ANALYSE

Krake kauft Krankendaten

Von Frank-Thomas Wenzel

Google schließt

SZ 13.11.19

Öffentlich krank

Die Bundesregierung will die Medizin digitalisieren. Kritiker fürchten, dass dabei zu leichtfertig mit sensiblen Daten umgegangen wird

VON KRISTIANA LUDWIG

Sanacon

Datenschutz, Datensicherheit und Compliance in der Arztpraxis

Auswertung der Umfrage 2019



SZ, S. 1. 13.11.19

Patientendaten meist schlecht geschützt

Viele Arztpraxen sichern sensible Informationen nicht ausreichend gegen Hacker-Angriffe. Das Gesundheitsministerium sieht sich nicht in der Pflicht – und verweist auf die Mediziner

VON CHRISTINA BERNDT, KATRIN

Vervielfältigung und Verbreitung der Inhalte dieser Präsentation nur mit schriftlichem Einverständnis der Sanacon. www.sanacon.de

Sehr geehrte Damen und Herren,

Ende Oktober/Anfang November 2019 baten wir niedergelassene Ärzte in Bayern um ihre Teilnahme an einer Online-Umfrage „Datenschutz, Datensicherheit und Compliance in der Arztpraxis“.

Die Ergebnisse zeigen, dass die zusätzlichen Anforderungen, die die Datenschutzgrundverordnung insbesondere für Arztpraxen brachte, noch zögerlich erfüllt werden.

In der vorliegenden Präsentation finden Sie die statistische Auswertung der Sanacon-Umfrage 2019, zusammengefasst auf 15 Seiten. Gewinnen Sie einen Eindruck, inwieweit die Themen Datenschutz, Datensicherheit und Compliance bereits in den Praxen etabliert sind und prüfen Sie, wie Ihre Praxis in den Umsetzungen aktuell positioniert ist.

Auf den letzten Seiten stellen wir Sanacon kurz vor, ausführliche Informationen über uns finden Sie auf der homepage www.sanacon.de.

Mit den besten Wünschen für 2020!

Ihr Sanacon-Team

Wichtiger Hinweis: Um den Lesefluss nicht zu beeinträchtigen wird in dieser Auswertung nur die männliche Form genannt, stets aber sind die weibliche und andere Formen gleichermaßen mitgemeint.

Was ist zu tun?

- In diesem blauen Kasten finden Sie in der Auswertung zu jedem bearbeiteten Thema allgemeine Handlungsempfehlungen bzw. Hinweise worauf jedenfalls zu achten wäre.

Grundlagen (u.a.)

- Unter „Grundlagen (u.a.)“ nennen wir Ihnen Fundstellen für Gesetzes- und Verordnungsvorgaben bzw. Fundstellen für Handlungsempfehlungen.

Editorial

Ein Gruß an die Leser und die freundliche Einladung die Ergebnisse der Sanacon-Umfrage 2019 kennenzulernen.

Seite 2

Wichtige Ergebnisse im Überblick

Für den schnellen Überblick finden Sie hier eine Übersicht, unserer Meinung nach wichtiger Ergebnisse der statistischen Auswertung.

Seite 4

Auswertungen Datenschutz und Datensicherheit

In 26 Fragen haben wir die Teilnehmer der Sanacon-Umfrage 2019 zu unterschiedlichen Aspekten des Themenbereichs „Datenschutz und Datensicherheit in der Arztpraxis“ befragt.

Seite 6 - 13

Auswertungen Compliance

Weitere 14 Fragen der Sanacon-Umfrage 2019 galten dem Themenschwerpunkt „Compliance in der Arztpraxis“. Die statistische Auswertung der Antworten finden Sie hier.

Seite 14 - 16

Methodik

Auf Seite 18 finden Sie einige Informationen zu Vorgehensweise und Hintergründen der Sanacon-Umfrage 2019.

Seite 18

Sanacon Beratung

Auf diesen Seiten lernen Sie unser Berater-Team sowie das Leistungsangebot der Sanacon Beratung kennen.

Seite 20 - 24

Elektronische Patientendaten

Nur noch 18% der Befragten arbeiten ohne **elektronische Datenerfassung und Datenverwaltung**.

Seite 6

Datenschutzbestimmungen

82% der teilnehmenden Praxen verarbeiten Patientendaten elektronisch, lediglich 62% der Befragten sind vertraut mit den Datenschutzbestimmungen für Ärzte!

Seite 6

Technische und organisatorische Maßnahmen (TOM)

Bei den TOM haben 40% bis 50% der Teilnehmer noch nichts unternommen bzw. sind sich nicht sicher, ob das Notwendige bereits erledigt wurde.

Seite 7

Verzeichnis von Verarbeitungstätigkeiten

Obwohl Pflicht für Arztpraxen, führen erst 60% der Befragten in ihrer Praxis ein Verzeichnis von Verarbeitungstätigkeiten.

Seite 8

Compliance

Der Themenkreis Compliance wird von der Mehrheit der teilnehmenden Praxen nur relativ oberflächlich beachtet.

Seite 14/16

Abrechnungen/Honorare

Rund um den Themenbereich Abrechnungen und Honorare für erbrachte Leistungen, bzw. die Qualität der dazu notwendigen Informationen, sind mindestens 85% der Befragten up to date.

Seite 15

Detaillierte Umfrageergebnisse

Vertraut mit DSGVO und BDSG?

Immerhin...

82%

Immerhin 82% der Befragten arbeiten in ihrer Praxis mit **elektronischer Datenerfassung und Datenverwaltung**.

aber nur...

62%

Aber nur 62% der Befragten sind nach eigener Einschätzung mit den aktuellen **Anforderungen des Datenschutzes** für Arztpraxen vertraut.

Was ist zu tun?

- Laufendes, konsequentes Monitoring gesetzlicher Entwicklungen.
- Einführung elektronischer Patientenverwaltung.
- Verfahrensanweisungen einführen.

Grundlagen (u.a.)

- Datenschutzgrundverordnung (DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- Div. Spezialvorschriften

DSGVO und BDSG im Praxisbetrieb umgesetzt?

Lediglich...

62%

Lediglich 62% der teilnehmenden Befragten geben an, dass die **analoge und elektronische Verarbeitung der Patientendaten** in ihrer Praxis datenschutzrechtlich geprüft wurde.

57%

In nur 57% der teilnehmenden Praxen wurden notwendige **TOM zum Datenschutz** ergriffen.

52%

Noch geringer ist die Quote der Praxen, in denen **TOM zur Sicherheit in der Daten-verarbeitung** eingeführt wurden.

Was ist zu tun?

- Laufendes, konsequentes Monitoring gesetzlicher Entwicklungen.
- Entwicklung und Einführung technischer und organisato-rischer Maßnahmen (TOM).

Grundlagen (u.a.)

- DSGVO Art. 9 Abs.2h
- BDSG § 22 Abs. 1 Nr. 1b
- DSGVO Art. 32
- BDSG § 64 Abs. 3

Verzeichnis von Verarbeitungstätigkeiten und Datenschutzfolgenabschätzung

Zu wenig...

60%

Nur 60% der Teilnehmer bestätigen, dass in ihren Praxen das bereits vorgeschriebene **„Verzeichnis von Verarbeitungstätigkeiten“** erstellt worden ist.

Noch ungeklärt...

56%

Lediglich in 56% der teilnehmenden Praxen ist geprüft worden, ob eine **Datenschutzfolgenabschätzung** durchgeführt werden muss.

Was ist zu tun?

- Notwendigkeit für eine Datenschutzfolge-abschätzung prüfen.
- Entwicklung und Einführung eines Verzeichnisses von Verarbeitungstätigkeiten.

Grundlagen (u.a.)

- DSGVO Art. 30
- DSGVO Art. 35

Rechtssicherheit im Thema Datenschutzbeauftragter?

Sehr gut!

94%

94% der Teilnehmer haben geprüft, ob für ihre Praxis ein **Datenschutzbeauftragter** benannt werden muss.

35%

35% der teilnehmenden Praxen haben Datenschutzbeauftragte installiert.

- 64% der Datenschutzbeauftragten sind interne Praxis-Mitarbeiter.
- 36% der Datenschutzbeauftragten sind externe Auftragnehmer.

Was ist zu tun?

- Laufendes, konsequentes Monitoring gesetzlicher Entwicklungen.
- Auf regelmäßige Fortbildungen des Datenschutzbeauftragten achten.
- Interne Mitarbeiter als Datenschutzbeauftragte haben das Recht auf eigene Ausstattungen.

Grundlagen (u.a.)

- DSGVO Art. 37
- BDSG § 38 Abs. 1 Satz 1

Informationspflicht zur Verarbeitung der Patientendaten

45%

informieren ihre Patienten auf **Formularen**, die sie auch unterschreiben lassen.

30%

informieren ihre Patienten zu der Verarbeitung der Patientendaten auf **Aushängen** in der Praxis.

...aber...

- 10% informieren lediglich auf ihrer **Homepage**.
- 10% informieren im **persönlichen Gespräch**.
- 5% informieren Ihre Patienten diesbezüglich **gar nicht**.

Was ist zu tun?

- Entwicklung und Einführung einer Verfahrensanweisung zur transparenten Information der Patienten über die praxisinterne Verarbeitung ihrer Daten.

Grundlagen (u.a.)

- DSGVO Art. 13 und 14

Umgang mit der ggfs. vorhandenen Pflicht zur Einholung einer Einwilligungserklärung

Der sichere Weg...

55%

holen grundsätzlich eine **Einwilligung der Patienten** zur Datenverarbeitung ein.

28%

der Befragten haben eine **Organisationsanweisung** zum fallweisen Einholen einer Einwilligung der Patienten.

17%

der Befragten gehen **eher intuitiv** vor, Einwilligungserklärungen werden mündlich oder gar nicht eingeholt.

Was ist zu tun?

- Entwicklung und Einführung einer Verfahrensanweisung zum Umgang mit der Pflicht zur Einholung einer Einwilligungserklärung von Patienten bei zustimmungspflichtigen Sachverhalten.

Grundlagen (u.a.)

- DSGVO Art. 13 und 14

Verantwortlicher Umgang mit elektronischen Daten

Handlungsbedarf!!!

47%

Lediglich 47% der Teilnehmer haben in ihrer internen Datenschutzrichtlinie ein Verfahren vorgesehen, um das **datenschutzrechtliche Auskunftsrecht** ihrer Patienten schnell bedienen zu können.

52%

der Befragten haben eine festgelegte Prozessroutine zur **Löschung von Patientendaten.**

53%

der Befragten haben eine festgelegte Prozessroutine zur **Meldung bei Datenpannen.**

Was ist zu tun?

Entwicklung und Einführung einer Verfahrensanweisung

- zum Umgang mit dem datenschutzrechtlichen Auskunftsrecht.
- zur vorgeschriebenen, turnusmäßigen Löschung von Patientendaten
- Zur Meldung von Datenpannen

Grundlagen (u.a.)

- DSGVO Art. 15, 17 und 33
- BGB § 630f Abs. 3

Datensicherheit gegenüber Dritten

Achtung Falle!!!

44%

88% der Teilnehmer erstellen täglich **Sicherungskopien** ihrer Patientendaten **auf externen Medien**. Allerdings haben lediglich 44 %, also knapp die Hälfte davon, die Voraussetzungen der Zulässigkeit dieses Vorgehens geprüft.

82%

82% halten es für gewährleistet, dass ein **Zugriff unbefugter Dritter** über ein öffentliches Datennetz ausgeschlossen ist.

76%

Bei **vertraglichen Vereinbarungen mit Externen** sichern 76% die relevanten Maßgaben des Datenschutzes incl. der Geheimhaltung.

Was ist zu tun?

Entwicklung und Einführung einer Verfahrensanweisung zur

- Einwilligung der Patienten in die Speicherung ihrer Daten auf externen Medien.
- Vermeidung des unbefugten Zugriffs Dritter.
- Beachtung des Datenschutzes bei vertraglichen Vereinbarungen.

Grundlagen (u.a.)

- Empfehlung BÄK und KBV: tägliche Datensicherung.
- DSGVO Art. 4 Nr. 8, 28 (3)f

Richtlinienkatalog und Verfahrensregeln

Auch hier besteht Handlungsbedarf!!!

35%

Erst 35% der Befragten haben für ihre Praxis einen **Richtlinien-katalog** zum Thema **„Compliance“** erstellt oder sind gerade dabei dies zu tun.

27% organisieren regelmäßige **Schulungen für die Mitarbeiter**.

45%

Nur 45% der Befragten haben in ihren Praxen für Kollegen und Mitarbeiter **verbindliche Verfahrensregeln zu Vorteilsannahmen,** wie Zuwendungen, Einladungen und Geschenken von weiter-behandelnden Krankenhäusern, Pharmareferenten, Patienten …

Was ist zu tun?

- Entwicklung und regelmä-ßige Aktualisierung eines Richtlinienkatalogs „Compliance“.
- Entwicklung Schulungs-konzept für Kollegen und Mitarbeiter.
- Festlegung verbindlicher Verfahrensregeln für die Vorteilsannahme.

Grundlagen (u.a.)

- QEP Qualitätsziel-Katalog der KV

Abrechnungen und Honorare

Sehr gut!!!

94%

94% der Befragten stellen die **nachvollziehbare Dokumentation** von Patienten und Behandlungs-daten sicher.

Der **Verlauf von Therapiemaß-nahmen** wird zuverlässig dokumentiert (90%).

94%

Um die **fachgerechte Eintragung der Leistungsziffern** entsprechend GoÄ sicherzustellen werden in den Praxen von 94% der Teilnehmer die zuständigen Mitarbeiter geschult und qualifiziert.

Die Praxisleitung überprüft die Dokumentation regelmäßig (85%).

Was ist zu tun?

- Entwicklung und Einführung einer Verfahrensanweisung zur Gewährleistung einer sachgerechten, nachvoll-ziehbaren Dokumentation von Patienten- und Behand-lungsdaten.
- Regelmäßige Schulung der Mitarbeiter

Grundlagen (u.a.)

- QEP Qualitätsziel-Katalog der KV

Die Praxis als Arbeitgeber

Verbesserungspotenzial!!!

91%

91% der Teilnehmer haben für alle Mitarbeiter in ihren Praxen **gültige Arbeitsverträge**.

Und von immerhin 87% der Mitarbeiter gibt es unterschriebene **Datenschutz- u. Verschwiegenheitserklärungen!**

39%

In lediglich 39% der teilnehmenden Praxen gibt es für die Mitarbeiter **festgeschriebene Stellenbeschreibungen.**

Noch geringer ist mit 30% die Quote der Praxen, die für die **Beendigung von Arbeitsverhältnissen** eine standardisierte Regelung haben.

Was ist zu tun?

- Sicherstellung gültiger Arbeitsverträge, Datenschutz- und Verschwiegenheitserklärungen.
- Anfertigung von Stellenbeschreibungen.
- Entwicklung und Einführung einer Verfahrensanweisung für die Beendigung von Arbeitsverhältnissen.

Grundlagen (u.a.)

- QEP Qualitätsziel-Katalog der KV

Methodik

Hintergrund und Herangehensweise

Erstellt wurde ein online zu beantwortender Fragebogen.

Umfang:
- 45 Fragen, jeweils ohne Antwortpflicht

Versand:
- per Mail an 6600 niedergelassene Ärzte in Bayern

Zeitraum der Umfrage:
- 21.10.2019 – 4.11.2019

Nachfassaktion:
- 3.11.2019

Teilnehmer an der Befragung:
- 174

Verteilung:
- 64% Einzelpraxen
- 32% Gemeinschaftspraxen
- 4% Praxisgemeinschaften

Adressen bezogen bei ArztData AG, Hamburg

Umfragetool
SurveyMonkey

Wissensstand zur Gesetzeslage:
November 2019

Datum der Veröffentlichung:

19. Januar 2020

Wir über uns – für Sie

Datenschutz/Datensicherheit

Entwicklung, Einführung und laufende Aktualisierung von **Verfahrensanweisungen** zu folgenden verpflichtenden Anforderungen:

- **Transparente Information** von Patienten über die Verarbeitung ihrer Daten sowie über die praktische Umsetzung ihres **datenschutzrechtlichen Auskunftsrechts** und des Rechts auf die vorgeschriebene, turnusmäßige **Löschung ihrer Daten**
- Pflicht zur Einholung einer **Einwilligungserklärung** von Patienten bei **zustimmungspflichtigen Sachverhalten** und der Einwilligung der Patienten in die **Speicherung ihrer Daten** auf externen Medien
- Vermeidung des unbefugten **Zugriffs Dritter** und **Meldung von Datenpannen**
- Beachtung des Datenschutzes bei **vertraglichen Vereinbarungen mit Dritten**

Weitere **Sanacon-Services**, die den Praxisablauf von aufwändigen Sonderarbeiten entlasten, die aus den Anforderungen der Datenschutzgrundverordnung resultieren, sind u.a.

- Entwicklung und Einführung **technischer und organisatorischer Maßnahmen (TOM)** zum Datenschutz und zur Sicherheit in der Datenverarbeitung
- Prüfung der Notwendigkeit einer **Datenschutzfolgeabschätzung** und den Konsequenzen hieraus
- Unterstützung bei der Überwachung des **Fortbildungsstandes** des (internen) Datenschutzbeauftragten
- Entwicklung und Einführung eines **Verzeichnisses von Verarbeitungstätigkeiten**
- Laufendes, konsequentes **Monitoring** der aktuellen Entwicklung relevanter **Gesetze und Verordnungen** und den daraus resultierenden, zusätzlichen Anforderungen

Compliance

Compliance meint die strukturierte Entwicklung von **praxisinternen Regeln**, die für Arzt und Mitarbeiter, entsprechend dem Qualitätsziel-Katalog der KV, straf- und zivilrechtliche Risiken minimieren sollen.

Im Rahmen unseres Beratungsangebots „Compliance“ bieten wir die Entwicklung und Einführung von individuell erstellten **Verfahrensanweisungen**, u.a. für die

- Gewährleistung einer sachgerechten, nachvollziehbaren **Dokumentation von Patienten- und Behandlungsdaten**
- **Gestaltung von Arbeitsverhältnissen**, z.B. bei Neueintritt von Mitarbeitern sowie bei der Beendigung von Arbeitsverhältnissen

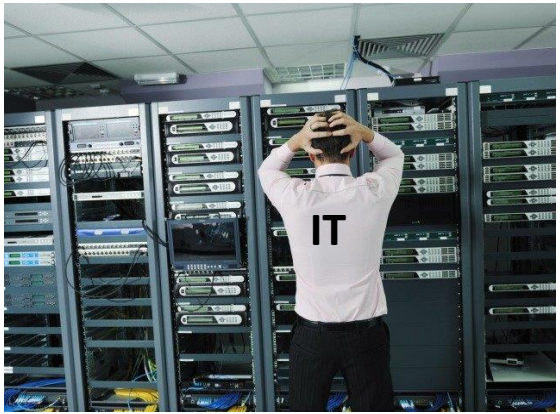
Weitere **Sanacon-Services** innerhalb des Beratungsangebots **Compliance** sind u.a.

- Entwicklung und regelmäßige Aktualisierung eines **Richtlinienkatalogs „Compliance“**
- Sicherstellung gültiger Arbeitsverträge, Datenschutz- und Verschwiegenheitserklärungen sowie Anfertigung von Stellenbeschreibungen
- Entwicklung von **Schulungskonzepten** für Kollegen und Mitarbeiter
- Festlegung verbindlicher **Verfahrensregeln für die Vorteilsannahme**
- Laufendes, konsequentes **Monitoring** der aktuellen Entwicklung relevanter **Gesetze und Verordnungen** und den daraus resultierenden, zusätzlichen Anforderungen


Prozess- und
Organisationsoptimierung


§
Compliance


Datenschutz


IT


Personal


Finanzierung und
Versicherungen

Prozess- und Organisationsoptimierung

Klar definierte Aufgaben, eine sachgerechte Rollenverteilung und geeignete technische Hilfsmittel tragen zum reibungslosen Ablauf des täglichen Geschehens bei. Wir analysieren Ihre Prozesse mit dem Ziel, Potenzial für Verbesserungen aufzuzeigen.

Compliance

Die Einhaltung der berufsrelevanten Vorschriften sollte nutzenstiftend gestaltet werden. Wo möglich, zeigen wir Wege auf, die einerseits Rechtssicherheit, andererseits einen Mehrwert für unsere Kunden mit sich bringen.

Datenschutz

Der permanent zunehmenden Bedeutung des Datenschutzes muss mit Pragmatik und Augenmaß Rechnung getragen werden. Wir erarbeiten Empfehlungen und Hinweise, die ressourcenschonend umgesetzt werden können und den Vorgaben genügen.

IT

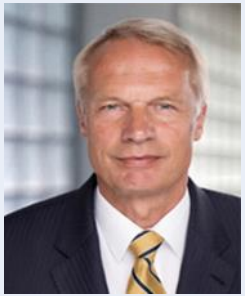
Wie sieht die "richtige" IT-Ausstattung aus? Nutzt man die im Paket enthaltenen Möglichkeiten überhaupt, bzw. was braucht man wirklich? Die Vermeidung sinnloser, weil überdimensionierter IT-Architekturen ist uns ein wesentliches Anliegen.

Personal

Qualifizierte Mitarbeiter werden zunehmend rarer. Der Arbeitsmarkt wandelt sich zum Verkäufermarkt. Die Arbeitgeber müssen sich attraktiv präsentieren. Wir unterstützen Sie dabei, ein modernes und sachgerechtes Personalmanagement zu betreiben.

Finanzierung und Versicherungen

Wann haben Sie das letzte Mal Ihre Konditionen auf Marktkonformität überprüft? Entsteht Finanzbedarf infolge größerer Investitionen? Unsere umfassende Expertise verschafft Ihnen Gewissheit, hier auf zeitgemäßem Niveau zu liegen.



Martin Hallinger
Senior Consultant

Dipl.-Kaufmann
Dipl. Betriebswirt (FH)

Compliance
Datenschutz/Datensicherheit
Prozess- u. Organisationsoptimierung
Personal



Angelika Zinner
Senior Consultant

M.A.

Compliance
Datenschutz/Datensicherheit
Personal



Norbert Zinner
Senior Consultant

Dipl.-Kaufmann

Compliance
Prozess- u. Organisationsoptimierung
Finanzierung, Versicherungen