

5.1 Speichersysteme und Backup

Daten managen – 5 Datenaufbewahrung

Unsere Versorgungsforscherin, arbeitet nun schon seit drei Jahren an einem Projekt zur Langzeitversorgung von Herzpatienten. Die Daten sind umfangreich – Interviews, Messwerte, und komplexe statistische Modelle. Eines Montagmorgens will sie eine alte Datei bereinigen und klickt versehentlich auf *Löschen...* und bestätigt ohne zu überlegen. Wenige Stunden später überschreiben ihre Hiwi-Mitarbeiter beim Import neuer Datensätze irrtümlich die Originaldateien. Eine Woche darauf meldet sich die IT: Die externe Festplatte mit Backup ist defekt, unlesbar. Noch schlimmer: der USB-Stick mit sensiblen Rohdaten ging auf dem Heimweg verloren, vermutlich ist er im Zug liegen geblieben. Im Juni trifft ein schweres Unwetter ihre Stadt. Das Archiv im Keller steht binnen Minuten unter Wasser; ein Jahr an Papierakten ist zerstört. Im September verursacht ein kleiner Brand im Serverraum Rauchschäden, die mehrere Laufwerke unbrauchbar machen. Während unsere Forscherin versucht, sich von diesen Rückschlägen zu erholen, infiziert ein Trojaner ihren Laptop während einer Konferenz. Die Hacker verschlüsseln einige Dateien und fordern Lösegeld, um sie wiederherzustellen. Gleichzeitig bemerkte die IT winzige Bitverluste in den ältesten Datenspeichern, da die maximal mögliche Lebensdauer überschritten ist. Als Ersatzhardware eintrifft, stellt sich heraus, dass neue Software-Versionen inkompatibel mit älteren Dateiformaten ist. Mehrere Archivdateien lassen sich nicht mehr öffnen. Schließlich verliert sie noch das Passwort zu einer verschlüsselten Cloud, weil ein Notizzettel in einem Stapel Altpapier landete. Am Ende sitzt sie vor dem Bildschirm, starrt auf die wenigen geretteten Fragmente und fragt sich: Hätte sich das alles vermeiden lassen?

Dieses Szenario in Gänze ist natürlich sehr unwahrscheinlich, aber solche kleinen Datenpannen passieren im Alltag immer wieder: Mal zu schnell irgendwo angeklickt oder nicht genau ausgepasst und stundenlange Arbeit ist verloren. Mit kleinen Maßnahmen, lassen sich aber die schlimmsten Folgen verhindern. Wichtig ist es erstmal verschiedene Möglichkeiten zu kennen, Daten und Dateien abzuspeichern, um entscheiden zu können, welche Variante(n) für die eigenen Zwecke am besten geeignet sind.

Datenspeicherung

Eine Variante, Daten abulegen, die hier etwas gesondert betrachtet, ist es Daten in physischen Akten festzuhalten. Das erscheint auf den ersten Blick sehr übersichtlich und simpel, aber bringt auch einige Nachteile im Vergleich mit digitaler Speicherung mit sich: Einerseits gibt es die Platzproblematik, denn irgendwo müssen die ganzen Dokumente gelagert werden. Papierakten sind selbst bei sorgfältiger Archivierung schwierig zu durchsuchen, denn anders als bei digitalen Dokumenten gibt es keine Möglichkeit der Stichwortsuche. Papierakten sind (meistens) nur einmal vorhanden, was es unmöglich macht sie mit mehreren Personen gleichzeitig zu verwenden. Die physischen Daten sind schwierig weiterzubearbeiten, beispielsweise können Dokumente nicht mal eben ergänzt oder verbessert werden. In manchen Fällen kann sich eine (zusätzliche) physische Speicherung natürlich anbieten, aber meistens ist es sinnvoll physischen Daten zu analogisieren.

Im Folgenden sind die Vor- und Nachteile von verschiedenen digitalen Speichermöglichkeiten ausgeführt:

	(eigener) PC	Mobile Speichermedien (CD, DVD, USB-Sticks, Externe Festplatten)	Server der Institution	Cloud-Dienste
+	- Schnelle und (relativ) zuverlässige Speichermöglichkeit - Keine Zusatzkosten - Verantwortung und Sicherheit liegt bei einem selbst - Maximale Kontrolle	- Leichter Transport - Aufbewahrung an einem sicheren Ort möglich (z.B. Safe) - Geringe Kosten	- Backup der Daten ist geregelt - Professionelle Durchführung und Wartung - Datenschutzrichtlinien der Institution werden berücksichtigt - Kooperatives Arbeiten ist möglich	- Einfache Nutzung und Verwaltung - Backup der Daten ist gegeben - Besonders für mobiles Arbeiten leicht nutzbar - Simultane Bearbeitung möglich - Professionelle Durchführung und Wartung
-	- PC und Backup sind miteinander verbunden und bei Verlust ist eine Datenrettung nicht möglich - Einzellösungen sind insbesondere bei kooperativen Arbeiten schwierig - eigenes IT-Wissen für eine gute Speicherung wird gefordert	- Verlust oder Diebstahl möglich - Inhalte müssen separat verschlüsselt werden - externe Festplatten sind stoß- und verschleißanfällig - Optische (CD/DVD) oder magnetische Speicherformate (Festplatten) sind sehr anfällig für Schäden - Teilweise kurze Lebensdauer der Speichermedien (2-10 Jahre bei Festplatten, CD und DVD 5-10 Jahre, USB-Sticks/SD Karten 10-30 Jahre (bei Nutzung)) - Kein gleichzeitiges Arbeiten an Dateien möglich	- Geschwindigkeit eventuell zu niedrig - Backup Zugang verzögert sich möglicherweise - Sicherheitsrisiken und -strategien nicht immer transparent einsehbar - Arbeit mit Externen schwierig/nicht möglich	- Datenschutz? - Sicherheit der Verbindung schwankt von Anbieter zu Anbieter - Abhängigkeit von Internetverbindung - Gefahren von Datenverlust bei Einstellung des Angebots oder Löschung des Kontos - Größeres Risiko von Hacking - Backup ggf. verzögert

Kostenlose Clouddienste (bspw. Google Drive, Dropbox, OneDrive) sollten bei der Speicherung von (sensiblen) Daten nicht verwendet werden, da deren Serverstandorte nicht in Deutschland, sondern in Amerika liegen. Aufgrund des USA PATRIOT Acts sind die eigenen Daten hier nicht vor einem Zugriff Dritter geschützt, da US-Behörden auch ohne richterliche Genehmigung auf Server von US-Unternehmen (und auch deren ausländische Tochterfirmen) zugreifen können (siehe für mehr Infos **4 Datenpflege und**

–schutz).

Eine mögliche Alternative bietet der nicht-kommerzielle Cloud-Speicherdienst für Forschung, Studium und Lehre [sciebo](#).

Bei der Verwaltung einer großen Anzahl an Dateien und Dokumenten (z.B. in Arztpraxen) bietet sich zusätzlich ein Dokumenten-Management-System an. Dort liegen die Dokumente, denen ein eindeutiger Schlüssel zur Identifikation zugeordnet wird mit Metadaten (z.B. Urheber, Art des Dokuments, Status,...), Informationen zur Struktur des Dokuments und Regeln zur Dokumentverwaltung (z.B. Zugangsverwaltung und Aufbewahrungsrichtlinien). Dies spart Zeit und Kosten und vereinfacht die Verwaltung. Mehr Informationen dazu [hier](#).

Backup vs. Archivierung

Beide Begriffe werden häufig synonym verwendet, allerdings unterscheiden sich die Bedeutungen stark:

Bei einem Backup wird regelmäßig eine Kopie der Daten für den Fall erstellt, dass diese beispielsweise durch Benutzerfehler oder defekte Hardware verloren gehen und wiederhergestellt werden müssen. Speichermedien reichen hier von Festplatten, über mobile Speichermedien, bis hin zu Online-Speichersystemen. Wichtig ist, dass nach einem Datenverlust über das Backup Daten schnell wiederhergestellt werden können. Ein Backup System sollte immer getestet werden um sicherzustellen, dass Daten im Extremfall immer wiederhergestellt werden können.

Bei einer Archivierung werden Daten systematisch auf langlebige Speichermedien wie z.B. optische Speichermedien und Festplatten übertragen. Dies geschieht meistens zu festgelegten Zeitpunkten, wenn Daten in ihrer vollständigen und endgültigen Version vorliegen. Die Daten werden so gespeichert, dass nachträgliche Änderungen nicht möglich sind. Von einer Langzeitarchivierung redet man bei einem Aufbewahrungszeitraum von 10 Jahren oder länger. Mehr dazu wird im Dokument zur Langzeitarchivierung thematisiert.

Verschiedene Backup Routinen

Es gibt verschiedene Möglichkeiten Backups zu erstellen: Ausgangspunkt ist immer ein vollständiges Backup, das in Kombination mit inkrementellen oder differenziellen Backups regelmäßig durchgeführt wird. Auch die optimale Häufigkeit von Backups ist von den jeweiligen Umständen abhängig. Unter anderem die Art der Dateien, Menge der Daten, Häufigkeit von Änderungen, vorhandener Speicherplatz und Größe der Unternehmung beeinflussen die individuelle optimale Backup Strategie

- **Vollständiges Backup:** Ein vollständiges Backup ist die umfangreichste Art Daten zu sichern. Hierbei werden Kopien von allen Dateien erstellt, was eine große Menge an Speicherplatz erfordert, aber eine schnelle und zuverlässige Wiederherstellung garantiert. Diese Art von Sicherung sollte nur gelegentlich durchgeführt werden.
- **Inkrementelles Backup:** Hier werden nur Daten gespeichert, die sich seit dem letzten Backup-Vorgang verändert haben, weswegen diese Speicherungen zusätzlich mit einem Zeitstempel verbunden werden sollten
- **Differenzielles Backup:** Diese Art der Sicherung funktioniert ähnlich wie ein inkrementelles Backup, aber es werden bei jeder Ausführung alle Daten gespeichert, die sich seit dem letzten **vollständigen** Backup verändert haben. Dieser letzte vollständige Backup dient als Referenzpunkt

3-2-1 Backup Regel

Die 3-2-1-Regel ist die gängigste Faustregel für die Erstellung von Backups. Sie besagt, dass von allen Datensätzen **drei** Versionen existieren sollen, die auf **zwei** unterschiedlichen Speichersystemen abgelegt werden. **Eine** Kopie sollte dezentral auf einem externen Speichermedium gespeichert sein.

Weitere Infos, wie Sicherheitskopien auf verschiedenen Betriebssystemen (Windows, macOS, iOS, Android, Linux) gemacht werden können, finden sich [hier](#).

Backups in Arztpraxen

In der (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (§ 10 Abs. 5 MBO-Ä) sind Ärzt:innen angehalten, besondere Schutzmaßnahmen für Aufzeichnungen auf elektronischen Datenträgern und Speichermedien zu treffen, um Veränderung, Vernichtung oder unrechtmäßige Verwendung zu verhindern. Eine Maßnahme ist die Anfertigung von täglichen Sicherungskopien in Form von inkrementellen Backups zur Sicherung der Patient:innendaten auf ein externes Medium. Zu verwenden sind entweder nicht-veränderbare Speichermedien oder das Versehen mit einem qualifizierten elektronischen Zeitstempel oder einer elektronischen Signatur bei Speicherung auf einem veränderbaren Medium. Die externe Speicherung von Patientendaten außerhalb der Praxis ist nur unter bestimmten Voraussetzungen unter der Beachtung der Grundsätze für Auftragsarbeiten zulässig (Art 28 ff. DSGVO).

Quellenverzeichnis

Bundesärztekammer & Kassenärztliche Bundesvereinigung (2014). Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis. Deutsches Ärzteblatt. 111(21). 963-972. Abgerufen am 30.09.2025, von <https://www.aerzteblatt.de/archiv/empfehlungen-zur-aerztlichen-schweigepflicht-datenschutz-und-datenverarbeitung-in-der-arztpraxis-1-e8a3e7d1-125e-4426-8079-68c48b3e84ed>

Canavan, M.J., McGinty, S., Reznik-Zellen, R. (2022). Module 4: Data Storage, Backup and Security. New England Collaborative Data Management Curriculum. Abgerufen am 30.09.2025, von <https://oercommons.org/courses/new-england-collaborative-data-management-curriculum>

Forschungsdaten.info. (2023). Datenspeicherung und die Lebensdauer von Datenträgern. Abgerufen am 30.09.2025, von <https://forschungsdaten.info/themen/speichern-und-rechnen/datenspeicherung-und-die-lebensdauer-von-datentraegern/>

Haselmann, S. (2025). Informationen speichern und abrufen - Teil 1: Verwalten von Daten. Abgerufen am 30.09.2025, von <https://www.twillo.de/edu-sharing/components/render/61ad8b7e-e118-41f7-9772-5303e257f4c7>

Haselmann, S. (2025). Informationen speichern und abrufen – Teil 2: Strukturieren von Daten. Abgerufen am 30.09.2025, von <https://www.twillo.de/edu-sharing/components/render/f0a7611a-9be5-4124-84ab-dba918edc2a7>

Krähwinkel, E., Langner, P., Lipp, R., & Pietsch, A. M. (2022). HeFDI Data OER: Forschungsdatenmanagement – eine Online-Einführung. Zenodo. <https://doi.org/10.5281/zenodo.6373596>

Weiterführende Info

Blümm, M., Fritsch, K., Bock, S., Hackenbuchner, J., Arning, U., & Förstner, K. U. (2024). 08_LE_Daten-Speichern. FDM@Studium.nrw Blended-Learning-Basiskurs „Forschungsdatenmanagement“ (Version 1.0). Abgerufen am 30.09.2025, von https://landesinitiativefdmnrw.github.io/FDMatStudium/thk/texte/08_LE_Daten-Speichern.html

Bundesärztekammer & Kassenärztliche Bundesvereinigung (2014). Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis. Deutsches Ärzteblatt. 111(21). 963-972. Abgerufen am 30.09.2025, von <https://www.aerzteblatt.de/archiv/empfehlungen-zur-aerztlichen-schweigepflicht-datenschutz-und-datenverarbeitung-in-der-arztpraxis-1-e8a3e7d1-125e-4426-8079-68c48b3e84ed>

Canavan, M.J., McGinty, S., Reznik-Zellen, R. (2022). Module 4: Data Storage, Backup and Security. New England Collaborative Data Management Curriculum. Abgerufen am 30.09.2025, von <https://oercommons.org/courses/new-england-collaborative-data-management-curriculum>

Gatzlaff, F. (2021). Dokumenten-Management-Systeme. Abgerufen am 30.09.2025, von <https://www.twillo.de/edu-sharing/components/render/5d980e38-d840-47de-84a5-b035f71de260>

Haselmann, S. (2025). Informationen speichern und abrufen - Teil 1: Verwalten von Daten. Abgerufen am 30.09.2025, von <https://www.twillo.de/edu-sharing/components/render/61ad8b7e-e118-41f7-9772-5303e257f4c7>

Haselmann, S. (2025). Informationen speichern und abrufen – Teil 2: Strukturieren von Daten. Abgerufen am 30.09.2025, von <https://www.twillo.de/edu-sharing/components/render/f0a7611a-9be5-4124-84ab-dba918edc2a7>

Das Material ist im Rahmen des Projekts „DIM.RUHR: Datenkompetenzzentrum für die interprofessionelle Nutzung von Gesundheitsdaten in der Metropole Ruhr“ (Förderkennzeichen: 16DKZ2008[A-F]) entstanden. Dementsprechend spiegelt das Material in Version 1.0 den Stand von 2025 wider.

„Daten managen - 5.1 Datenaufbewahrung – Speichersysteme und Backup“ von Anne Mainz und Sven Meister.

Dieses Werk und dessen Inhalt sind – sofern nicht anders angegeben – lizenziert unter CC BY 4.0. Ausgenommen aus der Lizenz sind die verwendeten Logos.

