Datenschutz in der Cloud - Auf den richtigen Partner kommt es an!

Cloud Computing ist sicher ein sehr kontrovers diskutiertes Thema unter IT-Verantwortlichen in Krankenhäusern. Entgegen dem allgemeinen Hype rund um Applikation in der Datenwolke, ist im deutschen Gesundheitswesen eher eine skeptische Grundhaltung festzustellen.

In der Diskussion stellt sich häufig die Problematik, dass keine eindeutige Definition des Begriffes Cloud Computing existiert. Stattdessen handelt es sich um einen Sammelbegriff, der unterschiedlichste Serviceangebote – wie Infrastruktur-, Plattform- und Softwareangebote – umschreibt. Neben dieser technischen Sichtweise findet sich in der Literatur auch immer eine Differenzierung nach organisatorischen Aspekten (private, öffentliche oder hybride Cloud), die praktisch den Grad der Nutzungsexklusivität beschreibt. Eine weitere Herausforderung stellt die Heterogenität daraus resultierender möglicher Vertragstypen (Miet-, Service oder Werkvertrag) mit ihren unterschiedlichen Abrechnungsmodalitäten (zum Beispiel Pay-per-use oder Abrechnung von Zeiteinheiten) dar.

Vor dem Hintergrund dieser komplexen Abhängigkeiten fallen die Einordnung der eigenen Rechte und Pflichten sowie die Abschätzung möglicher Risiken im Einzelfall häufig schwer.

Rechtliche Rahmenbedingungen

Die normativen Rahmenbedingungen, wie Datenschutzgesetze, ärztliche Schweigepflicht und SGB, sind analog auch auf die Nutzung eines Cloud- Angebotes anzuwenden. Ist es dem Provider grundsätzlich möglich, im Rahmen seiner Leistungserbringung auf personenbezogene Gesundheitsdaten zuzugreifen, so müssen mindestens die Voraussetzungen für eine Datenverarbeitung im Auftrag (gemäß BDSG §11) erfüllt sein. Der Provider darf nur als „verlängerter Arm“ des Servicenehmers tätig werden. Gleichzeitig bleibt dieser in der Verantwortung, die Sicherheit und Integrität der Daten zu gewährleisten. Viele Angebote zielen jedoch gerade auf die Entlastung des Dienstenutzers von diesen Aufgaben ab, sodass sich ein möglicher Interessenkonflikt ergeben kann.

Ein weiterer wichtiger Aspekt bei der Verarbeitung von Gesundheitsdaten („personenbezogene Daten der besonderen Art", vgl. §3 Abs. 9 BDSG, EG Richtlinie 95/46/EG) stellt die Schweigepflicht dar, die sich aus der Musterberufsordnung für Ärzte und dem Strafgesetzbuch(StGB §203) ergibt. Sie gilt auch für Menschen, die in Heilberufen tätig sind, für Apotheken, Psychologen und Mitarbeitende der Versicherungsträger.

Eine Verarbeitung ist dann nur zulässig, sofern eine ausdrückliche gesetzliche Grundlage oder eine

andere Rechtsvorschrift dies erlaubt bzw. anordnet, was im Kontext des Cloud Computing im Allgemeinen verneint werden kann. Andernfalls müsste der Betroffene einwilligen, dass sein Recht auf informationelle Selbstbestimmung eingeschränkt wird. Der Gesetzgeber fordert in diesen Fällen eine sogenannte „informierte Einwilligung“ (§ 4a Abs. 1 Satz 2 BDSG).

Datenverarbeitung in Deutschland

Die Nutzung von Cloud-Angeboten erfolgt in der Regel über das Internet und ist somit nicht an geographische Grenzen gebunden. Als Servicenehmer sollte man daher darauf achten, dass keine Datenverarbeitung außerhalb des europäischen Wirtschaftsraumes erfolt. Um sicherzustellen, dass in jedem Fall deutsches Datenschutzrecht zur Anwendung kommt, sollte ein Anbieter mit Serverstandort in Deutschland gewählt werden.

Dieser Aspekt sollte kritisch geprüft und vertraglich festgehalten werden. Es ist nicht unüblich, dass der Anbieter einer Softwarelösung selbst wiederum Serviceangebote auf Plattform- oder Infrastrukturebene nutzt und trotz deutscher Anbieterkennung letztendlich eine Datenverarbeitung und -speicherung außerhalb der EU erfolgt („Subcontracting-Problematik“).

Verfügbarkeit, Vertraulichkeit und Integrität

Die bekannten Schutzziele gelten un- verändert auch bei der Nutzung eines cloud-basierten Serviceangebotes. Die Zusicherung der Schutzziele – insbesondere der Verfügbarkeit des Serviceangebotes – sollte mit dem Provider auf Basis sogenannter Service Level Agreements (SLA) vertraglich vereinbart werden.

Das SLA spezifiziert unter anderem die durchschnittliche Verfügbarkeit (zum Beispiel im Jahresmittel) und auch Reaktionszeiten bei Fehlerfällen, Fehlerschwere. Für jeden Dienstneh- mer sollte das SLA eine vertragliche Kernkomponente eines Cloud-Service- Angebotes darstellen.

Fazit und Ausblick

Aus informationstechnischer Sicht wäre eine Datenverarbeitung außerhalb der eigenen Räumlichkeiten ausschließlich in pseudonymisierter Form wünschenswert. Jedoch werden erst zukünftige Softwaregenerationen dies umfassend unterstützen können. Besonderes Augenmerk muss daher auf die Auswahl des Cloud-Anbieters gelegt werden, sodass eine dem deutschen Datenschutzrecht konforme Verarbeitungerfolgt. Dabei sollten auch Umfang und Güte des Angebots in jedem Fall vertraglich definiert und ein SLA festgelegt sein. Empfehlenswert ist die aktive Beteiligung des zuständigen (Landes-)Datenschützers bereits in einer frühen Phase der Umsetzung einer Cloud-Strategie. Es gilt: Auf den richtigen Partner kommt es an!

Verfasst am: Montag, 10. September 2012 - 9:00
Autor: Prof. Dr. Thomas Jäschke
Herausgeber: iSOFT Magazine [1]

Ausgabe: Januar 2012
Copy: Erledigt

Links
[1] http://www.isofthealth.com/de-DE/Downloads/iSOFT Magazin.aspx