Informationssicherheit bei der EPD-Anbindung

Wenn sich eine Gesundheitseinrichtung einer EPD-Stammgemeinschaft und damit dem nationalen EPD-Vertrauensraum anschliesst, dann bleibt dies nicht ohne Auswirkungen auf die internen Prozesse und Systeme. Dieser Artikel beleuchtet den Handlungsbedarf speziell im Bereich der Informationssicherheit.

*Thomas Kessler **

Spitäler und Heime müssen sich bis 2020 respektive 2022 einer EPD-Gemeinschaft anschliessen. Sie werden damit Teil des Vertrauensraums EPD, dessen Regeln von Gesetz und Ausführungsrecht bestimmt werden.

In dieser ersten Phase geht es darum, das Spital oder Heim an eine EPD-Stammgemeinschaft anzubinden im Sinne einer ungerichteten Kommunikation mit Patienten und anderen Einrichtungen wie Spitälern, Arztpraxen oder Apotheken. Das Spital oder Heim wird zum Lieferanten von Daten zu Handen anderer Einrichtungen und zum Bezüger von Daten anderer Einrichtungen, die am Vertrauensraum EPD partizipieren. Mittelfristig können auf dieser Basis auch neue B2B-Geschäftsprozesse definiert und eingeführt werden, die durch das elektronische Patientendossier vereinfacht oder überhaupt erst praktikabel werden. Langfristig wird das EPD auch Rückwirkungen auf die internen Systeme und Prozesse der Gesundheitseinrichtung haben. Illustrative Beispiele wären eine spitalinterne Verwendung der nationalen Patientenidentifikationsnummer (PID) oder die Verwendung eines EPD-Authentisierungsmittels für die Anmeldung am Klinik Informationssystem (KIS).

Der Bund wird einige zentrale Dienste bereitstellen, von denen das nationale Verzeichnis aller Gesundheitsfachpersonen (HPD) besonders wichtig ist. Weitere Infrastrukturen wie das regionale Patientenverzeichnis der Gemeinschaft (MPI), das Dokumentenverzeichnis (Registry) und die Zugangsportale für Patienten und Gesundheitsfachpersonen werden von den Betreibern der EPD-Stammgemeinschaften aufgebaut und betrieben. Diese werden allerdings verschiedene Aufgaben und Prozesse rund um das EPD auch an die teilnehmenden Gesundheitseinrichtungen wie Heime und Spitäler delegieren. Für diese ist es wichtig, an dieser Aufgabenverteilung aktiv mitzuwirken und die Umsetzung der ihnen übertragenen Aufgaben rechtzeitig an die Hand zu nehmen.

Relevante Aspekte

Die Informationssicherheit wird über den erhofften Erfolg des elektronischen Patientendossiers mitentscheiden. Die Sicherheitsvorgaben sind deshalb ein wichtiges Element der Regulierung auf den Ebenen Bund, Stammgemeinschaft und Gesundheitseinrichtung. Die für Heime und Spitäler besonders relevanten Aspekte der Informationssicherheit im EPD und die davon betroffenen operativen Bereiche sind nachfolgend aufgeführt:

- Die Patientenadministration: Patienten, die das EPD nutzen wollen, müssen in verschiedenen Verzeichnissen registriert und mit sicheren Identifikationsmitteln ausgestattet werden, ähnlich wie dies beim E-Banking der Fall ist. Dies wird die Patientenadministration beeinflussen. Insbesondere für grosse Spitäler stellt sich die Frage, ob sie in den Prozessen für das EPD Onboarding eine aktive Rolle wahrnehmen wollen und beispielsweise die gesetzeskonforme Patienteninformation als Dienstleistung anbieten. Im Minimum wird sich jede Einrichtung überlegen müssen, wie sie die eigenen Patientendaten mit dem Patientenverzeichnis der Gemeinschaft (MPI) abgleichen wird.
- Die Benutzer- und Berechtigungsverwaltung: Jede Gesundheitseinrichtung muss klären, welche Gesundheitsfachpersonen und Hilfspersonen Zugriff auf das EPD erhalten sollen. Ausserdem muss die Verwaltung von Gruppen von Gesundheitsfachpersonen geregelt werden, weil die Zugriffsberechtigung im elektronischen Patientendossier wesentlich auf einem praktikablen Gruppenkonzept beruht. Diese Angaben müssen mit dem nationalen Verzeichnis des Bundes (HPD) sowie dem Identity Provider (IdP) abgeglichen und laufend aktualisiert werden. Das im Spital oder Heim bestehende interne System für Identity and Access Management (IAM) muss entsprechend erweitert werden. Siehe zu diesem Themenbereich auch Abbildung 1 mit der RACI Tabelle für eine mögliche Aufgabenverteilung zwischen den Teilnehmern einer Stammgemeinschaft.
- Login an den IT Systemen: Das EPD verlangt eine sogenannt starke Authentifizierung von Gesundheitsfachpersonen mit zwei Faktoren. Auch wenn hierfür die Infrastruktur eines externen Identity Providers (IdP) genutzt werden sollte, ist zu überlegen, ob, beziehungsweise wie die EPD Authentifizierungslösung mit den internen Anmeldesystemen des Spitals verknüpft wird. In diesem Zusammenhang stellt sich auch die Frage, ob eine vom Spital angestellte Gesundheitsfachperson nur am Spital-Arbeitsplatz Zugriff auf das EPD erhalten soll oder ob sie auch andere (insb. private) Geräte nutzen darf. Eine solche Kontextabhängige Zugriffskontrolle wird von der EPD Gesetzgebung heute nicht vorgeschrieben, ist aus Sicht der Informationssicherheit aber empfehlenswert.
- Der IT Systembetrieb: Vom Spital selber betriebene IT-Komponenten, die zum EPD-Vertrauensraum gehören, müssen die vom EPD-Ausführungsrecht definierten Anforderungen an den Grundschutz erfüllen. Dies betrifft insbesondere allfällige lokale EPD-Dokumentenablagen (Repositories) sowie alle internen Arbeitsplätze mit Zugriff auf das elektronische Patientendossier.
- Die Sicherheitsorganisation: Die Gemeinschaften werden für das Manage-

RACI-Tabelle zur Benutzer- und Rechteverwaltung in einer EPD-Stammgemeinschaft

	Stamm-Gemeinschaft	Gesundheits-einrichtung	Betreiber ePD Plattform	Identity Provider	GFP, Hilfsperson	Patientin, Patient
Qualitätsvorgaben definieren *- Aktualisierungsfristen für die verschiedenen Verzeichnisse* *- Aufbewahrungsfristen* *- Regeln für GFP Gruppenkonzepte*	A,R	C	-	-	-	-
GFP / HIP identifizieren *- Ausweis prüfen und scannen* *- GLN erfassen (ggf. beschaffen)* *- Passwortbrief und Aktivierungs-code für ID-Mittel aushändigen*	-	R (im Auftrag des IdP)	-	A, C (beglaubigte Dokumente aufbewahren)	-	-
Qualifikation prüfen *Qualifikationen prüfen (manuelle oder elektronische Registerabfrage)*	-	-	-	A, R (Register-Abfrage)	-	-
ePD Zugang autorisieren *Zugang zum ePD erteilen, z.B. anhand von Funktion oder OE-Zugehörigkeit bei der GE*	-	A,R	-	-	C	-
Im regionalen HPD registrieren *Eintrag mit Stammdaten im HPD der Gemeinschaft erfassen und pflegen, manuell oder über IAM*	-	A,R	C (Daten ent-gegennehmen)	R (Falls von der GE beauftragt)	I	-
HIP den GFP zuordnen *Im HPD erfassen und pflegen, welche Gesundheitsfachperson für eine Hilfsperson verantwortlich ist*		A,R	C (Daten ent-gegennehmen)	-	I	-
GFP Gruppen zuteilen *Im HPD erfassen und pflegen, welche GFP und HIP welchen GFP Gruppen angehören*	-	A,R	C (Daten ent-gegennehmen)	-	I	-
Beim IdP registrieren *Identität erfassen und pflegen, manuell oder über IAM*	-	A,R	-	C (Daten ent-gegennehmen)	I	-
ID-Mittel zustellen *Zustellen/aktivieren der Authenti-sierungsmittel für den ePD-Login*	-	R (AD Passwort falls genutzt)	-	A,R	C	-
Im nationalen HPD registrieren *Eintrag im nationalen HPD erfassen und pflegen (GFP, keine HIP)*	-	I	A,R	-	I (nur GFP)	-

R=Responsible (durchführungsverantwortlich); A=Accountable (rechenschaftspflichtig), C=Consulted (zu konsultieren); I=Informed (zu informieren)

ment von Datensicherheit und Datenschutz einen DSDS-Verantwortlichen etablieren. Dieser wird gemeinsam mit dem EPD-Betreiber auch die Prozesse für die Erkennung und Behandlung von Sicher-heitsvorfällen vorantreiben. Es ist aber wichtig, dass auch die Sicherheits-beauftragten der teilnehmenden Gesundheitseinrichtungen in die Sicher-heitsorganisation der Gemeinschaft einbezogen werden, beispielsweise durch Einsitz in einem übergreifenden Security Board.

Was ist zu tun?

Den Spitälern in der Schweiz verbleiben noch gut zwei Jahre, um sich einer EPD-Gemeinschaft anzuschliessen. Angesichts der vielen zu klärenden Fragen ist dies wenig Zeit. Die meisten Stammgemeinschaften befinden sich heute in der Aufbauphase und diverse, auch grundsätzliche, Fragen sind noch nicht definitiv geklärt. Trotzdem sollte sich das Management bereits konkret damit auseinandersetzen, wie die EPD-Anbindung angegangen wird, welche Rolle das eigene Haus in der Gemeinschaft spielen soll und wie sich das EPD auf die internen Systeme und Prozesse auswirken wird. Eine aktive Aufbauarbeit aller Teilnehmer ist für jede Gemeinschaft essentiell und bietet die beste Gewähr dafür, dass aus dem Zusammenschluss schlussendlich ein für alle Beteiligten stimmiges Ganzes entsteht. ■

* *Geschäftsführer Temet AG*