Telemedizin ist nicht einfach ein Videotermin. Sie verändert, wie Patientinnen und Patienten Kontakt aufnehmen, wie medizinische Anliegen eingeschätzt werden und wie Informationen zwischen Ordination, Ambulanz und Klinikteam fliessen. Damit das sicher und verlässlich funktioniert, braucht es mehr als ein geeignetes Videotool: Entscheidend ist ein klarer End-to-End-Prozess – von der ersten Anfrage bis zur Dokumentation und Nachbetreuung.

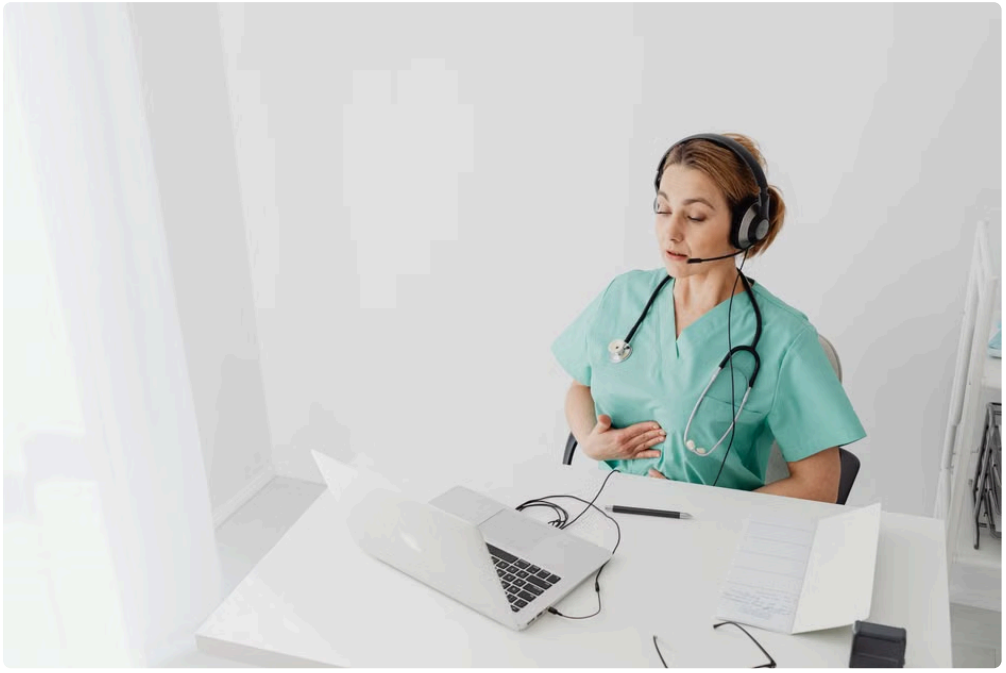
Gerade beim Thema **Datenschutz Telemedizin** entstehen Probleme oft nicht wegen eines einzelnen technischen Fehlers, sondern an Übergängen: Eine Anfrage landet im falschen Postfach, ein Befund wird über einen ungeeigneten Kanal übermittelt oder ein Teammitglied hat Zugriff auf mehr Daten als für die Aufgabe nötig. Ein gut gestalteter Ablauf macht Zuständigkeiten, Entscheidungen und Schutzmassnahmen daher konkret.

Dieser Beitrag zeigt, welche Prozessschritte in einer Praxis oder Klinik fix geregelt sein sollten und wo Einwilligung, Dokumentation und **Zugriffsrechte** verankert werden.

Telemedizin als End-to-End-Kette denken

Ein digitaler Patientenprozess beginnt nicht erst, wenn der Videoanruf startet. Er umfasst alle Stationen, an denen Gesundheitsdaten erhoben, geprüft, verwendet oder weitergegeben werden. Dazu gehören auch jene Schritte, die im Alltag gern als „nur organisatorisch“ betrachtet werden – etwa die Terminbestätigung oder die Weiterleitung einer Anfrage.

Eine typische Prozesskette sieht so aus:



1. **Kontaktaufnahme:** Die Patientin oder der Patient erreicht die Einrichtung über einen definierten Zugangskanal.
2. **Ersteinschätzung und Triage:** Das Anliegen wird nach festgelegten Kriterien eingeordnet; Dringliches wird erkannt und weitergeleitet.
3. **Terminierung:** Es wird entschieden, ob ein telemedizinischer Termin geeignet ist und wann er stattfindet.

4. **Vorbereitung:** Identität, Erreichbarkeit, benötigte Unterlagen und technische Voraussetzungen werden geklärt.
5. **Telemedizinischer Kontakt:** Die Beratung oder Behandlung erfolgt über einen freigegebenen Kanal.
6. **Dokumentation und Folgeprozess:** Gespräch, Entscheidung, Vereinbarungen und nächste Schritte werden nachvollziehbar festgehalten.

Für jeden Schritt braucht es eine klare Antwort auf drei Fragen: Wer ist verantwortlich? Welche Information wird benötigt? Was passiert, wenn der geplante Ablauf nicht funktioniert? Diese Fragen verbinden den medizinischen Prozess mit Datenschutz und Betriebssicherheit.

Zugangskanäle und Triage eindeutig festlegen

Patientinnen und Patienten nutzen oft mehrere Wege: Telefon, Webformular, Patientenportal, E-Mail oder eine bestehende Kassen- beziehungsweise Klinikplattform. Das ist für sie bequem, kann intern aber zu parallelen Postfächern, Doppelmeldungen und unklaren Zuständigkeiten führen. Legen Sie deshalb fest, welche Kanäle für welche Anliegen vorgesehen sind und wo eingehende Anfragen zentral bearbeitet werden.

Was bei der Triage geregelt sein muss

- Welche Anliegen für eine telemedizinische Einschätzung geeignet sind.
- Welche Warnzeichen eine sofortige telefonische oder persönliche Abklärung erfordern.
- Wer die Ersteinschätzung durchführt und wann medizinisches Personal übernimmt.
- Wie Rückfragen, nicht erreichbare Personen und ausserhalb der Öffnungszeiten eingehende Anfragen behandelt werden.
- Wie Patientinnen und Patienten über Notfallwege informiert werden.

Achtung: Ein Webformular oder ein Postfach ist kein Notfallkanal. Das muss für Patientinnen und Patienten an der passenden Stelle sichtbar sein – nicht nur in einer langen Datenschutzerklärung. Bei akuten Beschwerden braucht es eine klare Handlungsanweisung, etwa den Hinweis, die zuständige Notfallstelle oder den Rettungsdienst zu kontaktieren.

Die Triage soll nur jene Informationen erheben, die für die Einordnung tatsächlich notwendig sind. Fragen Sie beispielsweise nicht routinemässig nach einem vollständigen Krankheitsverlauf, wenn die erste Entscheidung lediglich lautet, ob ein Video- oder Präsenztermin benötigt wird. Weniger unnötige Datenerhebung bedeutet weniger Aufwand und ein geringeres Datenschutzrisiko.

Einwilligung: verständlich, passend und dokumentiert

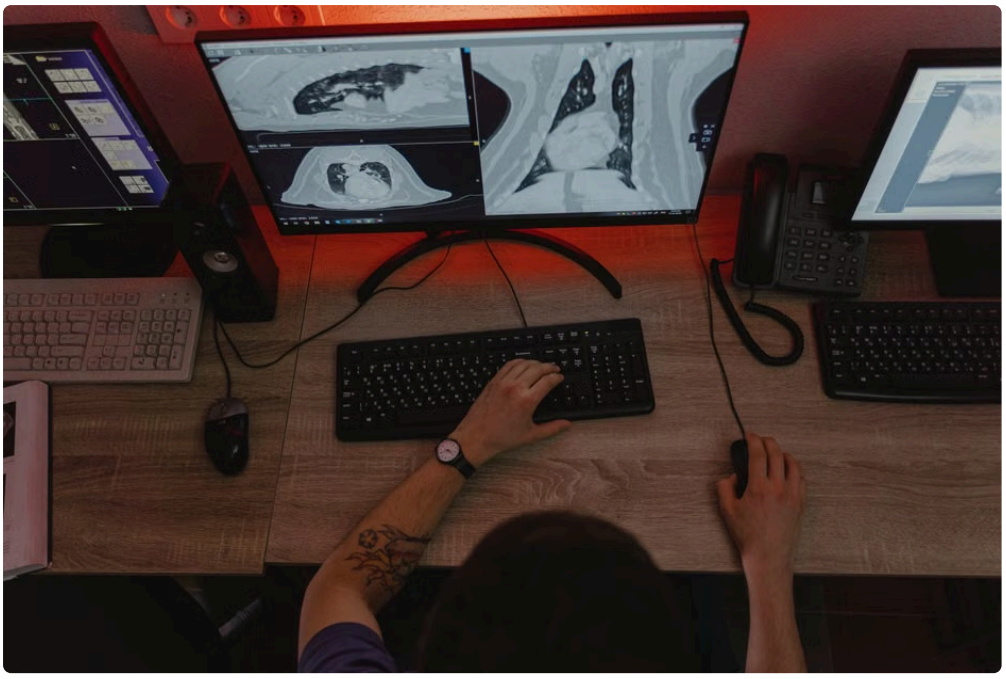
Die **Einwilligung des Patienten** ist kein einzelner Haken, der alle rechtlichen und organisatorischen Fragen löst. Je nach Verarbeitung kann eine datenschutzrechtliche Rechtsgrundlage auch unabhängig von einer Einwilligung bestehen. Die konkrete Beurteilung hängt vom Zweck, der Einrichtung und dem jeweiligen Ablauf ab. Holen Sie daher Datenschutzbeauftragte und gegebenenfalls Rechtsberatung frühzeitig ein, statt Einwilligung als pauschale Standardlösung zu verwenden.

Unabhängig davon sollte der Prozess sicherstellen, dass Patientinnen und Patienten wissen, was im telemedizinischen Kontakt passiert. Dazu gehören verständliche Informationen über:

- Art und Zweck des Termins, zum Beispiel Beratung, Verlaufskontrolle oder Befundbesprechung;
- den verwendeten Kommunikationskanal und allfällige Grenzen der Fernbehandlung;

- welche Daten verarbeitet und in der Patientenakte dokumentiert werden;
- welche Personen oder Berufsgruppen im Behandlungsteam die Angaben benötigen können;
- was bei technischen Problemen oder einem Abbruch des Gesprächs geschieht.

Wenn für einen konkreten Verarbeitungsschritt eine Einwilligung erforderlich ist, muss sie freiwillig, informiert und nachvollziehbar eingeholt werden. Der Prozess sollte ausserdem regeln, wie eine Ablehnung oder ein Widerruf behandelt wird und welche alternative Versorgung angeboten werden kann. Eine Ablehnung der Videoübertragung darf nicht dazu führen, dass die Person ohne angemessene Information oder nächste Schritte zurückbleibt.



Praktisch bewährt sich ein fest definierter Zeitpunkt: Die Information erfolgt bei der Terminvereinbarung oder vor dem Termin; die erforderliche Einwilligung wird vor Beginn des betreffenden Verarbeitungsschritts erfasst. So muss das Team nicht während des Gesprächs improvisieren.

Zugriffsrechte: nur so viel wie nötig

In telemedizinischen Abläufen arbeiten häufig mehrere Rollen zusammen: Administration, Pflege, Ärztinnen und Ärzte, IT-Support sowie gegebenenfalls externe Dienstleister. Nicht jede Rolle benötigt Zugriff auf dieselben Gesundheitsdaten. **Zugriffsrechte** sollten deshalb nach Aufgaben und Verantwortlichkeiten vergeben werden – nicht nach dem Prinzip „für alle Fälle Zugriff für alle“.

Rolle Typischer Zugriff im Prozess Wichtige Begrenzung Administration Kontaktdaten, Terminstatus und organisatorische Angaben Keine medizinischen Inhalte, sofern sie für die Aufgabe nicht erforderlich sind Medizinisches Team Für Behandlung und Verlauf notwendige Informationen Zugriff entsprechend Zuständigkeit und Behandlungsbezug IT-Support Technische Konten, Gerätestatus und Fehlerprotokolle Kein regulärer Zugriff auf Gesprächsinhalte oder Akteninhalte Externe Dienstleister Nur jene Daten, die für die vereinbarte Leistung erforderlich sind Rollen, Verantwortlichkeiten und vertragliche Datenschutzanforderungen klären

Verankern Sie im Prozess, wer Berechtigungen beantragt, freigibt und regelmässig überprüft. Ein Rollenwechsel, Austritt oder längerer Einsatzwechsel muss eine definierte Anpassung auslösen. Ebenso wichtig sind persönliche Benutzerkonten, eine sichere Anmeldung und nachvollziehbare Protokolle, soweit dies für Systeme und Zwecke angemessen ist.

Achtung: Ein gemeinsames Teamkonto wirkt im Alltag unkompliziert, erschwert aber die Nachvollziehbarkeit. Wenn später unklar ist, wer einen Eintrag geändert oder einen Befund geöffnet hat, fehlt eine wichtige Grundlage für die Aufklärung eines Vorfalls.

Der Termin selbst: Datenschutz im Arbeitsablauf

Vor dem Video- oder Telefontermin sollte klar sein, wer die Identität der teilnehmenden Person prüft und mit welcher angemessenen Methode. Die Prüfung muss zum Risiko passen und darf nicht dazu führen, dass unnötig sensible Angaben erhoben werden. Im Gespräch ist ausserdem zu berücksichtigen, dass Personen im Umfeld mithören könnten. Das Team sollte bei Bedarf kurz klären, ob die Patientin oder der Patient ungestört sprechen kann.

Die Einrichtung braucht eine Regel für den Umgang mit technischen Störungen. Zum Beispiel:

- Bei Verbindungsabbruch wird ein definierter Rückrufversuch unternommen.
- Falls der sichere Kanal nicht verfügbar ist, wird auf einen freigegebenen Ausweichweg gewechselt.
- Medizinisch relevante Anliegen werden nicht einfach als „Technikproblem“ geschlossen.
- Der weitere Kontakt und allfällige Einschränkungen werden dokumentiert.

Verwenden Sie für Terminlinks und Unterlagen nur freigegebene Systeme. Links sollten nicht offen zugänglich oder unnötig lange gültig sein. Ebenso braucht es eine klare Regel, ob eine Sitzung aufgezeichnet werden darf. Eine Aufzeichnung sollte nicht beiläufig oder aus Bequemlichkeit erfolgen; Zweck, Erforderlichkeit, Information und rechtliche Grundlage müssen vorab geklärt sein.

Dokumentation: medizinisch sinnvoll und nachvollziehbar

Die Dokumentation macht den telemedizinischen Kontakt für die weitere Versorgung anschlussfähig. Sie sollte nicht ausufernd sein, aber die relevanten Entscheidungen und Vereinbarungen abbilden. Dazu gehören – angepasst an den konkreten Fall – Datum und Art des Kontakts, beteiligte Personen, Anlass, wesentliche Einschätzung, vereinbarte Massnahmen und nächster Schritt.

Auch Besonderheiten gehören in den Prozess: Wurde ein Termin abgebrochen? Konnte eine Identität nicht ausreichend geklärt werden? Wurde wegen technischer Einschränkungen auf einen Präsenztermin verwiesen? Solche Informationen sind relevant, wenn sie die Versorgung oder die Nachvollziehbarkeit beeinflussen.

Vermeiden Sie jedoch, dieselben Inhalte in mehreren unverbundenen Systemen zu erfassen. Legen Sie fest, welches System die führende Dokumentation enthält und wie Informationen aus Terminbuchung, Kommunikation und Patientenakte zusammengeführt werden. Der Zugriff auf Notizen und Anhänge muss denselben Datenschutzgrundsätzen folgen wie der Zugriff auf die übrige Akte.

Datenschutz fest in die Prozessgestaltung einbauen

Datenschutz funktioniert am besten, wenn er Teil der Ablaufplanung ist – nicht eine Prüfung ganz am Ende. Bei der Einführung eines neuen Kanals oder einer Telemedizinlösung sollten medizinische Leitung, Administration, IT und Datenschutz gemeinsam prüfen, welche Daten fliessen, wer sie benötigt und welche Ausfallwege bestehen. Für bestimmte Verarbeitungsvorgänge kann zusätzlich eine Datenschutz-Folgenabschätzung erforderlich sein; das ist anhand des konkreten Risikos und der anwendbaren Vorgaben zu beurteilen.

Bei der Auswahl eines Anbieters gehören unter anderem Speicherorte, Unterauftragsverarbeiter, Sicherheitsmassnahmen, Löschfristen, Supportzugriffe und vertragliche Regelungen auf den Prüfstand. Die Prüfung sollte in der internen Freigabe dokumentiert sein. Ein bekanntes Produkt oder eine verschlüsselte Verbindung allein beantworten nicht alle Fragen rund um Datenschutz und Betrieb.

Für Prozessverantwortliche, die Abläufe in Ordinationen oder Ambulanzen harmonisieren, kann telemedizin kosten und preise es hilfreich sein, den gesamten Patientenweg als übersichtliche Prozesskarte darzustellen: Eingangskanal, Zuständigkeit, Datenübergabe, Entscheidung und Rückmeldung. Der Prozess Manager begleitet Organisationen bei der Strukturierung solcher Abläufe; wichtig ist dabei, Datenschutzanforderungen direkt in die Prozessschritte und Arbeitsunterlagen einzubauen.

Kurze Checkliste für die Umsetzung

- Ist für jeden Zugangskanal festgelegt, wer Anfragen prüft und bearbeitet?
- Gibt es Triagekriterien und einen sichtbaren Hinweis für Notfälle?
- Ist geregelt, wann Telemedizin geeignet ist und wann ein persönlicher Termin nötig wird?
- Erhalten Patientinnen und Patienten rechtzeitig verständliche Informationen?
- Ist die Einwilligung des Patienten dort dokumentiert, wo sie für den konkreten Zweck erforderlich ist?
- Sind Zugriffsrechte rollenbasiert, persönlich zugeordnet und regelmässig überprüft?
- Werden technische Abbrüche, alternative Kontaktwege und medizinische Folgeschritte geregelt?
- Ist klar, wo die verbindliche Dokumentation liegt und wer sie einsehen darf?
- Sind Anbieter, Datenflüsse, Aufbewahrung und Löschung geprüft?
- Wissen Mitarbeitende, wie sie Datenschutzvorfälle melden und an wen sie sich wenden?

Fazit: Sicherheit entsteht durch klare Übergaben

Ein sicherer Telemedizinprozess besteht aus vielen gut abgestimmten kleinen Schritten: passende Zugangskanäle, nachvollziehbare Triage, klare Zuständigkeiten, verständliche Information, angemessene Einwilligung, begrenzte Zugriffsrechte und eine vollständige, aber zweckmässige Dokumentation. Datenschutz ist dabei kein Zusatzmodul, sondern Teil der Versorgungskette.

Wenn jede Übergabe geregelt ist – von der ersten Anfrage bis zur Nachbetreuung –, werden Abläufe für Patientinnen und Patienten verständlicher und für Teams verlässlicher. Genau dort wird aus einem digitalen Termin ein tragfähiger telemedizinischer Prozess.