Medizinische Transkription im Ausland

Der Zeilenpreis sinkt – und der Risiko- und Kontrollberg wächst

Offerten aus dem grenznahen Ausland locken mit genügend Personal, tieferen Kosten und scheinbar vollständigem Vertragswerk. Doch mit dem Auslandzugriff wachsen Nachweis-, Kontroll- und Reaktionspflichten sowie die Rechtsunsicherheit. Der Auftrag kann Grenzen überschreiten, aber die Verantwortung bleibt im Spital.

Der interne Schreibdienst ist unterbesetzt, die Berichtsrückstände wachsen, zusätzliche Stellen liegen nicht im Budget. Da trifft die Offerte aus Deutschland ein: medizinische Fachterminologie, tieferer Zeilenpreis, ISO-zertifiziert, Auftragsbearbeitungsvertrag inklusive.

Die Lücke steht nicht in der Offerte

Die Offerte liefert das Datenschutz-Argument gleich mit: Deutschland stehe in Anhang 1 der Datenschutzverordnung, die Bekanntgabe brauche keine zusätzlichen Garantien. Das stimmt – und ist trotzdem die kleinste der anstehenden Fragen. Häkchen gesetzt, Business Case gerechnet, unterschriftsreif?

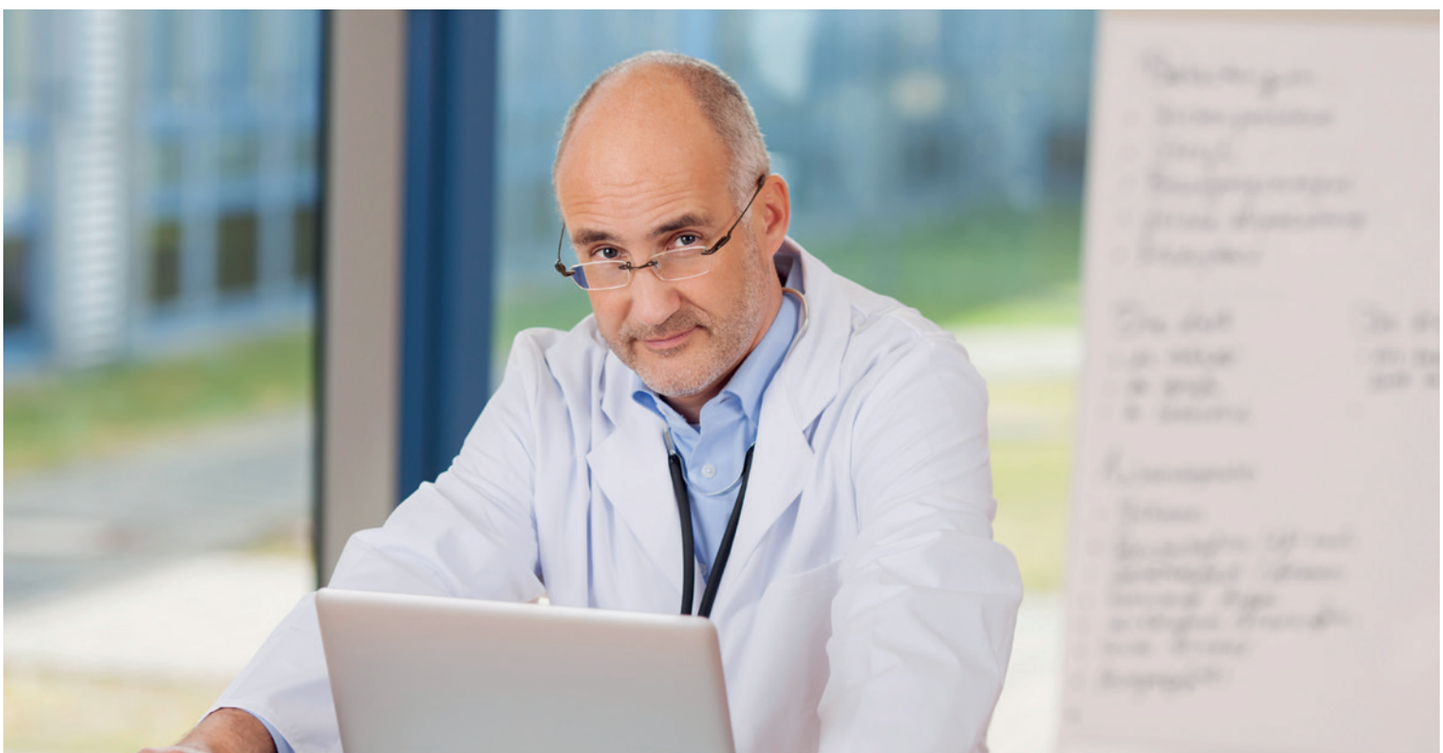
Angemessen ist nicht genug

Nein. Die Angemessenheit beantwortet nur eine Teilfrage. Sämtliche übrigen Pflichten bleiben bestehen: Zweckbindung, Datensicherheit, Information der Betroffenen, Kontrolle der Auftragsbearbeitung samt Unterauftragnehmern, bei hohem Risiko eine Datenschutz-Folgenabschätzung. Und: Eine Auftragsbearbeitung ist nur zulässig, wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht sie verbietet (Art. 9 Abs. 1 lit. b DSG).

Operations-, Psychiatrie- und Austrittsberichte enthalten zudem nicht nur besonders schützenswerte Personendaten, ihr Inhalt untersteht in aller Regel auch dem Berufsgeheimnis nach Art. 321 StGB. Eine datenschutzrechtlich zulässige Auslandbekanntgabe beantwortet die geheimnisrechtliche Frage noch nicht. Das Strafrecht kennt keine Staatenliste.

Ärztinnen und Ärzte dürfen Hilfspersonen beiziehen und dazu kann alles von der Praxissekretärin bis zum IT-Dienstleister gehören. Entscheidend ist nicht die Bezeichnung im Vertrag. Die Zugriffe müssen erforderlich sein, die Personen klar bestimmt, zur Geheimhaltung verpflichtet und wirksam in eine Weisungs- und Kontrollstruktur eingebunden sein. Das verlangen auch die kantonalen Datenschutzbeauftragten, zusammengeschlossen in der Konferenz privatim: Das blosse vertragsmässige Etikett «Hilfsperson» genügt nicht.

Deutschland kennt mit § 203 StGB einen eigenen Geheimnisschutz für mitwirkende Personen. Das Berufsgeheimnis fällt an der Grenze also nicht in einen rechtsfreien Raum. Ob sich beide Ordnungen in der konkreten Leistungskette aber lückenlos ergänzen – man denke an Transkription, Qualitätssicherung, Support, Homeoffice und jeden Unterauftragnehmer –, muss das Schweizer Spital prüfen und belegen können. Ein einfaches «Wir sind compliant» ersetzt diese Prüfung nicht.



Der Autor: Leander Isler ist Information Security & Compliance Consultant bei der Voicepoint AG, Anbieterin medizinischer Dokumentationslösungen mit Datenhaltung in der Schweiz.

An der Grenze wächst der Risiko- und Kontrollberg

Über die Grenze kommt ein zweiter Rechtsraum hinzu. Wer darf wo Klartext hören oder lesen? Welche Geheimhaltungspflicht gilt für welche Person? Welche Behörden können zugreifen? Wie sieht es in Notfallsituationen aus, wie in rechtlichen Konflikten? Wie werden Audit-, Lösch- und Weisungsrechte durchgesetzt? Grundsätzlich gilt das unabhängig davon, ob Menschen oder KI-gestützte Verfahren transkribieren: Entscheidend bleibt, wer wo Klartext erhält und welches Recht bindend ist.

Sogar die wohlwollendste öffentliche Einschätzung enthält Vorbehalte: Ein nicht rechtsverbindlicher Leitfaden der Zürcher KI-Innovation-Sandbox von 2025 hält Auslagerungen ins Ausland für öffentliche Spitäler grundsätzlich für möglich, weist aber auf erhöhte Risiken und zusätzliche Massnahmen hin. Der EDÖB führt demgegenüber aus, der Beizug von Dienstleistern im Ausland für die Bearbeitung medizinischer Personendaten sollte vermieden werden, weil ausländisches Recht nicht immer einen dem Art. 321 StGB gleichwertigen Schutz bietet. Das ist noch kein pauschales Verbot, aber ein deutliches Warnsignal, das eine Spitalleitung nicht mit einer Staatenliste abhaken kann.

Hochdeutsch reicht meistens nicht

Ein Posten, der in den wenigsten Offerten ausgewiesen ist: die Sprache. Medizinische Dokumentation in der Schweiz ist ein eigener Sprachraum. Der Austrittsbericht heisst in Deutschland Arztbrief, dazu kommen Kostengutsprache, Zuweiser, Präparatenamen, die es nur hier gibt, und Diktate mit Dialektfärbung. Wer das täglich hört, korrigiert nebenbei, und wer nicht, produziert Rückfragen und Korrekturschlaufen, die im Zeilenpreis nirgends auftauchen. Im schlechtesten Fall sind das Fehler im Bericht an die Zuweiserin. Entscheidend ist darum nicht der Firmensitz, sondern ob die Menschen im Transkriptionsprozess den schweizerischen Klinikalltag kennen. Diese Frage gehört in jede Ausschreibung und in jedes Pilotprojekt.

Überraschung ist keine Einwilligung

Eine konkludente Einwilligung reicht gemäss EDÖB nur so weit wie Bekanntgaben, die Durchschnittspatientinnen und -patienten vernünftigerweise erwarten können. Das Behandlungsteam gehört dazu, aber ein externes Schreibzentrum im Ausland kaum.

Wer Operations-, Psychiatrie- oder Austrittsberichte im Ausland hören und lesen lässt, darf nicht unterstellen, die Betroffenen hätten damit gerechnet. Schweigen macht aus einer Überraschung keine Einwilligung. Die Auslandbearbeitung muss transparent gemacht werden und je nach Konstellation braucht es zusätzlich eine Einwilligung zur Entbindung von der Schweigepflicht.

Die Verantwortung bleibt im Spital

Das Spital kann zwar die Arbeit delegieren, nicht aber seine Verantwortung. Es hat keine leichte Aufgabe, denn es muss den Anbieter auswählen, instruieren und überwachen, Unterauftragnehmer beherrschen, Betroffenenrechte ermöglichen und Vorfälle aufklären. Für Spitäler auf einer kantonalen Spitalliste kommt Zeitdruck hinzu: Meldepflichtige Cyberangriffe sind dem Bundesamt für Cybersicherheit grundsätzlich innert 24 Stunden nach Entdeckung zu melden. Eine lange Eskalationskette macht diese Uhr nicht langsamer.

Auch die Weiterverwendung der Daten, wie für Modelltraining, Produktverbesserung oder Benchmarking, braucht eine ausdrückliche Regelung. Ob und wozu ein Anbieter oder einer seiner Unterauftragnehmer die Daten über den Auftrag hinaus nutzen darf, muss im Vertrag stehen.

Mit Blick auf das elektronische Patientendossier hat der Bund auch Datenstandort und Rechtsraum gekoppelt: Die Datenspeicher müssen sich in der Schweiz befinden und schweizerischem Recht unterstehen (Art. 12 Abs. 5 EPDV). Kein ausdrückliches Verbot ausländischer Transkription – aber ein deutliches Signal für den Stellenwert der Datenhoheit bei sensiblen Gesundheitsdaten.

Öffentliche und öffentlich-rechtliche Spitäler müssen zusätzlich kantonales Informations- und Datenschutzrecht, Amtsgeheimnis und Outsourcing-Vorgaben beachten. Je nach Kanton und Risiko sind eine Datenschutz-Folgenabschätzung, Vorabkontrolle oder Konsultation der Aufsicht erforderlich. Wer diese Prüfung erst nach dem Zuschlag beginnt, riskiert den Projektstopp und, im Worst Case, Reputationsschaden.

Der Preis der Governance

An der Grenze steht kein Verbotsschild. Dort beginnt aber der steile Aufstieg über den eigentlichen Risiko- und Kontrollberg. Mit dem günstigeren Zeilenpreis auf der anderen Seite der Grenze kauft ein Spital einen zweiten Rechtsraum, mehr Zugriffspersonen und längere Reaktionswege mit ein.

Bleiben Daten, Bearbeitung und Zugriff in der Schweiz, garantiert das noch keine Sicherheit. Das kann aber die rechtliche und organisatorische Komplexität verringern und Audits sowie die Durchsetzung von Ansprüchen erleichtern. In den Business Case gehört deshalb neben dem Zeilenpreis auch der Preis der Governance – und dieser steht selten in der Offerte.

Fünf Fragen vor der Unterschrift

1. **Wer hat wo Klartextzugriff?** Transkription, Qualitätssicherung, Support, Homeoffice und Unterauftragnehmer erfassen.
2. **Welche Geheimhaltungspflicht gilt für welche Person?** Schutzkette, anwendbares Recht und Durchsetzbarkeit schriftlich beurteilen lassen.
3. **Wo liegen die Daten – und für welchen Zweck?** Audio, Text, Backups, Löschung und jede Sekundärnutzung prüfen.
4. **Ist das Spital innert Stunden handlungsfähig?** Meldewege, Logs, Forensik und Behördenanfragen testen.
5. **Wissen die Patientinnen und Patienten davon?** Auslandbearbeitung offenlegen und Einwilligungsbedarf prüfen.