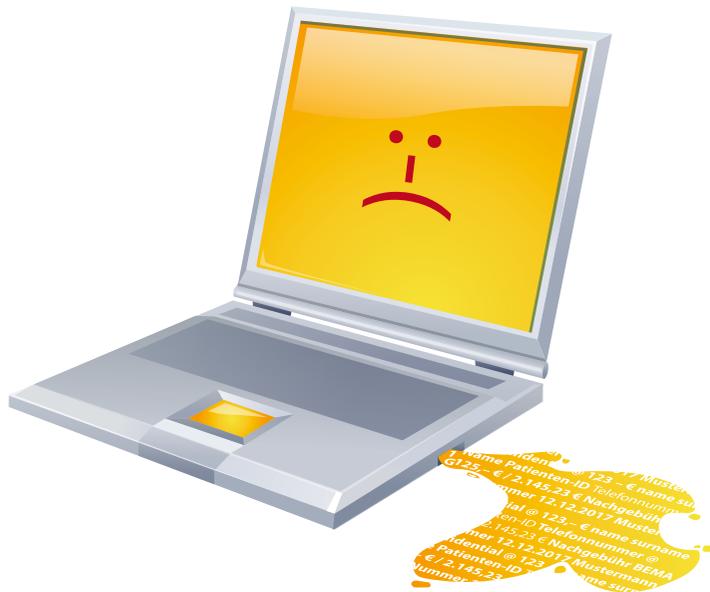


## Datenpannen vermeiden

Nina Richard, B. A.



**Ob die Entsorgung von Patientendaten im Altpapiercontainer hinter dem Haus oder der Virus auf dem PC – Datenpannen können vorkommen. Wie können Datenpannen verhindert werden und was ist zu tun wenn es zu einem Datenschutzvorfall kommt?**

Resultierend aus dem Zusammenspiel des Faktors Mensch mit den organisatorischen und technischen Kommunikationswegen kann es an jeder Schnittstelle zu Vorfällen kommen, die Patienten- oder Mitarbeiterdaten betreffen. Nicht immer fallen diese sofort auf. Erst dann, wenn beispielsweise ein externer Dritter involviert ist und meldet, dass ihm Daten einer für ihn fremden Person zugegangen sind, wird man aufmerksam. Auch wenn es sich um ein unangenehmes Ereignis handelt, sollten solche Vorfälle progressiv behandelt werden. Sonst kann ein solcher Vorfall von der Öffentlichkeit oder den Medien aufgegriffen werden – ohne Ihre Intervention besteht die Gefahr eines Reputationsschadens. Weiterhin können bei einer verschuldeten Untätigkeit Bußgelder auf Sie zukommen. Zudem sollte Ihnen bewusst sein, dass es sich um einen Verstoß gegen die ärztliche Schweigepflicht und das Persönlichkeitsrecht handelt.

### Was ist ein Datenschutzvorfall?

Jedes Ereignis, bei dem Daten von Patienten oder anderen Personen, wie z. B. Mitarbeitern, in die Hände unbefugter Dritter gelangen, ist ein Datenschutzvorfall. Hierbei spielt es keine Rolle, ob diese organisatorischer Natur sind, d. h. Einbrecher digitale Akten entwendet haben, Papierakten in der Mülltonne entsorgt wurden, Daten an den falschen Patienten übermittelt wurden oder ein Mitarbeiter seinen PC mit einem Virus infiziert hat.

Wichtig! Führen Sie eine offene Fehlerkultur ein, damit Probleme, Fehler oder Auffälligkeiten bei der computergestützten Arbeit auch tatsächlich gemeldet werden. Mitarbeiter sollten keine Angst vor Sanktionen haben, wenn sie ungewöhnliche Vorgänge und Fehler melden, sondern stattdessen von einer lösungsorientierten weiteren Vorgehensweise profitieren.

## Das richtige Vorgehen bei einem Datenschutzvorfall:

### 1. Die Situation einschätzen

Sie sollten sich einen genauen Überblick über den Sachverhalt verschaffen. Prüfen Sie, was genau passiert ist, wer involviert war und rekonstruieren Sie die Vorgänge.

### 2. Zuständigkeiten festlegen

Definieren Sie die Zuständigkeiten in Ihrer Praxis. Legen Sie einen Verantwortlichen fest, der bei einem Vorfall zu informieren ist und der sich um das weitere Vorgehen kümmert. Im optimalen Fall übernimmt diese Aufgabe Ihr Datenschutzbeauftragter.

### 3. Informieren Sie

Aus § 42 des Bundesdatenschutzgesetzes ergeben sich Informationspflichten für Ihre Praxis – zum einen die Information der Betroffenen und zum anderen die Unterrichtung der Aufsichtsbehörde. Gemäß des Gesetzes sind Sie dazu verpflichtet, diejenigen, deren Daten betroffen sind, zu informieren. Im Idealfall werden die Betroffenen einzeln per Brief darüber informiert. In Fällen, in denen eine große Menge von Patientendaten betroffen ist, kann auch die Bekanntgabe in den Medien erfolgen. Informieren Sie zudem die für Sie zuständige Aufsichtsbehörde Ihres Bundeslandes schriftlich über den Vorfall.

### 4. Bei welchen Daten muss reagiert werden?

Datenschutzvorfälle sind im Gesundheitswesen besonders kritisch, da hier mit personenbezogenen Daten der besonderen Art gearbeitet wird. Dies sind alle Daten, die Auskunft über den Gesundheitszustand, die sexuelle Orientierung, Gewerkschaftszugehörigkeit, Religion oder Ethnie geben. Gesundheitsdaten erfreuen sich auf diversen Märkten großer Beliebtheit.

### 5. Wann muss informiert werden?

Die Information von Betroffenen und der Aufsichtsbehörde hat unverzüglich zu erfolgen, nachdem entsprechende Maßnahmen zur Sicherung der Daten ergriffen wurden. Sollten Sie Ihren Informationspflichten nicht nachkommen, können je nach Schwere des Falles durch die Aufsichtsbehörden Bußgelder in Höhe von bis zu 300.000 Euro verhängt werden.



**Nina Richard, B.A.**

*Nina Richard, B.A., Leiterin Marketing und Kommunikation DATATREE AG/ ISDSG Institut für Sicherheit und Datenschutz im Gesundheitswesen. Zudem betreut Sie die Fort- und Weiterbildungsangebote, wie den zertifizierten Datenschutzbeauftragten (IOM) und die Angebote der DATATREE-Akademie.*

## Vorsicht ist besser als Nachsicht!

Die Erlangung eines 100%igen Schutzes vor Datenpannen ist nahezu unmöglich. Allerdings können Sie deren Eintrittswahrscheinlichkeit verringern, indem Sie die Mitarbeiter regelmäßig für die tägliche Arbeit mit personenbezogenen (besonderen) Daten sensibilisieren. Hierzu eignen sich regelmäßige Schulungen, die gemeinsam mit anderen Schulungsmaßnahmen beispielsweise einmal im Jahr stattfinden. Hier können datenschutzrelevante Themen im Arbeitsalltag, neue Herausforderungen zum Thema Datenschutz oder auch bereits vorgefallene Datenpannen erörtert werden. Eine Ergänzung kann das Bündeln von Informationen darstellen, zusammengestellte Informationen in Papier oder digitaler Form, die z. B. die Informationen der Schulung zusammenfassen oder einen „neuen“ Vorfall erläutern, Hilfestellungen für den Alltag bieten oder Formulare zur Verfügung stellen. Es kann sinnvoll sein, das Zusammenstellen der Informationen an einen Dienstleister, beispielsweise einen extern bestellten Datenschutzbeauftragten, abzugeben. Dieser unterliegt der Schweigepflicht, sodass keine rechtlichen Problemen in Bezug auf die Wahrung der eigenen Verschwiegenheitspflicht auftreten. Ebenso wie bei der Entwicklung Ihres persönlichen Notfallplans werden Sie und Ihre Mitarbeiter entlastet. Gemeinsam mit Ihnen verschafft sich der externe Datenschutzbeauftragte ein Bild über Arbeitsprozesse, IT-Systeme und organisatorische Gegebenheiten und kann anhand dessen, angepasst an Ihre persönlichen Bedürfnisse, aktiv werden. So können Sie sich dem Tagesgeschäft widmen.