Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
Conférence des directrices et directeurs cantonaux de la santé
Conferenza delle direttrici e dei direttori cantonali della sanità

Faktenblatt

Administrative Zugriffe auf das elektronische Patientendossier

Für den reibungslosen Betrieb des elektronischen Patientendossiers (EPD) und eine sinnvolle Anwenderunterstützung ist es notwendig, den Zugriff auf das EPD durch administrative Funktionen zu erlauben. Dabei ist grundsätzlich zwischen zwei Arten von Zugriffen zu unterscheiden.

Zum einen sind dies **Systemadministratoren**, welche die Systeme, auf denen die EPD-Infrastruktur aufgebaut ist, warten und den Betrieb sicherstellen. Zugriffe durch solche Systemadministratoren werden ausserhalb der IHE-Welt (z.B. direkt auf der Datenbank) getätigt und werden dadurch nicht durch das EPD-Berechtigungssystem durchgesetzt. Sie sind auch nicht im Patientenlog ersichtlich.

Zum anderen sind das administrative Funktionen, die für die korrekte Nutzung des EPD und eine inhaltliche Anwenderunterstützung notwendig sind. Zugriffe durch solche administrativen Funktionen werden innerhalb der IHE-Welt getätigt und somit auch durch das EPD-Berechtigungssystem durchgesetzt. Sie sind damit im Patientenlog ersichtlich. Administrative Funktionen verlangen eine starke 2-Faktor Authentisierung gemäss TOZ (Technische und organisatorische Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften - Anhang 2 der Verordnung des EDI zum EPD) Ziffer 4.13.1 a. Für das EPD wurden zwei solcher Funktionen eingeführt - der **Document Administrator** und der **Policy Administrator**. Die Aufgaben, die vom Policy Administrator wahrgenommen werden können, werden in der TOZ Ziffer 4.8.4 genauer beschrieben.

Aufgaben und Funktionen der administrativen Funktionen

Die **Systemadministratoren** sind zuständig für den reibungslosen Betrieb der EPD-Gemeinschaftsinfrastrukturen. Zu ihren Aufgabengebieten gehören unter anderem Monitoring (z.B. Disk space, Performance, Auslastung, etc.), Patchen von Betriebssystem, Virenschutz und weiteren Softwarekomponenten, Härten der Systeme, um sie gegen Angriffe sicherer zu machen, Datenbankoptimierungen, Systemmigration und das Backup von Daten.

Der **Document Administrator** unterstützt die Benutzer bei Bedarf beim Umgang mit Dokumenten im EPD. Der Document Administrator hat die Berechtigung, Dokumente aller Vertraulichkeitsstufen zu sehen (normal zugänglich, eingeschränkt zugänglich und geheim). Damit kann der Document Administrator Patienten und Gesundheitsfachpersonen folgende Unterstützung bieten.

Um Patienten zu unterstützen kann der Document Administrator im Auftrag eines Patienten/einer Patientin:

- Metadaten von Dokumenten ändern (insbesondere Ändern der Vertraulichkeitsstufe von annullierten Dokumenten im Auftrag der Stammgemeinschaft des Patienten oder der Patientin).
- Dokumente durch das Setzen des Löschflags (Metadatum «deletionStatus») löschen.

Schwarzenburgstrasse 157
CH-3003 Bern
www.e-health-suisse.ch

ehealthsuisse
Kompetenz- und Koordinationsstelle von Bund und Kantonen
Centre de compétences et de coordination de la Confédération et des cantons
Centro di competenza e di coordinamento di Confederazione e Cantoni

Um Gesundheitsfachpersonen zu unterstützen kann der Document Administrator im Auftrag einer Gesundheitsfachperson:

- Dokumente, die im falschen Dossier publiziert wurden, durch das Setzen des Löschflags löschen.

Weiter kann der Document Administrator:

- bei Aufhebung eines Dossiers nach verbliebenen Dokumenten suchen und diese durch Setzen des Löschflags löschen (solange die Berechtigungen noch nicht gelöscht sind).

Während der Document Administrator Dokumente im EPD gemeinschaftsübergreifend lesen kann, ist das Publizieren von Dokumenten und ändern von Metadaten (inkl. Setzen des Löschflags) nur gemeinschaftsintern möglich.

Der **Policy Administrator** wird verwendet, um beim Eröffnen eines Dossiers die initialen Berechtigungen im Policy Repository anzulegen (Bootstrap Policies) und allfällig gewünschte Startkonfigurationen für den Patienten/die Patientin vorzunehmen (z.B. Standardvertraulichkeitsstufe für neue Dokumente, Stellvertretung benennen, etc.). Zudem kann der Policy Administrator die Berechtigungen bei Aufhebung eines Dossiers wieder löschen. Zwischen diesen beiden Ereignissen darf der Policy Administrator keine Berechtigungen manipulieren. Diese Einschränkung, dass der Policy Administrator nur am Anfang und Ende eines EPD-Zyklus Policies manipulieren darf, wird technisch nicht durchgesetzt und muss deshalb organisatorisch geregelt werden.

Um den zeitlichen Aufwand für administrative Aufgaben möglichst gering zu halten, ist es durchaus möglich, administrative Prozesse zu automatisieren. Zum Beispiel könnte so ein Document Administrator oder Policy Administrator sich mit Zweifaktorauthentifizierung am System anmelden und dann unterstützt durch das System automatisiert die Berechtigungen anlegen lassen für alle neu zu eröffnenden Dossiers oder nach verbleibenden Dokumenten eines Dossiers suchen, das aufgehoben werden soll, um diese mit dem Löschflag zu versehen.

Wer darf welche Funktion wahrnehmen?

Die Verantwortung für die Vergabe von administrativen Funktionen und die damit verbundene Überprüfung der Einhaltung der Anforderungen obliegt den (Stamm-)Gemeinschaften. Die Funktion des Systemadministrators wird durch Mitarbeiter von Anbietern der Gemeinschaftsinfrastruktur (Plattformanbieter) wahrgenommen. Die Funktion des Document Administrator und Policy Administrator wird von geschultem Personal wahrgenommen, welches in Support- und Anlaufstellen (z.B. Eröffnungsstellen) der (Stamm-)Gemeinschaften tätig ist. Zudem wäre es für (Stamm-)Gemeinschaften denkbar in grösseren Gesundheitseinrichtungen einzelne Personen entsprechend zu schulen und mit gewissen administrativen Funktionen zu betrauen (z.B. ein Mitarbeiter in einem Spital zum Löschen von falscheingestellten Dokumenten durch Gesundheitsfachpersonen innerhalb des Spitals). Es ist nicht vorgesehen, dass Gesundheitsfachpersonen oder deren Hilfspersonen administrative Funktionen einnehmen.

Anforderungen an Personen, die eine administrative Funktion ausüben

Die TOZ beschreibt unter der Ziffer 4.8 die «Datenschutz- und Datensicherheitsanforderungen an das technische oder administrative Personal» von (Stamm-)Gemeinschaften. Die darin enthaltenen Anforderungen gelten für Systemadministratoren wie auch für den Document Administrator und den Policy Administrator. Ziffer 4.8.5. beschreibt zudem, dass administrative Zugriffe gemäss Ziffer 4.8.4 «nur in definierten Einzelfällen» erfolgen darf.