

Die digitale Identität in der Arztpraxis in Verbindung mit cloudbasierter Arztsoftware.

Identität ist, was uns einzigartig macht.

Diese Definition unserer Identität wird in der digitalen Welt auf den Kopf gestellt, weil die Einzigartigkeit uns nicht mehr besonders sondern nur noch berechenbar macht. Zwar bleibt die Identität, auch in der digitalen Welt, eine Ansammlung von Attributen die uns eindeutig identifizierbar macht – diese wird jedoch, ohne unser Wissen, mit weiteren Daten angereichert. Dadurch werden wir nicht Individueller, wie die Anreicherung vermeintlich einzigartiger Daten über uns zunächst vermuten lassen könnte, sondern wir werden vorhersagbarer, berechenbarer. Künstliche Intelligenzen und Algorithmen stellen uns in Bezug zu anderen Menschen und ermöglichen so, unter Einbeziehung von Wahrscheinlichkeiten, relativ genaue Vorhersagen über uns. Diese Vorhersagen führen die Identität aber ad absurdum: Wie ist meine politische Überzeugung, meine Wahrscheinlichkeit einen Herzinfarkt zu bekommen, wie alt werde ich statistisch gesehen werden, wo liegen meine Interessen und welche wahrscheinliche Finanzkraft in Abhängigkeit von meinem Familienstand und meinem Wohnort, habe ich. Am Ende dieses Prozesses bin ich kein Individuum mit eigener Identität mehr, sondern lediglich, in Bezug auf cloudbasierte Arztsoftware, ein Asset des Gesundheitssystems oder bestenfalls ein gläserner Patient.

In einer digitalen Welt, nach dem Wunsch des Bundesgesundheitsministers, soll der Patient lediglich über eine digitale Identität gegenüber dem überall verfügbaren Datensatz der cloudbasierten Arztsoftware identifizierbar sein und wird somit nicht viel mehr als eine Fußnote von genau diesem Datensatz. Eine persönliche Arzt-Patient-Beziehung spielt keine Rolle mehr – der Leistungserbringer ist austauschbar. Das spart Kosten, da die verfügbaren Ressourcen effizienter eingesetzt werden können. Nur wo ist die Grenze der Kostenersparnis? Bekomme ich die überlebenswichtige Organtransplantation noch bewilligt, wenn der Algorithmus meine verbleibende, wahrscheinliche Lebensdauer als zu gering einschätzt?

Nur um das klar zu stellen: Die Digitalisierung ist nicht mehr aufzuhalten – und letztlich auch zum Wohl der Menschen. Zukünftige Generationen (digital Natives – die heute 10- bis 20-Jährigen) verstehen die Bedenken gegen die Datenkraken im Internet gar nicht. Für sie ist es normal, dass ihre vielfachen digitalen Identitäten (mindestens eine je Dienst) miteinander verknüpft, mit dem Nutzerverhalten angereichert und ausgewertet werden. Ist doch „cool“, wenn Amazon schon weiß was ich will - noch bevor ich es selbst weiß. Es kommt jetzt darauf an, die Digitalisierung für den Menschen nutzbringend zu gestalten und nicht zum reinen Marketing-Werkzeug verkommen zu lassen. Nicht nur im Gesundheitssektor – aber hier im Besonderen.

Medizinische Daten und die dazugehörige Identität sind ungeeignet für eine unkontrollierte Anreicherung durch Metadaten und noch ungeeigneter für die Auswertung durch Industrie und Wirtschaft. Eine Cloud basierte Arztsoftware bzw. eine Cloud basierte Datenbank kann unberechtigte Zugriffe nicht verhindern. Das haben Hacker-Angriffe, auch bei hoch professionellen Unternehmen, vielfach gezeigt. Medizinische Daten gehören zu den sogenannten „Besonders schützenswerten

Daten“, einem Begriff aus der DSGVO (Datenschutz Grundverordnung), der alle Daten, die in die Privatsphäre des Menschen greifen, erstmals besondere Beachtung schenkt und diese in einen gesetzlich geschützten Rahmen stellt. Nur leider ist dieser gesetzliche Rahmen durchlässig – das s.g. „Berechtigte Interesse“ kann häufig verwendet werden, um doch wieder Zugriff auf diese Daten zu erhalten. Darüber hinaus können von der jeweiligen Landesgesetzgebung Teile der DSGVO per Gesetz ausgeklammert werden (Landesgesetze können über den europaweiten Regelungen der DSGVO stehen.) Die DSGVO ist dennoch ein Schritt in die richtige Richtung zum Schutz persönlicher Daten in der Digitalen Welt.

In dem Moment, in dem diese besonders schützenswerten Daten das geschützte Umfeld der Arztpraxis also verlassen, was in einer Cloud basierenden Lösung das normale Vorgehen ist, kommt der digitalen Identität eine besondere Bedeutung zu. Sie wird zum Schlüssel für den Zugriff auf diese, meine Daten. Der Zweifler könnte jetzt einwenden, dass der Datensatz in einer Arztpraxis nicht sicherer ist. Das ist zwar grundsätzlich richtig – betrifft aber im Verhältnis nur wenige hundert bis wenige Tausend Datensätze – nicht die über 80 Millionen aller Patienten in Deutschland.

Self-sovereign Identity, die selbstverwaltete Identität, wird hierfür angepriesen: Der Mensch als Eigentümer seiner eigenen Identität und aller mit ihr verknüpften Daten, entscheidet selbst, z.B. über eine App am Smartphone, welche Daten er preisgeben möchte. Sichergestellt werden soll das über eine transnationale Identität (also weltweit einheitlich gültig) auf der Basis von nicht fälschbaren Blockchain-Verfahren. Es verbleiben jedoch auch in diesem Konzept viele offene Fragen: wie detailliert können die Daten freigegeben werden? – Gibt es nur eine Kategorie „Medizinische Daten“ und mein Augenarzt erfährt, z.B. dass ich einen vererbten Senk-Spreizfuß habe. Oder werden die Daten so detailliert untergliedert, dass man seitenweise (Und damit ggf. minuten- oder gar stundenlang) durch Optionen klicken muss, bis man genau den Datensatz hat, den man bereit ist weiterzugeben? Und wie sollte verhindert werden, dass die Digitale Identität nicht doch im Hintergrund mit weiteren Daten angereichert wird? Möglich wäre zusätzliche Anreichern durch einen zweiten, offener zugänglichen Datensatz, der jedes Mal einfach aus der Cloud nachgeladen wird, wenn eine digitale Identität irgendwo genutzt wird. Und was ist mit zukünftigen Technologien – wer kann garantieren, dass heute geschützte Daten auch morgen noch sicher sind. Der Quantencomputer, der jegliche Verschlüsselung in Sekundenbruchteilen entschlüsseln kann, ist keine reine Theorie mehr. In Bezug auf die Blockchain-Technologie sollte es also besser heißen: Noch nicht fälschbar...

Eine digitale Identität wird also niemals in der Lage sein meine analoge Identität – also mein reales Sein – zu ersetzen. Und am allerbesten muss ich meine Identität gar nicht nachweisen, einfach nur, weil der Arzt / die Ärztin meines Vertrauens mich über eine langjährige Arzt-Patient-Beziehung eh bestens kennt. Dieses besonders hohe Maß an Schutz meiner persönlichen Patientendaten wird eine digitale Identität niemals erreichen können.