GATEKEEPER

FALLSTUDIE
Gesundheitswesen

Passwortlose Authentifizierung im Gesundheitswesen

DAS SZENARIO

> *“Der Schutz sensibler Patientendaten hat höchste Priorität.”*

Gesundheitsdaten fallen ebenso wie genetische und biometrische Daten natürlicher Personen, gemäß Artikel 9 der DSGVO in die Kategorie besonders schützenswerter personenbezogener Daten.

Digital Healthcare verlangt also eine **hohe Sensibilität beim Umgang mit Patienten- und Gesundheitsdaten**. Wegen der hohen Arbeitsbelastung ist das für die Beschäftigten im Gesundheitswesen eine Herausforderung.

Im eng getakteten Arbeitsalltag in Arztpraxen und in personell unterbesetzten Kliniken können so beim Thema Datenschutz Nachlässigkeiten entstehen: **Ärzte und Pflegepersonal wechseln ständig zwischen Patienten und Behandlungszimmern** und oft gibt es keine automatische Lösung fürs Sperren der Computer. Im Worst Case können nachfolgende Patienten andere Behandlungsdaten z.B. aus der elektronische Patientenakte ePa einsehen – dies ist jedoch den behandelnden Ärzten vorbehalten.

Daraus ergeben sich drei Herausforderungen an die IT im Gesundheitswesen:

- Wie stellt man sicher, dass alle unbeaufsichtigten Behandlungs-Computer zu 100 % gesperrt sind?
- Wie lässt sich die Compliance einhalten und nachweisen, wer welche Eingaben durchgeführt hat?
- Wie erreicht man eine optimale Balance zwischen Datensicherheit und schnellen Datenzugriffen?

Eine Gemeinschaftspraxis in Calgary, Kanada hat diese IT-Herausforderungen lösen können, wie in dieser Fallstudie gezeigt wird. Die Herausforderungen und Ergebnisse treffen auch in der EU zu.

DIE HERAUSFORDERUNGEN

1. Wie stellt man sicher, dass alle unbeaufsichtigten Behandlungs-Computer zu 100 % gesperrt sind?

In der kanadischen Gemeinschaftspraxis behandeln drei Ärzte durchschnittlich je 50 Patienten pro Tag. Daraus ergeben sich mindestens 150 Anmeldungen und 150 Abmeldungen pro Tag am Praxis-Netzwerk.
Durch die Nutzung eines **Hardware Token mit Bluetooth Smart Technologie** (wie im Bild oben) melden sich alle Verantwortlichen automatisch an den Computern in den Behandlungszimmern an, sobald sie einen definierten Nahbereich erreichen. Der Nahbereich kann je nach räumlichen Gegebenheiten von 30 cm bis auf mehrere Meter eingestellt werden.
Verlassen Ärzte oder Personal den Nahbereich, sperrt sich der PC sofort wieder. Mögliche menschliche Versäumnisse durch vergessenen Logout o.ä. sind ausgeschlossen.
Wartet der nächste Patient im Behandlungszimmer, ist bei Bluetooth Token sichergestellt, dass die Daten der vorherigen Patientin nicht offen einzusehen sind.

> *“Sich wenige Male am Tag einzuloggen, gehört für viele dazu. Aber diese Prozedur dann 50-mal am Tag?*
> *Mit Bluetooth Token geht das schneller und einfacher.”*

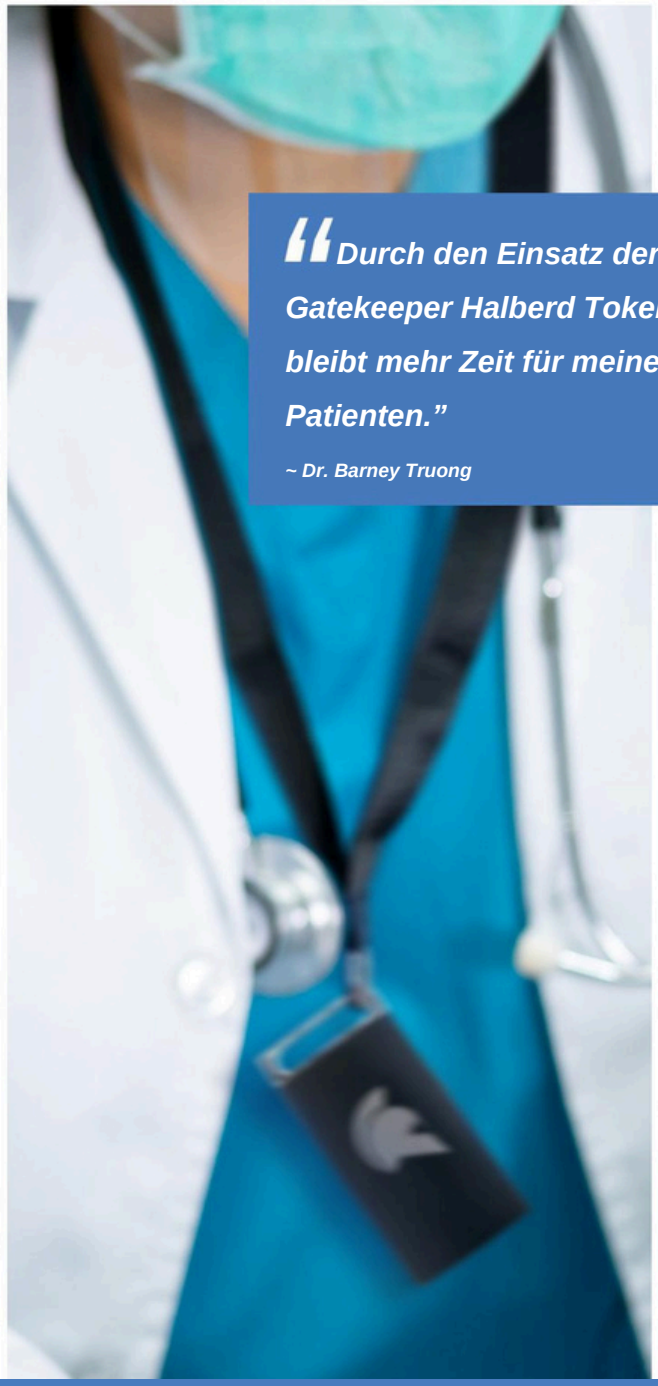
2. Wie lässt sich die Compliance einhalten und nachweisen, wer welche Eingaben durchgeführt hat?

Die Sensibilität von Behandlungs- und Gesundheitsdaten erfordert eine Nachvollziehbarkeit, wenn etwas geändert oder veranlasst wurde. Und zwar auch, wenn sich mehrere Kolleg:innen einen Computer oder sogar einen Geräte-Account teilen. Mit einem **Bluetooth-Token erfolgt die Anmeldung ohne weitere Interaktion sicher und automatisch**, nur durch die Annährung des Token ans Gerät. Jeder Bluetooth Token ist dabei genau einer:m Mitarbeitenden zugeordnet.
Damit ist jederzeit nachweisbar, wer wann an welchem Computer eingeloggt war. So kann man auch nachvollziehen, wer welche Behandlungs- oder Patientendaten geändert hat.

3. Wie erreicht man eine optimale Balance zwischen Datensicherheit und schnellen Datenzugriff?

In der Gemeinschaftspraxis gehen die Logins mit Bluetooth Token – ohne Einschränkungen bei der IT-Sicherheit – nun etwa **4-mal schneller als vorher**.
Multipliziert mit der Anzahl an Logins pro Tag, ergibt sich dadurch eine **signifikante Steigerung der Netto-Behandlungszeit für jeden Patienten**.

Die kanadische Gemeinschaftspraxis hatte auch verschiedene 2FA-Methoden getestet. Jedoch hat sich, wegen der Wartezeiten z.B. auf OTP oder Push-Notification, die Dauer der Logins (gegenüber bisheriger Passwort-Eingabe) nahezu verdreifacht.



> *"Durch den Einsatz der Gatekeeper Halberd Token bleibt mehr Zeit für meine Patienten."*
>
> *~ Dr. Barney Truong*

DIE LÖSUNG

Mit dem **GateKeeper Halberd Bluetooth Token** wurde es für Ärzte und die Pflegekräfte möglich, sich nur **durch Annähern schnell und sicher** an den Behandlungs-PCs anzumelden.
Umgekehrt werden sie beim Verlassen des Bereichs nun automatisch abgemeldet, was für den gebotenen Datenschutz sorgt.

FAZIT

Bluetooth Token, welche einen annährungsbasierten Login ermöglichen, bieten der Gemeinschaftspraxis in Calgary erhebliche Vorteile. Sowohl die Zeit-Effizienz als auch die Sicherheit der Computer-Systeme konnte verbessert werden.
Zudem konnte man durch den schnelleren Zugang zu elektronischen Patientenakten die Netto-Behandlungszeit erhöhen bzw. mehr Patient:innen pro Tag behandeln.

Die Implementierung der **GateKeeper Halberd Token**-Lösung hat zu **signifikanten Verbesserungen** der IT-Sicherheit, zu besser geschützten Patientendaten und zu effizienteren Arbeitsabläufe geführt.
Dies unterstreicht die **Bedeutung zeitgemäßer Authentifizierungsmethoden für das Gesundheitswesen**.

GATEKEEPER Proximity

ProSoft
SECURE|MANAGE|OPTIMISE IT

Kontakt:
+49 8171 405-200
info@prosoft.de
www.prosoft.de