Anwendungsbeispiel: Austausch von Patientendaten

1. Beschreibung

Patienten werden in Kliniken eingewiesen. Für die dort behandelnden Ärzte und Krankenschwestern ist es wichtig die Vorgeschichte des Kranken zu kennen. Hierfür müssen verschiedene vertrauliche Dokumente zwischen externen Ärzten und Klinik-Ärzten ausgetauscht werden, ohne dass Fremde Zugriff auf diese haben und die Daten der Patienten gesichert sind. Nach der Entlassung oder Überweisung in eine andere Klinik / Rehabilitation oder zurück zum Hausarzt bzw. behandelnden Facharzt können so auch die Klinik-Unterlagen an diese weitergeleitet werden. Bisher werden diese Informationen aus Sicherheitsgründen nicht elektronisch verschickt. Eine sichere, elektronische Übermittlung würde in vielen Situationen schnelleren Zugriff auf diese Informationen ermöglichen.

2. Anforderungen

- Gemeinsamer Onlinespeicher für sicheren Dateiaustausch zwischen Kliniken, zwischen niedergelassenen externen Ärzten sowie zwischen Ärzten und Kliniken
- höchste Sicherheit für Daten von Patienten – alle Daten sind vertraulich
- möglichst einfache Nutzung ohne Bedarf an Training
- Echtzeitbenachrichtigung (eMail oder Benachrichtigungston) über Eingang neuer Dokumente
- sicherer Nachrichtenaustausch zwischen den zugangsberechtigten Personen
- jederzeit Zugriff vom PC und von mobilen Geräten wie Tablets und ggfs. Smartphones aus
- einfache Verwaltung – hinzufügen und entfernen von zugangsberechtigten Personen und Patienten-Ordnern
- rückstandsfreies Löschen des Onlinespeichers z.B. nach Übertragen der Daten eines Patienten ins Archiv nach seiner Entlassung
- geringe Kosten je Lizenz und Patientenakte.

3. Betrachtete Lösungsoptionen

1) eMail
   Patientenakten, Röntgenbilder etc. sind oft zu groß für einen Austausch per eMail. Außerdem müsste für alle Beteiligten die Etablierung von eMail-Verschlüsselung geklärt werden, die oft nicht vorhanden ist. Ein gemeinsamer Speicher für mehrere Personen fehlt.
   Ergebnis: Anforderungen nicht erfüllt

2) Bestehendes Informationssystem eines Klinikums
   Hier werden die meisten Anforderungen erfüllt. Es hat sich jedoch als schwierig erwiesen, externen Nutzern einen Zugriff auf interne Systeme zu gewähren bzw. die Systeme verschiedener Kliniken und Ärzte miteinander zu verbinden.
   Ergebnis: Anforderungen nicht erfüllt

3) Öffentliche Dienste für einen gemeinsamen Dokumentenspeicher (file-sharing)
   Diese Dienste bieten einfachen und bequemen Zugang sowie Nutzung. Leider erfüllen sie nicht die Sicherheitsanforderungen von Kliniken. Außerdem dürfen Ärzte die Daten und Dokumente ihrer Patienten nicht auf Systemen speichern, wenn der Anwender eines Dienstes (Service Provider) prinzipiell auf die Dokumente zugreifen könnte.
   Ergebnis: Anforderungen nicht erfüllt

4) Datenraumdienste
   Diese Dienste sind bekannt als Dokumentenspeicher für vertrauliche Vertragsverhandlungen und ähnliche Anwendungsfälle. Sie bieten ein hohes Maß an Sicherheit und erfüllen viele der genannten Anforderungen. Die Dienste sind jedoch sehr teuer und erfordern zumeist höheren Verwaltungsaufwand.
   Ergebnis: Anforderungen weitgehend erfüllt jedoch teuer und aufwendig

5) iDGARD Dienst
   iDGARD erfüllt alle Anforderungen bei geringen Kosten, einfacher Nutzung und Verwaltung. Außerdem schließt iDGARD durch die ihm zugrunde liegende Sealed Cloud Technologie, als einziger Dienst den Zugriff des

Anbieters (Service Providers) auf die Daten seiner Anwender aus. Damit ist iDGARD einzigartig sicher, denn nur der Eigentürmer der Daten kontrolliert vollständig den Zugriff auf seine Daten.
Ergebnis: Anforderungen erfüllt

4. Konkreter Einsatz von iDGARD

Nach einer Analyse wird iDGARD für einen ersten Probedurchgang eingesetzt. Die Registrierung des Krankenhauses bzw. einer einzelnen Station bei iDGARD dauerte nur zwei Minuten. Anschließend kann iDGARD sofort verwendet und den Mitarbeitern Zugänge eingeräumt werden.
Ein Nutzer kann nun innerhalb von wenigen Sekunden eine Privacy Box, d.h. ein elektronisches Schließfach für Dokumente, anlegen und gleichzeitig die behandelnden Ärzte und ggfs. das Pflegepersonal dort integrieren. Insgesamt steht ein Pool mit 100 GB Speicherplatz im Starter-Paket für alle Lizenzen zur Verfügung, innerhalb derer bis zu 2.000 solcher Privacy Boxen angelegt werden können. Weiterer Speicher kann bei Bedarf flexibel und individuell dazu gebucht und sofort genutzt werden.

Sind Funktionen wie Journal, Wasserzeichen oder Dokumente nur zur Ansicht notwendig, lässt sich jede Privacy Box ganz einfach und schnell in einen Datenraum umwandeln.

Die internen Mitglieder einer Privacy-Box, wie behandelnde Ärzte und das Pflegeperson, werden vom verantwortlichen Verwalter, beispielsweise dem Stationsarzt oder der jeweiligen Oberschwester einer Station, per Auswahl aus dem iDGARD-Verzeichnis (eine Liste aller bisher angelegten User) zu einer Privacy Box hinzugefügt – ganz einfach, jeweils nur mit einem Klick.
Darüber hinaus können Externe Zutritt zu einer Box bekommen, wenn beispielsweise die Patientenakte des Hausarztes für die Behandlung benötigt wird. So kann diesem sofort eine Zugangsberechtigung erteilt und jederzeit auch wieder entzogen werden. Der Hausarzt kann seine bisherigen Unterlagen, unter Wahrung geltender Datenschutzgesetze, in eine Privacy Box ablegen und diese so den Klinikärzten zur Verfügung zu stellen. Benötigt werden für die Einladung des Hausarztes lediglich seine eMail-Adresse und seine Mobilnummer, zur Übermittlung des Passwortes per SMS.

Alle Mitglieder einer Patienten-Box, intern (Volllizenz) und extern (Gastlizenz), nutzen die Privacy Boxen zum Austausch von Dateien, Dokumenten und Nachrichten sowie wichtige Notizen zu einem Patienten. Die Dokumente werden dabei in entsprechenden Verzeichnissen strukturiert, z.B. durch Unterordner für Hausarzt, Facharzt, Physiotherapie und Anweisungen für die Nachbehandlung u.v.m. – thematisch geordnet und für alle Zugangsberechtigten übersichtlich und sicher gespeichert.
Zugriff haben alle Box-Mitglieder per Internet-Browser (z.B. Firefox oder Internet-Explorer) von Ihrem Stations-PC auch mobil von überall über mobile Geräte wie Tablets und Smartphones auf die Unterlagen zugreifen. Für diese Geräte gibt es eine passende iDGARD App.

Zum Nachrichtenaustausch zwischen den zugangsberechtigten Personen gibt es verschiedene Methoden:

1) iDGARD Notizen für das Ablegen von Nachrichten, die für eine Nachverfolgung der Anweisungen parallel zu den jeweiligen Dokumenten des Patienten gespeichert werden per Internet-Browser oder App für mobile Geräte
2) iDGARD Chat für den Austausch in Echtzeit, d.h. eine sofortige Diskussion ist online möglich per Internet-Browser oder App für mobile Geräte
3) eMail steht natürlich weiterhin zur Verfügung für nicht schützenswerte Daten.

Generell zeigte sich, dass iDGARD intuitiv, ohne Training und ohne Softwareinstallation, sofort von sowohl internen Mitarbeitern als auch von den externen Ansprechpartnern genutzt werden kann.