- Sicherstellung einer einheitlichen Time Server Konfiguration
- Einfordern einer ATNA Schnittstelle beim KIS Produkthersteller (Hinweis: Alle KIS Hersteller welche den EPD Akteur für das Healthprofessional Portal umgesetzt haben, haben diese Funktionalität schon verfügbar -> siehe KIS Teilnehmer an den EPD Projectathons)
- Umsetzungsplanung für die weiteren Systeme

Tipps zur Nutzung der Datenzugriffe in der Gesundheitseinrichtung

Information Security in Healthcare

Was kann mit einer solchen Umsetzung erreicht werden?

- Reduzierung des Aufwandes für die Erfüllung von datenschutzrechtlichen Pflichten
- Vermehrte Awareness bei den eigenen Mitarbeiter/-innen
- Verbesserter Schutz der eigenen Mitarbeiter/-innen

Wie realistisch ist eine Umsetzung?

- Je nach Hersteller stehen die notwendigen Komponenten schon bereit; siehe (Kapitel: Participating Organisations) https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/E/final-report-epr-projectathon-2019.pdf
- Weitere Hersteller stehen in den Startlöchern

Auf was muss bei der Umsetzung geachtet werden?

- Die Umsetzung muss unbedingt mit einer Informationskampagne für die eigenen Mitarbeiter/-innen begleitet werden, da durch die erhöhte Transparenz durchaus Ängste entstehen können
- Bei der Beschaffung müssen die entsprechenden Anforderungen gestellt werden

Agenda

Information Security in Healthcare

Fazit

Information Security in Healthcare

- Zentralisierung der Zugriffsinformationen kann als Instrument für die Awareness Bildung genutzt werden
- Die Nachvollziehbarkeit der Datenbearbeitung auch von externen Mitarbeiter*innen ist transparenter gewährleistet
- Die Technologie und die Lösungen sind vorhanden
- Mit den entsprechenden Anforderungen in einem Lastenheft bewegt sich der Markt und die Lösungen werden integraler Bestandteil der Offerten

Gerne unterstützen wir Sie in Ihren Vorhaben

Information Security in Healthcare

Christoph Knöpfel

Direkt +41 44 520 33 66
christoph.knoepfel@csp-ag.ch

CSP AG
Schützengasse 23
CH-8001 Zürich
Tel +41 44 520 33 60
www.csp-ag.ch

Thomas Akermann

Direkt +41 71 231 10 86
thomas.akermann@csp-ag.ch

CSP AG
Teufener Strasse 5
CH-9000 St.Gallen
Tel +41 71 231 10 60
www.csp-ag.ch