INHALTSVERZEICHNIS

1. ZWECK

Diese Regelung soll den Schutz personenbezogener Daten von Mitarbeiten und Patienten (Patientendaten) im Klinikum sicherstellen, unabhängig von der Form ihrer Erhebung, der Art ihrer Verarbeitung und ihrer Nutzung.
Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen.
Patientendaten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse eines bestimmten oder bestimmbaren Patienten. Patientendaten sind auch die personenbezogenen Daten von Angehörigen und anderen Bezugspersonen des Patienten sowie sonstiger Dritter, die dem Krankenhaus im Zusammenhang mit der Behandlung bekannt werden. Außer den in automatisierten Dateien gespeicherten oder in Karteien oder Krankenakten aufgezeichneten Daten gehören auch die auf andere Weise festgehaltenen Informationen über den Patienten dazu (z.B. Röntgenaufnahmen, graphische Aufzeichnungen wie EKG, Blut- und Gewebeproben usw.).

2. GELTUNGSBEREICH

Dieses Konzept ist gültig für alle Mitarbeiter des Klinikums Aschaffenburg - Alzenau unabhängig von der Art oder Umfang der Beschäftigung. Es gilt insbesondere für Personen die im Rahmen ihrer dienstlichen Aufgabenstellung mit dem „Verarbeiten“ (Erheben, Speichern, Verändern, Übermitteln, Nutzen, Sperren, Löschen und Anonymisieren) von personenbezogenen Daten betraut sind.

3. ALLGEMEINE DATENSCHUTZRECHTLICHE ZUORDNUNG

Wesentliche Rechtsgrundlagen des Datenschutzes ist die Europäische Datenschutzgrundverordnung (EU-DSGVO), das Bundesdatenschutzgesetz (BDSG) und die Datenschutzgesetze der Länder (in Bayern das Bayer. Datenschutzgesetz, BayDSG). Art. 1 Abs. 3 Satz 1 BayDSG: Soweit öffentliche Stellen als Unternehmen am Wettbewerb teilnehmen, gelten für diese die Vorschriften für nicht öffentliche Stellen. Daneben gibt es bereichsspezifische Vorschriften, die den Datenschutz in einzelnen Gesetzen entweder umfassend oder in Teilbereichen regeln. Das maßgebliche Datenschutzrecht für die meisten bayerischen öffentlichen Stellen ergibt sich seit dem 25. Mai 2018 aus der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU) und dem sie ergänzenden nationalen Bundes- und Landesrecht.

Seit dem 25. Mai 2018 gilt in der gesamten EU die neue Datenschutz-Grundverordnung. Sie gilt verbindlich und unmittelbar und wird ohne weiteren Umsetzungsakt Bestandteil der in Deutschland geltenden Rechtsordnung. Gegenüber dem nationalen Recht genießt sie einen Anwendungsvorrang. Die Datenschutz-Grundverordnung enthält eine Reihe von Öffnungs- und Spezifizierungsklauseln, die den nationalen Gesetzgebern Gestaltungsspielräume eröffnen oder Regelungsaufträge erteilen.
Der Bundesgesetzgeber hat aus diesem Grund das Bundesdatenschutzgesetz (BDSG), das insbesondere für Behörden und andere öffentliche Stellen des Bundes sowie für die Verarbeitung von Daten bei nicht öffentlichen Stellen gilt, geändert.
Für die Einhaltung des Datenschutzes ist jede Behörde und jedes Unternehmen selbst verantwortlich.
Das Klinikum Aschaffenburg - Alzenau ist ein Krankenhaus, welches als öffentlich – rechtliche Dienststelle im Bundesland Bayern geführt wird. Das bayerische Krankenhausgesetz enthält in Art. 27 Regelungen zum Datenschutz die zu beachten sind.

Weitere bereichsspezifische Rechtsvorschriften, die den Datenschutz an Krankenhäusern sind z. B.:
Meldegesetze
Telekommunikationsgesetz
Infektionsschutzgesetz
Strafgesetze
Strafprozessordnung
Sozialgesetzbuch
u.s.w.

4. DIE DATENSCHUTZKONZEPTION UND DATENSCHUTZORGANISATION

4.1. NOTWENDIGKEIT EINER DATENSCHUTZGERECHTEN ORGANISATION

Die Bestimmungen des Datenschutzrechts verfolgen insbesondere das abstrakte Ziel, die Wahrung des Persönlichkeitsrechts des Einzelnen sicherzustellen. Dies kann nur dann wirksam geschehen, wenn der Datenschutz fester Bestandteil der Organisation des Klinikums Aschaffenburgs- Alzenau und damit im Bewusstsein jedes einzelnen Mitarbeiters ist.

Bei abstrakten Rechtsbegriffen wie „Schutz des Persönlichkeitsrechts“ besteht häufig die Schwierigkeit, sich den Mitarbeitern verständlich zu machen. Anders als der Begriff „Datenschutz“ zunächst nahelegt, geht es hier nicht primär darum, greifbare Dinge zu schützen, wie z. B. Datenträger mit den darauf gespeicherten Daten. Vielmehr soll vor allem Sorge getragen werden, dass Daten nicht beliebig, sondern nur bei Vorliegen gesetzlicher Zulässigkeitsvoraussetzungen erhoben, verarbeitet oder genutzt werden. Das dafür notwendige Verständnis kann nur dann entstehen, wenn die Mitarbeiterinnen und Mitarbeiter aller Hierarchiestufen des Klinikums Aschaffenburg - Alzenau über Datenschutzpflichten- und -verantwortungen aufgeklärt und in eine entsprechend ausgerichtete Organisation eingebunden werden.

Die Stabsstelle Informationssicherheit- und Datenschutz erarbeitet mit den verantwortlichen Stellen des Klinikums Grundsätze zur Datensicherheit. Maßnahmen, die notwendig sind Integrität, Authentizität, Verfügbarkeit und Vertraulichkeit personenbezogener Daten zu gewährleisten werden nach Stand der Technik ergriffen und kontinuierlich umgesetzt und ausgebaut.

4.2. VERANTWORTLICHKEITEN UND KOMPETENZEN BEIM DATENSCHUTZ

Generell richten sich alle datenschutzrechtlichen Bestimmungen an das Klinikum im Gesamten. Als rechtlicher Vertreter des Unternehmens ist die Geschäftsführung für die Umsetzung und Einhaltung der Datenschutzgesetze verantwortlich und haftet für etwaige Schäden.
Alle Führungskräfte sind für die Einhaltung der Bestimmungen des Datenschutzes in ihren Organisationseinheiten verantwortlich. Sie übernehmen die Organisationsverantwortung ihrer Abteilung und sorgen für eine angemessene Information ihrer Mitarbeiter.
Die Mitarbeiterinnen und Mitarbeiter des Klinikums Aschaffenburg – Alzenau verarbeiten personenbezogene Daten und Unternehmensdaten nur im Rahmen ihrer dienstlichen Aufgabenstellung und beachten die Datenschutzanweisungen. Über die geltenden Rechtsvorschriften und deren Umsetzung in der Praxis werden regelmäßig Schulungen für die Mitarbeiter angeboten. Alle Mitarbeiter werden bei Einstellung zur Verschwiegenheit verpflichtet

Als Betreiber kritischer Infrastruktur gemäß BSI-Kritis-Verordnung und des IT- Sicherheitsgesetzes hat das Klinikum Aschaffenburg-Alzenau Strukturen etabliert welche die Vorgaben zur Informationssicherheit und zum Datenschutz im Rahmen eines Managementsystems sicherstellen. Die Geschäftsführung hat hierzu eine Stabstelle Informationssicherheit- und Datenschutz geschaffen und einen Beauftragten (ISB/DSB) bestellt. Regelungen zu den Verantwortlichkeiten, Aufgaben und zur organisatorischen Struktur sind in der Leitlinie und Geschäftsordnung zum Informationssicherheits- und Datenschutzmanagement veröffentlicht. Für die Funktion sind Vertreter benannt.

4.3. DATENSCHUTZ UND ÄRZTLICHE SCHWEIGEPFLICHT

Die für das Klinikum Aschaffenburg - Alzenau geltenden gesetzlichen Bestimmungen zum Datenschutz, konkretisiert im

- Bayerisches Krankenhausgesetz
- Bundesdatenschutzgesetz
- Europäische Datenschutzgrundverordnung

sind weitgehender als die Bestimmungen der "Ärztlichen Schweigepflicht" nach §203 Strafgesetzbuch (StGB).

Das Datenschutzrecht regelt detailliert das

- Erheben
- Speichern
- Verändern
- Übermitteln
- Nutzen
- Sperren
- Löschen
- Anonymisieren

von personenbezogenen Daten, ungeachtet der dabei angewendeten Verfahren (maschinell, manuell). Die vorstehende Aufzählung wird im Datenschutzrecht auch zusammengefasst unter dem Begriff "verarbeiten" bezeichnet.

Die "Ärztliche Schweigepflicht" bestimmt, dass es (bei Strafe) verboten ist, ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis zu offenbaren. Die "Ärztliche Schweigepflicht" betrifft also die Bekanntgabe oder Mitteilung eines Geheimnisses. Im Datenschutzrecht wird solche Offenbarung/Bekanntgabe/Mitteilung als Übermittlung bezeichnet.
Da die Regelungen des Datenschutzrechts bedeutend weiter gefasst sind als die "Ärztliche Schweigepflicht" müssen in der praktischen und täglichen Arbeit zusätzlich die umfangreichen Bestimmungen des Datenschutzrechts beachtet werden.

4.4. ZIELE UND AUFGABEN DES DATENSCHUTZBEAUFTRAGTEN

Der Informationssicherheits- und Datenschutzbeauftragte ist eine Institution der Selbstkontrolle für den Datenschutz im Klinikum. Er ist bei der Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei und durch die Geschäftsführung bestellt. In seiner Funktion steht er der Geschäftsführung, allen Führungskräften, der Mitarbeitervertretung, sowie anlassbezogen für betroffene Einzelpersonen zur Verfügung. Dabei werden nachfolgende Ziele verfolgt
1. Schutz des Persönlichkeitsrechts der betroffenen Personen
2. Gesetzeskonforme Ausgestaltung der Verarbeitungsprozesse
Neben diesen Zielen werden die Wirksamkeit, Wirtschaftlichkeit, Praktikabilität, Angemessenheit sowie Akzeptanz der Maßnahmen berücksichtigt.

Aufgaben und Befugnisse des Informationssicherheits- und Datenschutzbeauftragten sind konkret in einer Funktionsbeschreibung und in der Geschäftsordnung für das Informationssicherheits- und Datenschutzmanagement beschrieben.

5. PRÜFUNGEN ZUM DATENSCHUTZ

Zur Einhaltung datenschutzrechtlicher Vorgaben werden Geschäftsprozesse, Systeme und Organisationsstrukturen und die damit verbundenen technischen und organisatorischen Maßnahmen überprüft. Die Prüfungsergebnisse werden strukturiert dokumentiert und an die Geschäftsführung berichtet. Auf festgestellte Risiken wird gesondert hingewiesen.

5.1. PRÜFGRUNDLAGEN

Als Prüfmaßstab werden nachfolgende Punkte herangezogen

- die Einhaltung der Rechtskonformität:
  - anzuwendende Gesetze,
  - anzuwendende Verordnungen,
  - Gerichtsurteile
- die IT-Sicherheitsgrundsätze und der Informationssicherheitsstandard, die sich am „Stand der Technik“ orientieren:
  - Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit,
  - Vorgaben aus Informationssicherheitsstandards wie die ISO/IEC 27000-Reihe und Regelungen des BSI IT-Grundschutz
- Anerkannte branchenspezifischen Vorgaben – Durch Verbände oder durch andere Vereinigungen erarbeitete Verhaltensregelungen, die der DSGVO entsprechen und von Aufsichtsbehörden anerkannt sind
- klinikinterne Regelungen:
  - Richtlinien und Anweisungen
  - Betriebs- bzw. Dienstvereinbarungen

5.2. PRÜFMETHODEN

Vor der Durchführung einer Prüf-und Kontrollaufgabe definiert der Informationssicherheits- und Datenschutzbeauftragte das zu prüfende Projekt / den Prüfgegenstand. Er bestimmt im Rahmen seiner Weisungsfreiheit die notwendigen Prüfverfahren, wie bspw.:

- rechtliche Prüfung organisatorischer Vorgaben, Dokumente und Verträge
- Begehung von Örtlichkeiten
- Befragung verantwortlicher und ausführender Personen
- Stichprobenüberprüfung von Dokumenten und Daten
- automatisierte Testverfahren
- Kontrollen zu Verfahren und Leistungen externer Dienstleister im Auftrag (z. B. Datenschutzentsorgung, digitale Archivierung etc).
- Auswertung von Aufzeichnungen wie beispielsweise Log-Dateien, Protokolle, Logbücher

Das Prüfungsergebnis wird in einem Prüfbericht dokumentiert und an den für die Verarbeitung Verantwortlichen kommuniziert. Erkannte Schwachstellen werden auf Basis der im Klinikum definierten Risikomatrix einer Risikobewertung unterzogen und im Risikokatalog Informationssicherheit- und Datenschutz dokumentiert. In Abstimmung mit dem betroffenen Fachbereich erfolgt dabei eine Maßnahmenplanung mit festgeschriebenen Bearbeitungsfristen. Für die Umsetzung der Maßnahmen sind die Abteilungsleitungen verantwortlich. Der Informationssicherheits- und Datenschutzbeauftragte hält diese nach.

5.3. SONSTIGE INTERNE/EXTERNE PRÜFUNGEN/AUDITS ZUM DATENSCHUTZ

Externe Prüfungen zum Datenschutz finden aufgrund von gesetzlichen Vorgaben (Nachweisverfahren KRITIS Verordnung, IT Sicherheitsgesetz) und im Rahmen von freiwilligen Zertifizierungsverfahren (KTQ Kooperation und Transparenz im Gesundheitswesen, Zentrumszertifizierungen) statt.
Des Weiteren, ist die Einhaltung datenschutzrechtliche Vorgaben Bestanteil interner Qualitätsaudits.

5.4. DATENSCHUTZFOLGEABSCHÄTZUNG

Die Verarbeitung von besonderen Kategorien von Daten entsprechend Art.9 DS-GVO beinhaltet i.d.R. ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen, sodass bei Verarbeitungsvorgängen eine Datenschutz-Folgenabschätzung entsprechend Art.35 DS-GVO vorzunehmen ist. Auf Basis einer Risikobewertung werden hierbei mögliche Folgen für eine geplante Verarbeitung eingeschätzt.

Die Abteilungsleitungen des Klinikums binden den Informationssicherheits- und Datenschutzbeauftragten vor Einführung und Änderung einer Verarbeitung ordnungsgemäß und frühzeitig ein. Er berät im Rahmen der Datenschutz-Folgenabschätzung den für die Verarbeitung Verantwortlichen und prüft die Einhaltung der DSGVO. Ist eine Datenschutz-Folgenabschätzung durchzuführen, wird diese maßgeblich durch den Informations- und Datenschutzbeauftragten begleitet.

6. VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

Das Klinikum Aschaffenburg-Alzenau kommt seiner Verpflichtung gemäß Artikel 30 DSGVO zur Führung eines „Verzeichnisses von Verarbeitungstätigkeiten“ nach. Das Verzeichnis dient der Transparenz über die Verarbeitung personenbezogener Daten und enthält alle geforderten Vorgaben. Es wird zentral im Risiko- und Maßnahmenmanagementsystem geführt. Die Abteilungsleitungen sind für die Korrektheit und Vollständigkeit der Einträge in Ihrem Verantwortungsbereich verantwortlich. Die Abteilungsleitungen sind verpflichtet neue Verarbeitungsverfahren an den Datenschutzbeauftragten zu melden. Der Datenschutzbeauftragte unterstützt bei der Erfassung einer Verarbeitungstätigkeit im Verzeichnis.

7. DATENTRÄGERENTSORGUNG

Zur Vernichtung bestimmte Datenträger sind sicher aufzubewahren und sicher zu vernichten.
Listen, Karteien, Register, Akten, EDV-Datenträger, Tonträger, Videoaufzeichnungen und andere Datenträger dürfen nur im Rahmen der klinikinternen Bestimmungen vernichtet werden
(s. auch Entsorgung von Unterlagen mit personenbezogenen Daten)

8. MELDUNGEM ZU DATENSCHUTZVERSTÖßEN

Gemäß Art. 33 Abs. 1 Satz 1 DSGVO werden Datenschutzverstöße an die Aufsichtsbehörde gemeldet. Hierzu ist im Klinikum Aschaffenburg-Alzenau ein Meldeverfahren etabliert und den Mitarbeitern bekannt gemacht. Dieses gewährleistet, dass innerhalb der Frist von 72 Stunden nach bekannt werden einer Datenschutzpanne eine Meldung erfolgen kann. Der Verantwortliche kann das Melden an den Datenschutzbeauftragten delegieren. Dieser analysiert und dokumentiert die Ursachen die zu einer Datenschutzverletzung geführt haben, bewertet deren Auswirkung und leitet mit Abstimmung der betroffenen Bereiche ggf. der Geschäftsführung Maßnahmen zur Verhütung von Folgeschäden ein. Sofern Risiken für die Rechte oder Freiheiten betroffener Person nicht ausgeschlossen werden können, werden diese informiert.

9. SCHULUNGEN ZUM DATENSCHUTZ

Eine wichtige Aufgabe zur nachhaltigen Sicherung eines hohen Datenschutzstandards im Klinikum ist eine regelmäßige Aufklärung und Sensibilisierung der Mitarbeiter, Führungskräfte und der Geschäftsführung hinsichtlich der geltenden Vorschriften, zu beachtenden Verfahren bzw. Sicherheitsmaßnahmen und relevanter technischer und organisatorischer Änderungen. Schulungsinhalte und Umfang sind nach Art der Verarbeitung und entsprechend der Datenschutzrisiken gestaltet. Die Durchführung erfolgt zielgruppenspezifisch und handlungsorientiert. Dazu gehören:

- regelmäßig angebotene Schulungen für das Pflegepersonal und den ärztlichen Dienst über das innerbetriebliche Fortbildungsprogramm
- bereichsspezifische Schulungen hinsichtlich der jeweiligen Erfordernisse des Datenschutzes für einzelne Abteilungen/Arbeitsplätze wie EDV, Personalabteilung, Aufnahme, Archiv, Information, Patientenverwaltung etc.
- schriftliche Regelungen zum Datenschutz die im Intranet jedem Mitarbeiter zur Verfügung gestellt werden
- Erörterung von Datenschutzfragen im Rahmen von Datenschutzbegehungen

10. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUM DATENSCHUTZ

Maßnahmenbereiche, die sich aus Art. 32 Abs. 1 DS-GVO ergeben und im Klinikum etabliert sind:
Organisationen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen der Vorschriften der Datenschutzgesetze zu gewährleisten. Das Klinikum Aschaffenburg-Alzenau kommt dieser Verpflichtung mit nachfolgenden Maßnahmen nach:

10.1. ZUTRITTSKONTROLLE:

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogenen Daten verarbeitet oder genutzt werden, zu verwehren

- Chipkarten/Transponder-Schließsystem
- Sicherheitsschlösser
- Videoüberwachung der Eingänge
- Besucher in Begleitung der Mitarbeiter
- Empfang/Pförtner
- Zonenkonzept

10.2. ZUGANGSKONTROLLE:

Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können

- Verwaltung von Benutzerberechtigungen
- Erstellung von Benutzerprofilen
- Passwortvergabe
- Passwortrichtlinie
- Authentifizierung mit Benutzername/Passwort
- Multi-Faktor Authentifizierung (z.B. MS Authenticator)
- Passwortgeschützte Bildschirmsperre
- Sperren von externen Schnittstellen (USB)
- Einsatz VPN-Remote-Zugriff
- Endpoint Protection
- Firewall
- Mobile Device Management
- Verschlüsselung von Datenträgern
- Verschlüsselung von Notebooks
- Verschlüsselung Smartphones
- BIOS Schutz (separates Passwort)
- Regelungen zum sicheren Umgang

10.3. ZUGRIFFSKONTROLLE:

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert oder entfernt werden können.

- Einsatz von Rollen- und Berechtigungskonzepten
- Verwaltung der Benutzerrechte durch Administrator
- Beschränkung der Administratorrechte
- Protokollierung von Zugriffen auf Anwendungen (Eingabe, Änderungen, Löschung)
- Einsatz Aktenshredder (Cross-Cut)
- Datenträgervernichtung gem. DIN EN 66399
- Protokollierung der Vernichtung
- Begleiteter Transport für digitale Datenträgervernichtung

10.4. WEITERGABEKONTROLLE:

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder bei der Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen sind.

- Einsatz VPN
- E-Mail Verschlüsselung
- Bereitstellung verschlüsselte Verbindungen (sftp, https)
- Beim physischen Transport sorgfältige Auswahl von Transportpersonal und –fahrzeugen
- Beim physischen Transport sichere Transportbehälter-verpackungen
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Einhaltung der Vertraulichkeit für den internen Postweg (Arbeitsanweisung)

- Protokollierung der Zugriffe und Abrufe für bestimmte Systeme
- Organisatorische Regelungen zum sicheren FAX Versand

10.5. EINGABEKONTROLLE:

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Rollen- und Berechtigungskonzepts

10.6. AUFTRAGSKONTROLLE:

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend der Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl der Auftraggeber unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Schriftliche Weisungen an den Auftragnehmer gem. Art. 28 DSGVO (auch Anpassung Altverträge)
- Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- Vertragsstrafe bei Verstößen
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Übersicht der AV Verträge im zentralen Vertragsverzeichnis
- Überprüfung des Auftragnehmers und seiner Tätigkeiten

10.7. VERFÜGBARKEITSKONTROLLE:

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Unterbrechungsfreie Stromversorgung (USV)
- Schutzsteckdosenleisten Serverraum
- Serverraumüberwachung / Klimatisierung
- Feuer- und Rauchmeldeanlagen
- RAID System Festplattenspiegelung
- Feuerlöschanlage in Serverräumen
- Redundantes Rechenzentrum
- Backup- & Recovery-Konzepte
- Kontrolle des Sicherungsvorganges
- Aufbewahrung der Sicherungsmedien außerhalb des Serverraumes
- Getrennte Partitionen für Betriebssysteme und Daten
- Notfallpläne/Ausfallkonzepte für wichtige Systeme
- Effektive Angriffserkennung
- Schulungen von Mitarbeitern hinsichtlich Datensicherheit

10.8. TRENNUNGSKONTROLLE:

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystem
- Festlegung von Datenbankrechten
- Rollen- und Berechtigungskonzepte
- Physikalische Trennung (Systeme, Datenbanken, Datenträger)

10.9. DATENSCHUTZMANAGEMENT

Verfahren für die regelmäßige Überprüfung, Bewertung und Evaluation des Datenschutzes

- Zentrale Dokumentation aller Regelungen, zum Datenschutz mit Zugriffmöglichkeit für die Mitarbeiter (Intranet)
- Unabhängige Stabstelle für Informationssicherheit und Datenschutz etabliert, Benennung des Beauftragten einschließlich dessen Vertretung
- Verpflichtung der Mitarbeiter auf das Datengeheimnis bei Einstellung
- Schulungsangebote für die Mitarbeiter
- Jährliche Risikobewertung zur Informationssicherheit und zum Datenschutz
- Externe Audits im Rahmen der Nachweisführung zum IT Sicherheitsgesetz
- Formalisiertes Vorgehen für die Bearbeitung von Auskunftsanfragen seitens Betroffener
- Umsetzung der Informationspflichten nach Art. 13 und 14 DSGVO (Patienten, Mitarbeiter, Besucher, Geschäftspartner)

10.10. INCIDENT-RESPONSE-MANAGEMENT

Maßnahmen/Vorgehen

- Prozessbeschreibung mit Regelungen zu nachfolgenden Punkten
  - Erkennung und Meldung von Sicherheitsvorfällen
  - Umgang mit Sicherheitsvorfällen
  - Einbindung Informationssicherheits- und Datenschutzbeauftragter
  - Dokumentation von Sicherheitsvorfällen und Datenpannen

11. DOKUMENTENINFORMATION

Revisionshistorie			
Datum	**Revision**	**Prüfung/Änderung/Stilllegung**	**Ausführender**
28.08.2017	RV06	Änderung TOMs	Mitarbeiter
29.01.2019	RV07	Änderung Gesetzliche Vorgaben und Umbenennung	Mitarbeiter
25.3.2021	RV08	Änderung DSFA und Incident Response	Mitarbeiter
22.3.2023	RV08	Prüfung	Mitarbeiter
02.07.2024	RV09	Änderung, zentrales Verzeichnis der Verarbeitungstätigkeiten in Intrafox	Mitarbeiter
14.04.2025	RV09	Prüfung, MFA zu TOM hinzugefügt, Rechtschreibfehler korrigiert	Mitarbeiter