Protokoll

Die Kommunikation im Gesundheitsbereich ist ein wichtiges Thema, das Austauschen sensibler Daten muss daher gut überdacht sein.

Wäre es sinnvoll per Mailing zu kommunizieren → Nein, wir haben keine Zustellbestätigung und der Schutz fehlt hier. Sensible Daten können hier also nicht verschickt werden, ein Hacker/Angreifer hätte sofortigen Zugriff darauf. Vielleicht haben auch mehrere Personen Zugriff auf eine E-Mail.

Mögliche Vorgehensweise:

- Portal
    - Ein Portal für die Kommunikation, so könnten Patienten an die sensible herankommen.
    - Per Mail dürfte nach Gesetz der Link/Pfad zu dem Portal versendet werden, die Anmeldedaten per Mail zu senden wäre nicht sinnvoll.
- Anmelden: Der Patient müsste im System bereits vorhanden sein, bevor dieser sich anmelden kann, es gibt auch andere Möglichkeiten, indem wir die Benutzerverwaltung nicht übernehmen, sondern externe Dienste verwenden wie die Handysignatur.
- Vorteile vom Portal
    - Dokumentenablage
    - Nachweis, dass Patient sich zu einem bestimmten Zeitpunkt eingeloggt hat.
    - 24/7 erreichbar? Innerhalb der Organisation kann man ermöglichen, dass unser Portal auf unserem Server 24/7 läuft. Jedoch kann man niemals garantieren, dass die Verbindung zum Portal auf der Seite des Users besteht. Beispielweise hat der User keine Verbindung zum Internet, wegen eines Stromausfalles. Unser Server läuft, trotzdem kann der User keine Verbindung zum Portal herstellen.
    - Das heißt eine 24/7 Verbindung zwischen Client und Server kann man nicht garantieren.

IDAS: Bürgerkarte wird vom IDAS abgelöst: auch essenziell für Personen, welche die aus einem anderen Land kommen, so können diese Personen ihren Führerschein, etc. verwenden, um sich elektronisch zu identifizieren.

- Müssen alle Daten trotzdem verschlüsselt werden?
    - Alle sensiblen Daten müssen verschlüsselt sein, außer wenn man sich in einem gesicherten Bereich befindet, wo die Berechtigungen geregelt sind. (Bauliche Maßnahmen)
    - Außer genetische Daten, diese sind hoch sensibel und dürfen nur von bestimmten Gruppen angeschaut werden, diese darf man auch nicht speichern.

Wenn man sich nun in einem gesicherten Bereich befindet, und das Gerät (Client) welches man Z.B als Mitarbeiter verwendet auch gesichert ist, hat man trotzdem auf viele Faktoren zu achten. Wenn die Mitarbeiter auch von zuhause arbeiten können, steht es in ihrer Verantwortung, jegliche Information vor Anderen zu verstecken bzw. zu schützen. Personen ohne Berechtigungen könnten auf den Bildschirm schauen und die Informationen ablesen.