Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Sicherheitspanne bei der Einführung des elektronischen Patientendossiers im Kanton Wallis

Dorfmatt Zentrum, Rotkreuz

09.30 – 10.15 Uhr

14. Juni 2016

Prof. Ursula Sury, Vizedirektorin Hochschule Luzern
Departement Informatik, Rechtsanwältin

FH Zentralschweiz

EFQM
Recognised for excellence
5 star - 2015

Was war ursprünglich geplant und warum?

- Das **elektronische Patientendossier** ist ein virtuelles Dossier, zentral abgelegt mit den behandlungsrelevanten Daten eines Patienten und der Zugriffsmöglichkeit der an der Behandlung beteiligten Gesundheitsfachpersonen.

- **Ziel:** Die Qualität der medizinischen Behandlung soll gestärkt, Behandlungsprozesse verbessert, Patientensicherheit erhöht, die Effizienz des Gesundheitssystems gesteigert, Doppelbehandlungen verhindert sowie die Gesundheitskompetenz der Patienten gefördert werden.

Was war ursprünglich geplant und warum?

- **Einführung des elektronischen Patientendossiers** im Kanton Wallis per *1. September 2015* als zweiter Kanton (nach Genf)

- Förderung des Austausches von medizinischen und pflegerischen Informationen zwischen Gesundheitspartnern zur Verbesserung der Patientenbetreuung und Konsultation ihrer medizinischen Daten

- **Vorstellung und Ankündigung** an Pressekonferenz vom *27. August 2015*

- **Infomed** sollte der eHealth-Strategie des Bundes entsprechen
  - Beim Infomed handelt es sich um ein Umsetzungsprojekt und nicht um ein Patientendossier nach EPDG, dieses wird es erst ab Inkrafttreten (ab 2017) des EPDG geben

Was ist passiert?

- Die Piratenpartei Schweiz gab *vor* dem *1. September 2015* **Hinweise zur mangelhaften Sicherheit**. Sie führten eine **externe Prüfung** durch.

- Der **Datenschutzbeauftragte** des Kantons Wallis **empfahl** dem Kanton daraufhin die **Einführung** des elektronischen Patientendossiers **auszusetzen** aufgrund von Sicherheitsbedenken.

- Der **Kanton Wallis** kommt dieser Empfehlung nach und **suspendiert** das Projekt **Infomed**.

Was ist schief gelaufen?

Gemäss der Piratenpartei Schweiz, welche durch eine externe Prüfung die mangelhafte Sicherheit entdeckte, sind **zwei Punkte** als **kritisch** auszumachen:

1. Bei der **Verschlüsselung** der Webseiten seien **veraltete Standards** verwendet worden.

   - Dies führe zu **ungenügendem Schutz vor Hackerangriffen**.
   - Im schlimmsten Fall könnten von Unbefugten Gesundheitsdaten nicht nur eingesehen, sondern auch verändert werden.

Was ist schief gelaufen?

2. Dienste von **Google Analytics** kämen zum Einsatz.

- **Google wisse** dadurch, **wer** wann auf sein **Dossier zugreife**.
- In **Kombination mit Surfverhalten** der Person könnte Google **Rückschlüsse auf** deren **Gesundheitszustand** ziehen.

Die Piratenpartei Schweiz hat offenbar nur öffentlich zugängliche Informationen ausgewertet.

Überblick

Teil I Datenschutz und Datensicherheit

1. Bundesrechtliche Grundlagen
2. Strategie E-Health Schweiz
3. Verhältnis zwischen Bund und Kantone (Patientendossier)
4. Rechtliche Grundlagen Kanton Wallis
5. Werden diese Voraussetzungen mit elektronischem Patientendossier des Kantons Wallis erfüllt?

Überblick

Teil II Elektronisches Patientendossier im Wallis

1. Was war ursprünglich geplant und warum?
2. Was ist passiert?
3. Was ist schief gelaufen?
4. Warum wurde dies zu spät bemerkt?
5. Wie hätte man es machen müssen und warum?
6. Was kann daraus gelernt werden (Lessons learned)?
7. Wie weiter?
8. Öffentlichkeits- und Datenschutzbeauftragter Kanton Wallis
9. Exkurs: ELGA (elektronische Gesundheitsakte) Österreich

Teil I Datenschutz und Datensicherheit

1. Bundesrechtliche Grundlagen
2. Strategie E-Health Schweiz
3. Verhältnis zwischen Bund und Kantone (Patientendossier)
4. Rechtliche Grundlagen Kanton Wallis
5. Werden diese Voraussetzungen mit elektronischem Patientendossier des Kantons Wallis erfüllt?

1. Bundesrechtliche Grundlagen

Wann ist eine Datenbearbeitung erlaubt?

Eine Datenbearbeitung ist legal, wenn sie rechtmässig, verhältnismässig, zweckgebunden und integer ist. Bevor Sie Daten bearbeiten können, müssen Sie folgende vier Fragen mit Ja beantworten können:

Art. 4 ff. DSG

- Ist die vorgesehene Bearbeitung der Daten **rechtmässig**?
- Dient die vorgesehene Bearbeitung dem richtigen **Zweck**?
- Ist die vorgesehene Bearbeitung **verhältnismässig**?
- Sind die verwendeten Daten korrekt?

1. Bundesrechtliche Grundlagen

Wann ist eine Datenbearbeitung erlaubt?

Wenn Sie alle diese **Fragen** bez. einer Datenbearbeitung **mit Ja** beantworten können, dann ist diese **erlaubt.**

- Ist die von mir vorgesehene Bearbeitung der Daten rechtmässig?
- Dient die von mir vorgesehene Bearbeitung dem richtigen Zweck?
- Ist die von mir vorgesehene Bearbeitung verhältnismässig?
- Sind die von mir verwendeten Daten korrekt?

2. Strategie E-Health Schweiz

- Vom Bundesrat am 27. Juni 2007 verabschiedet
- Bestandteil der Strategie „Gesundheit 2020"

Ziele
- Einführung des elektronischen Patientendossiers auf nationaler Ebene
- Schaffung eines Gesundheitsportals mit gesundheitsrelevanten Informationen verfügbar für die ganze Schweiz
- Vernetzung der Akteure im Gesundheitswesen, um die Qualität der Behandlungsprozesse, die Patientensicherheit und die Effizienz im Gesundheitswesen zu erhöhen

Umsetzung
- Bundesgesetz über das elektronische Patientendossier (EPDG), das 2017 in Kraft treten soll
- Koordinationsorgan „eHealth Suisse"

2. Strategie E-Health Schweiz

Elektronisches Patientendossier

- Virtuelles Dossier
- Freiwillig, ohne Angabe von Gründen widerrufbar
- Der Patient kann selber eigene Daten (z.B. Infos über Allergien) in sein elektronisches Patientendossier hochladen
- Der Patient hat immer Zugriff, Gesundheitsfachpersonen nur, wenn sie vom Patienten die Zugriffsrechte erhalten.
- Auch ohne Zugriffsrechte ist Zugriff möglich (z.B. in Notfallsituationen), sofern dies nicht vorgängig untersagt wurde
- Der Patient kann einsehen, wer auf sein Dossier zugegriffen hat
- Identifikation durch eine elektronische Identität und ein Identifikationsmittel eines zertifizierten Herausgebers

3. Verhältnis zwischen Bund und Kantone

- Bundeskompetenzen im Gesundheitssystem beschränkt
- Regelung der allgemeinen Gesundheitsversorgung ist grundsätzlich den Kantonen vorbehalten
- Art. 95 Abs. 1 und Art. 122 BV
  - Erlaubnis des Bundes sämtliche Formen und Stufen der privatwirtschaftlichen Tätigkeit zu regeln unter Beachtung des Grundsatzes der Wirtschaftsfreiheit
    - ➢ Voraussetzungen für Berufsausübung und Berufsausübung
  - Darunter fällt auch die Regelung des privatrechtlichen Verhältnisses zwischen Gesundheitsfachpersonen und Patienten (Auftragsrecht)
  - Festlegung der notwendigen Standards ist Vorschrift zur Berufsausübung und kann vom Bund geregelt werden

3. Verhältnis zwischen Bund und Kantone

- EPDG legt lediglich Rahmenbedingungen für die Bearbeitung der Daten des elektronische Patientendossier auf Bundesebene fest
  - ➢einheitliche Umsetzung
- Umgang mit abgerufenen Daten richtet sich nach geltendem Recht
- Mitfinanzierung beim Aufbau durch den Bund (Art. 20 ff. EPDG)
- Zentrale Ausgleichsstelle (ZAS) für Umsetzung der sicheren Ausgabe und Nutzung der neuen Patientenidentifikationsnummer zuständig
- Koordiantionsorgan Bund-Kantone „eHealth Suisse" als fachliche Kompetenzstelle
- Kantone müssen ihre Rechtslage auf die Vereinbarkeit mit dem EPDG überprüfen und allenfalls Anpassungen vornehmen

4. Rechtliche Grundlagen im Kanton Wallis

Art. 17 ff. GIDA, Art. 28 ff. ARGIDA, Art. 17 ff. „Infomed"-Verordnung:

- Ist die vorgesehene Bearbeitung der Daten **rechtmässig, d.h. besteht eine gesetzliche Grundlage oder ist diese für die Erfüllung einer gesetzlichen Aufgabe notwendig**?
- Sind die Daten geeignet, zutreffend, richtig und vollständig in Bezug zum Zweck?
- Besteht für die besonders schützenswerten Daten ein Gesetz i.f.S.?
- Ist die vorgesehene Bearbeitung **verhältnismässig**?
- Sind die verwendeten Daten korrekt?
- Sind geeignete Massnahmen für die **Datensicherheit** vorhanden?

5. Werden diese Voraussetzungen mit elektronischem Patientendossier des Kantons Wallis erfüllt?

Rechtmässigkeit, Zweck, Verhältnismässigkeit und Korrektheit der Daten vorliegend unproblematisch

Geeignete Massnahmen für die **Datensicherheit** vorhanden?
→ Offensichtlich nicht! - Teil II Elektronisches Patientendossier

Teil II Elektronisches Patientendossier im Wallis

1. Was war ursprünglich geplant und warum?
2. Was ist passiert?
3. Was ist schief gelaufen?
4. Warum wurde dies zu spät bemerkt?
5. Wie hätte man es machen müssen und warum?
6. Was kann daraus gelernt werden (Lessons learned)?
7. Wie weiter?
8. Öffentlichkeits- und Datenschutzbeauftragter Kanton Wallis
9. Exkurs: ELGA (elektronische Gesundheitsakte) Österreich

1. Was war ursprünglich geplant und warum?

- Das **elektronische Patientendossier** ist ein virtuelles Dossier, zentral abgelegt mit den behandlungsrelevanten Daten eines Patienten und der Zugriffsmöglichkeit der an der Behandlung beteiligten Gesundheitsfachpersonen.

- **Ziel:** Die Qualität der medizinischen Behandlung soll gestärkt, Behandlungsprozesse verbessert, Patientensicherheit erhöht, die Effizienz des Gesundheitssystems gesteigert, Doppelbehandlungen verhindert sowie die Gesundheitskompetenz der Patienten gefördert werden.

1. Was war ursprünglich geplant und warum?

- **Einführung des elektronischen Patientendossiers** im Kanton Wallis per *1. September 2015* als zweiter Kanton (nach Genf)

- Förderung des Austausches von medizinischen und pflegerischen Informationen zwischen Gesundheitspartnern zur Verbesserung der Patientenbetreuung und Konsultation ihrer medizinischen Daten

- **Vorstellung und Ankündigung** an Pressekonferenz vom *27. August 2015*

- **Infomed** sollte der eHealth-Strategie des Bundes entsprechen

1. Was war ursprünglich geplant und warum?

- **Einführung des elektronischen Patientendossiers** im Kanton Wallis per *1. September 2015* als zweiter Kanton (nach Genf)

- Förderung des Austausches von medizinischen und pflegerischen Informationen zwischen Gesundheitspartnern zur Verbesserung der Patientenbetreuung und Konsultation ihrer medizinischen Daten

- **Vorstellung und Ankündigung** an Pressekonferenz vom *27. August 2015*

- **Infomed** sollte der eHealth-Strategie des Bundes entsprechen
  - Beim Infomed handelt es sich um ein Umsetzungsprojekt und nicht um ein Patientendossier nach EPDG, dieses wird es erst ab Inkrafttreten (ab 2017) des EPDG geben

2. Was ist passiert?

- Die Piratenpartei Schweiz gab *vor* dem *1. September 2015* **Hinweise zur mangelhaften Sicherheit**. Sie führten eine **externe Prüfung** durch.

- Der **Datenschutzbeauftragte** des Kantons Wallis **empfahl** dem Kanton daraufhin die **Einführung** des elektronischen Patientendossiers **auszusetzen** aufgrund von Sicherheitsbedenken.

- Der **Kanton Wallis** kommt dieser Empfehlung nach und **suspendiert** das Projekt **Infomed**.

3. Was ist schief gelaufen?

Gemäss der Piratenpartei Schweiz, welche durch eine externe Prüfung die mangelhafte Sicherheit entdeckte, sind **zwei Punkte** als **kritisch** auszumachen:

1. Bei der **Verschlüsselung** der Webseiten seien **veraltete Standards** verwendet worden.

   - Dies führe zu **ungenügendem Schutz vor Hackerangriffen**.
   - Im schlimmsten Fall könnten von Unbefugten Gesundheitsdaten nicht nur eingesehen, sondern auch verändert werden.

3. Was ist schief gelaufen?

2. Dienste von **Google Analytics** kämen zum Einsatz.

- **Google wisse** dadurch, **wer** wann auf sein **Dossier zugreife**.
- In **Kombination mit Surfverhalten** der Person könnte Google **Rückschlüsse auf** deren **Gesundheitszustand** ziehen.

Die Piratenpartei Schweiz hat offenbar nur öffentlich zugängliche Informationen ausgewertet.

4. Warum wurde dies zu spät bemerkt?

- **Komplexität** des Projekts

- Mangelhafte Überprüfung / Kontrolle

5. Wie hätte man es machen müssen und warum?

- Datenschutz und Datensicherheit ist Chefsache!

- Grösste Sorgfalt walten lassen, noch bevor ein solches Projekt online geht.

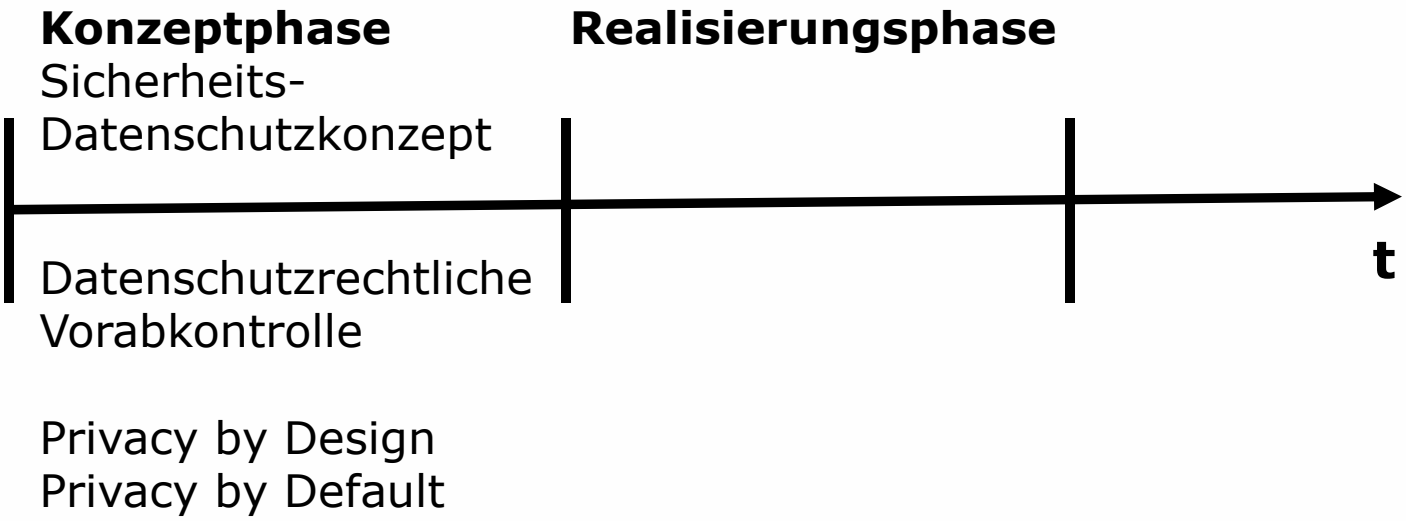
Zusätzlich im Sinne der Transparenz:

- Die dem elektronischen Patientendossier zugrunde liegende **Software veröffentlichen bzw. deren Quellcode**.

- Dadurch hätten u.a. die Piratenpartei und/oder der Chaos Computer Club das System auf Schwachstellen testen können.

5. Wie hätte man es machen müssen und warum?

Projektphasen



6. Was kann daraus gelernt werden (Lessons learned)?

- Datenschutz und Datensicherheit ist **Chefsache**!

- **Sorgfältige Planung** des Konzeptes bei einem solchen Projekt

- **Bewusstsein** fürs Thema haben

7. Wie weiter?

- **Chef muss Ruder übernehmen** (Führung)
- **Sauberes Konzept** der zu beachtenden Vorschriften und zu behebenden Probleme
- Ggfs. Begleitung durch **externe Spezialisten**
- **Schulung** der Mitarbeitenden
- **Sensibilisierung** für datenschutzrechtliche Themen

8. Öffentlichkeits- und Datenschutzbeauftragter Kanton Wallis

- Kein Öffentlichkeits- und Datenschutzbeauftragter im Kanton Wallis bis 2010
- 2010 Wahl von Ursula Sury als Öffentlichkeits- und Datenschutzbeauftragte
- 2011 Inkraftsetzung GIDA
- Budget Vollkosten für Datenschutz und Öffentlichkeit, inkl. zweisprachig, Kommissions- und Expertenentschädigung Fr. 100‘000

8. Öffentlichkeits- und Datenschutzbeauftragter Kanton Wallis

- Kurzfristige Erhöhung des Budgets bis auf Fr. 300‘000
- Kurzfristige Reduktion des Budgets auf Vorschlag gewisser politischer Parteien auf Fr. 100‘000
- Sofortiger geschlossener Rücktritt der Datenschutzkommission
- Ursula Sury verzichtet auf weitere Amtsdauer

9. Exkurs: ELGA (elektronische Gesundheitsakte) Österreich

Allgemeines

- Umsetzung seit Dezember 2015
- Flächendeckende Vernetzung der Gesundheitsdaten von Patienten
- Flächendeckende Vernetzung von Spitälern, Ärzten, Apotheken und Pflegeeinrichtungen in Österreich
- PatientInnen können eigene Gesundheitsdaten einsehen und verwalten
- Unterstützung der medizinischen, pflegerischen und therapeutischen Behandlung und Betreuung durch besseren Informationsfluss

9. Exkurs: ELGA (elektronische Gesundheitsakte) Österreich

Sicherheit

- Protokollierung aller ELGA-Transaktionen
- Zugriff Gesundheitsanbieter nur bei aufrechtem Behandlungs- bzw. Betreuungsverhältnis
  - ➢e-Card als Schlüssel, der Zugriff auf Daten gewährt
- Zugriff Bürger via Handysignatur
- Verschlüsselter Datentransport
- Sicherheits-Audits bei Betreibern von ELGA-Komponenten
- Bei Verdacht auf Datenmissbrauch Meldung an Ombudsstelle
  - ➢Strafen in der Höhe von mehreren 10‘000 Euro oder bis zu einem halben Jahr Haft

9. Exkurs: ELGA (elektronische Gesundheitsakte) Österreich

Sicherheit

- Zugriffsdauer
  - Arzt hat bis 28 Tage nach Behandlung/Entlassung Zugriff auf ELGA des Patienten
  - Apotheke hat 2 Stunden Zugriff auf Medikationsdaten
  - Zugriffsdauer kann von Patient verlängert oder verkürzt werden
- Speicherort
  - Gesundheitsdaten (z.B. Befunde oder Entlassungsbriefe) werden dort gespeichert, wo sie entstehen
  - Medikationsdaten werden zentral in verschlüsselter Form gespeichert

Fragen?

Danke

Publikationen

- **IT-Fehler**
  In: Handbücher für die Anwaltspraxis – Haftung und Versicherung, Weber/Münch, Helbling & Lichtenhahn Verlag 2015

- **IT-Outsourcing Verträge**
  In: Prinzipen des Vertragsrechts,Böhringer/Müller/Münch/Waltenspühl, Schulthess-Verlag 2015

- **BGE 125 III 263: Softwarelizenz: Wie weit reichen die Nutzungsrechte der Lizenznehmerin?**
  In: Immaterialgüterrecht in kommentierten Leitentscheiden, Schulthess-Verlag 2015

Danke

Sofort lieferbar

CHF 69.00

Informatikrecht

Sury, Ursula

Verlag	Stämpfli Verlag AG, Bern
Erscheinungsjahr	2013
Auflage	1. Auflage
ISBN	978-3-7272-7996-6
Sprache	Deutsch
Seiten	240
Produkttyp	Buch (Broschiert)
Warengruppe	Recht
Detailwarengruppe	Informatikrecht

DIE ADVOKATUR SURY

Prof. Ursula Sury, Rechtsanwältin

www.dieadvokatur.ch
ursula.sury@dieadvokatur.ch

www.hslu.ch
ursula.sury@hslu.ch