283/17-1/62/SP/48-1

D O K U M E N T A T I O N S P F L I C H T E N
D A T E N S C H U T Z - G R U N D V E R O R D N U N G

des Arztes

Dr. Martina Binder

Datum: 3.4.2018

Soweit personenbezogene Bezeichnungen in diesem Schriftstück nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise.

Inhaltsverzeichnis:

I. Allgemeine Informationen

1. Name und Anschrift des Verantwortlichen:

Dr. Martina Binder
1010 Wien, Rotenturmstraße 17/18
Tel.: 01 5321011
Mail: ordination@martinabinder.at

2. Kontaktinformationen des Ansprechpartners:

Dr. Martina Binder
1010 Wien, Rotenturmstraße 17/18
Tel.: 01 5321011
Mail: ordination@martinabinder.at

3. Kontaktinformationen des Datenschutzbeauftragten:

lt. DSGVO nicht erforderlich

II. Verzeichnis von Verarbeitungstätigkeiten

Hier findet sich eine Übersicht über sämtliche Datenanwendungen samt einer Definition des Zwecks, die der Verantwortliche betreibt. Zur besseren Übersicht sind die Datenanwendungen in folgende Kategorien eingeteilt:

- Verwaltung der Ordination
- Patientenverwaltung

Sofern nichts Anderes angegeben ist, verweist das Verzeichnis von Verarbeitungstätigkeiten auf folgende Kategorien von Übermittlungsempfängern:

1 Banken
2 Rechtsvertreter
3 Wirtschaftstreuhänder, Wirtschaftsprüfer
4 Gerichte
5 Zuständige Verwaltungsbehörden
6 Inkassounternehmen
7 Fremdfinanzierer
8 Vertrags- und Geschäftspartner
9 (private) Versicherungen
10 Statistik Österreich
11 Inspektorate
12 betriebliche und außerbetriebliche Interessenvertretungen
13 Vorsorgekassen, Abfertigungskassen, Sozialversicherungen, Pensionskassen
14 Transportunternehmen
15 Lieferanten
16 Ärzte, Krankenhäuser, Ambulatorien, Labore, Physiotherapeuten, Pflegeheime
17 Apotheken, Gesundheitsdiensteanbieter, nicht-ärztliche Gesundheitsberufe

A. Verwaltung der Ordination

1. Datenanwendung: Kommunikation mit der Kammer

1.1. **Zweck** der Verarbeitung: Abwicklung von organisatorischen Fragen mit der jeweiligen Ärztekammer zum Betrieb der Ordination einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in dieser Angelegenheit.

Beinhaltet auch: Beiträge und Umlagen, die Beantragung von Fortbildungsnachweisen.

1.2. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage

1.3. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer, Mitglieder und Arbeitnehmer der Ärztekammer

1.4. Verarbeitung durch **Auftragsverarbeiter: KEINE**

1.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: nicht erforderlich

Betroffene Personengruppe: Arbeitnehmer, Mitglieder und Arbeitnehmer der Ärztekammer					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax)	12		unbegrenzt	
2	Kommunikationsdaten (insb. Korrespondenz)	12		unbegrenzt	
3	Bankverbindungsdaten	12		unbegrenzt	
4	Ausbildungs- und Gerätenachweis	12		unbegrenzt	
5	Verrechnungsdaten	12		unbegrenzt	

2. Datenanwendung: Finanzbuchhaltung, Rechnungswesen und Logistik

2.1. **Zweck** der Verarbeitung:
Verarbeitung und Übermittlung von Daten im Rahmen einer Geschäftsbeziehung (bzw. zur Abwicklung dieser) mit Patienten und Lieferanten einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Risikomanagement, Kreditoren- und Debitorenverwaltung, Budgetierung und Kostenrechnung.

2.2. **Rechtsgrundlage** der Verarbeitung: Gesetzliche Verpflichtung

2.3. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer, Patienten, Lieferanten

2.4. Verarbeitung durch **Auftragsverarbeiter: KEINE**

2.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Buchhaltungssoftware nicht vorhanden

Betroffene Personengruppe: Arbeitnehmer					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax, UID-Nr.)	1 - 10, 14		gemäß steuerrechtlicher und unternehmensrechtlicher Aufbewahrungspflichten: mindestens 7 Jahre	
2	Bankverbindungsdaten	1 - 9			
3	Daten über Buchhaltung und Controlling	5			
4	Bestell- und Vertragsdaten	14, 15			
5	Finanzierungs- und Zahlungsbedingungen	1 - 10			
6	Bonitätsinformationen	3			

7	Gegenstand der Lieferung oder Leistung	1 - 10, 14, 15			
8	Daten über Lieferung- und Leistungsbedingungen	1 – 10			

Betroffene Personengruppe: Lieferanten					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax, UID-Nr.)	1 - 10, 14		gemäß steuerrechtlicher und unternehmensrechtlicher Aufbewahrungspflichten: 7 Jahre	
2	Leistungsdaten und -nachweise	3			
3	Daten über Buchhaltung und Controlling	3, 5			
4	Bankverbindungsdaten	1 – 9			
5	Bonitätsinformationen	3			
6	Gegenstand der Lieferung oder Leistung	1 - 10, 14			
7	Daten über Lieferungs- und Leistungsbedingungen	1 - 10			
8	Finanzierungs- und Zahlungsbedingungen	1 - 10			

3. Datenanwendung: Personalverwaltung

3.1. **Zweck** der Verarbeitung: Verarbeitung und Übermittlung von Daten für Lohn,- Gehalts- und Entgeltverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten (inkl. Strahlenschutz), soweit dies aufgrund von Gesetzen oder Normen kollektiver Rechtsgestaltung oder arbeitsvertraglicher Verpflichtungen jeweils erforderlich ist einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz, Zeugnisse) in diesen Angelegenheiten.

Beinhaltet auch: Verwaltung von Urlauben, Karenzierungen, Pflegefreistellungen sowie Pensionierung

3.2. **Rechtsgrundlage** der Verarbeitung: Erfüllung eines Vertragsverhältnisses, gesetzliche Grundlage

3.3. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer

3.4. Verarbeitung durch **Auftragsverarbeiter: KEINE**

3.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**:

Betroffene Personengruppe: Arbeitnehmer (besondere Kategorien von Daten)					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten über den Arbeitnehmer inkl. Kontaktinformationen (etwa Adresse, Tel, Mail, Fax)	1 - 5, 11 - 13		unbegrenzt (nach Ausscheiden des Mitarbeiters)	
2	Sozialversicherungsdaten	2 - 5, 11 - 13		7 Jahre (nach Ausscheiden des Mitarbeiters)	
3	Bankverbindungsdaten	1 - 4, 11 - 13		6 Monate (nach Ausscheiden des Mitarbeiters)	
4	Personalverrechnungsdaten	1 - 5, 12 - 13		3 Jahre (nach Ausscheiden des Mitarbeiters)	

4. Datenanwendung: Führen von Arbeitszeitaufzeichnungen

4.1. **Zweck** der Verarbeitung: Führen von Arbeitszeitaufzeichnungen

4.2. **Rechtsgrundlage** der Verarbeitung: Erfüllung eines Vertragsverhältnisses

4.3. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer

4.4. Verarbeitung durch **Auftragsverarbeiter: KEINE**

4.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**:

Betroffene Personengruppe: Arbeitnehmer					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten über den Arbeitnehmer inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax)	3		bis 3 Jahre nach Ende des Beschäftigungsverhältnisses	
2	Zeiterfassung (Fehlzeiten, Urlaube)	3			

5. Datenanwendung: Verwaltung von Zeiten der Arbeitsunfähigkeit

5.1. **Zweck** der Verarbeitung: Verwaltung von Zeiten der Arbeitsunfähigkeit der Mitarbeiter einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

5.2. **Rechtsgrundlage** der Verarbeitung: Gesetzliche Verpflichtung, Erfüllung eines Vertragsverhältnisses

5.3. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer

5.4. Verarbeitung durch **Auftragsverarbeiter: KEINE**

5.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**:

Betroffene Personengruppe: Arbeitnehmer (besondere Kategorien von Daten)					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Mitarbeiterdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax)	2, 4, 11 - 13		Bis 3 Jahre nach Ende des Beschäftigungsverhältnisses	
2	Ärztliche Bestätigungen				

6. Datenanwendung: Bewerbungsmanagement

6.1. **Zweck** der Verarbeitung: Organisation, Verwaltung und Abwicklung sowie das Bearbeiten von Bewerbungen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

6.2. **Rechtsgrundlage** der Verarbeitung: Einwilligungserklärung, berechtigtes Interesse, Erfüllung eines Vertragsverhältnisses

6.3. Beschreibung der **Kategorien betroffener Personen**: Bewerber

6.4. Verarbeitung durch **Auftragsverarbeiter: KEINE**

6.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**:

Betroffene Personengruppe: Bewerber					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax)			12 Monate nach Abschluss des Bewerbungsverfahrens	
2	Fähigkeiten und Kenntnisse sowie Qualifikationen (Zeugnisse, Lebenslauf, Beurteilungen, Ausbildungen)			6 Monate nach Abschluss des Bewerbungsverfahrens	
3	Informationen zum beruflichen Werdegang				

7. Datenanwendung: Verwaltung von Benutzerkennzeichen sowie Zugangs- und Zutrittssystemen

7.1. **Zweck** der Verarbeitung: Systemzugriffskontrolle und Verwaltung von Benutzerkennzeichen für die Datenanwendungen des Verantwortlichen sowie die Verwaltung der Zuteilung von Hard- und Software an die Systembenutzer einschließlich automationsunterstützt erstellter und archivierter Textdokumente (z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Zuteilung von Schlüsseln und anderen für den Zutritt notwendigen Systemen.

7.2. **Rechtsgrundlage** der Verarbeitung: Erfüllung eines Vertragsverhältnisses

7.3. Beschreibung der **Kategorien betroffener Personen**: Zugangs- und Zutrittsberechtigte

7.4. Verarbeitung durch **Auftragsverarbeiter: Dr. Martina Binder**

7.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Zugriff ausschließlich mit Passwort möglich

Betroffene Personengruppe: Zugangs- und Zutrittsberechtigte					
Nr	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Beziehung des Berechtigten zum Auftraggeber			10 Jahre	
2	Benutzerkennzeichen, Passwörter				
3	Zuteilung von Schlüsseln und anderen für den Zutritt notwendigen Systemen				
4	Zugriffs- und Zutrittsrechte (Gültigkeitsdauer, Bereiche, Zeiten)				

8. Datenanwendung: Verwaltung von Vertretungen

8.1. **Zweck** der Verarbeitung: Organisation und Abwicklung von Vertretungen in der Ordination im Verhinderungsfall (auch: Urlaubsvertretung) einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

8.2. **Rechtsgrundlage** der Verarbeitung: Erfüllung eines Vertragsverhältnisses

8.3. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer, Vertretungen

8.4. Verarbeitung durch **Auftragsverarbeiter: KEINE**

8.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**:

Betroffene Personengruppe: Arbeitnehmer, Vertretungen					
Nr	**Kategorien**				
	von personenbezogenen Daten:	**an Empfängern**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax, UID-Nr., Mitgliedsnummer)	12, 16		Speicherung im Rahmen der Patientendokumentation	
2	Organisationsdaten	12, 16			

9. Datenanwendung: Aktenverwaltung / Büroautomation

9.1. **Zweck** der Verarbeitung: Formale Behandlung der vom Verantwortlichen zu besorgenden Geschäftsfälle (einschließlich der Aufbewahrung der bei dieser Tätigkeit anfallenden Dokumente).

Beinhaltet auch: Inventarverwaltung und Verwaltung von Anlagevermögen.

9.2. **Rechtsgrundlage** der Verarbeitung: Erfüllung eines Vertragsverhältnisses

9.3. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer, Interessenten, Lieferanten

9.4. Verarbeitung durch **Auftragsverarbeiter: Dr. Martina Binder**

9.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Zugriff ausschließlich mit Passwort möglich

Betroffene Personengruppe: Arbeitnehmer, Interessenten, Lieferanten					
Nr	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax) sowie Bestell- und Vertragsdaten			gemäß steuerrechtlicher und unternehmensrechtlicher Aufbewahrungspflichten: zumindest 7 Jahre	
2	Gegenstand und Referenz				
3	Unterlagen zu den Geschäftsfällen				
4	Liste des Inventars und Anlagevermögens	3			

B. Patientenverwaltung

1. Datenanwendung: Patientenakte

1.1. **Zweck** der Verarbeitung: Erfüllung der Dokumentationspflicht gemäß § 51 Ärztegesetz sowie die Erfassung sämtlicher Leistungen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Ausstellung von Bescheinigungen, Terminmanagement (Terminvereinbarung mit Patienten), die Wahrnehmung der Anzeige- und Meldepflicht gemäß § 54 Ärztegesetz, die Wahrnehmung der Anzeige- und Meldepflicht im Missbrauchsfall sowie Meldungen an div. Gesundheitsregister und im öffentlichen Meldewesen (Meldepflichten bei ansteckenden Krankheiten); die Mitwirkung bei Verfahren bei der Patientenanwaltschaft, der Schlichtungsstelle sowie dem Beschwerdemanagement bei der Standesvertretung und Versicherungen; die Erstellung medizinischer Gutachten.
Verwaltung von Transportscheinen, Zuweisungen und Überweisungen.

1.2. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage

1.3. Beschreibung der **Kategorien betroffener Personen**: Arbeitnehmer, Patienten

1.4. Verarbeitung durch **Auftragsverarbeiter: Dr. Martina Binder /MS Access basiert**

1.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Zugriff ausschließlich mit Passwort möglich verschlüsselt

Betroffene Personengruppe: Arbeitnehmer					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax)	2, 4, 5, 9, 16,17		30 Jahre	

2	Behandlungsinformationen				

Betroffene Personengruppe: Patienten (besondere Kategorien von Daten)					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel, Mail, Fax)	2, 4, 5, 9, 16,17		30 Jahre	
2	Zustand (bei Übernahme der Beratung oder Behandlung)				
3	Vorgeschichte einer Erkrankung				
4	Patienteninformationen (etwa Befunde, Diagnosen)				
5	Krankheitsverlauf				
6	Behandlungsinformationen				
7	Sozialversicherungsdaten				
8	Bankverbindungsdaten				
9	Leistungen				
10	Daten über Aufklärungsgespräch				
11	Gesetzliche Vertreter				

2. Datenanwendung: Abrechnung (sowohl Krankenkasse / Privat)

2.1. **Zweck** der Verarbeitung: Abrechnung der erbrachten Leistungen gegenüber Versicherungen (Krankenkassen oder den Patienten) einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Die Übermittlung an die Standesvertretung zur Prüfung und Evaluierung der Abrechnung.

2.2. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage, Erfüllung eines Vertragsverhältnisses

2.3. Beschreibung der **Kategorien betroffener Personen**: Patienten

2.4. Verarbeitung durch **Auftragsverarbeiter: Dr. Martina Binder/ MS Acess basiert**

2.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Zugriff ausschließlich mit Passwort möglich, verschlüsselt

Betroffene Personengruppe: Patienten					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel, Mail, Fax)	2, 9,12, 13		gemäß steuerrechtlicher und unternehmensrechtlicher Aufbewahrungspflichten: 7 Jahre	
2	Bankverbindungsdaten				
3	Abrechnungsdaten				
4	Leistungsdaten				
5	Sozialversicherungsdaten				
6	Behandlungsinformationen				
7	Patienteninformationen (etwa Befunde, Diagnosen)				

3. Datenanwendung: Befundanforderung / Befundübermittlung

3.1. **Zweck** der Verarbeitung: Anforderung von Befunden von Ärztinnen und Ärzten, Krankenanstalten, Labore, sowie anderen Gesundheitsberufen und den Betroffenen sowie die (Rück-)Übermittlung von Befunden einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Rückfragen bei Überweisungen

3.2. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage

3.3. Beschreibung der **Kategorien betroffener Personen**: Ärzte, Patienten

3.4. Verarbeitung durch **Auftragsverarbeiter: Dr. Martina Binder/ MS Access basiert**

3.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Zugriff ausschließlich mit Passwort möglich, verschlüsselt

Betroffene Personengruppe: Ärzte					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax)	16		gemäß der gesetzlichen Aufbewahrungspflicht (mindestens 10 Jahre)	

Betroffene Personengruppe: Patienten (besondere Kategorien personenbezogener Daten)

Nr	Kategorien von personenbezogenen Daten:	an Empfängern	Übermittlung an ein Drittland	Speicherdauer	Anmerkung
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel, Mail, Fax)	16		gemäß der gesetzlichen Aufbewahrungspflicht (mindestens 10 Jahre)	
2	Patienteninformationen (etwa Befunde, Diagnosen)	16			
3	Sozialversicherungsdaten	16			
4	Behandlungsinformationen	16			

4. Datenanwendung: Untersuchung von Proben

4.1. **Zweck** der Verarbeitung: Beauftragung, Organisation und Verwaltung von Probenmaterial einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

Beinhaltet auch: Verwaltung des Versands von Sekret-, Blut- oder Gewebsproben an Labore inkl. Pathologische Labore und Pathologen zur Untersuchung (samt der Abrechnung derartiger Leistungen).

4.2. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage

4.3. Beschreibung der **Kategorien betroffener Personen**: Ärzte, Patienten

4.4. Verarbeitung durch **Auftragsverarbeiter: Dr. Martina Binder/ MS Access basiert**

4.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Zugriff ausschließlich mit Passwort möglich, verschlüsselt

Betroffene Personengruppe: Ärzte					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel, Mail, Fax)	16		gemäß der gesetzlichen Aufbewahrungspflicht (mindestens 10 Jahre)	

Betroffene Personengruppe: Patienten (besondere Kategorien personenbezogener Daten)					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax)	16		gemäß der gesetzlichen Aufbewahrungspflicht (mindestens 10 Jahre)	
2	Patienteninformationen (etwa Befunde, Diagnosen)	16			
3	Proben von Patienten	16			

5. Datenanwendung: Organisation von Konsilien

5.1. **Zweck** der Verarbeitung: Organisation, Abwicklung und Abrechnung von Konsilien einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

5.2. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage

5.3. Beschreibung der **Kategorien betroffener Personen**: Patienten

5.4. Verarbeitung durch **Auftragsverarbeiter: KEINE**

5.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**:

Betroffene Personengruppe: Patienten (besondere Kategorien personenbezogener Daten)					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax)	16		gemäß der gesetzlichen Aufbewahrungspflicht (mindestens 10 Jahre)	
2	Patienteninformationen (etwa Befunde, Diagnosen)	16			
3	Bankverbindungsdaten	16			
4	Abrechnungsdaten	16			
5	Leistungsdaten	16			
6	Sozialversicherungsdaten	16			

6. Datenanwendung: Verwaltung von Rezepten

6.1. **Zweck** der Verarbeitung: Ausgabe, Verwaltung und Organisation von Rezepten und Verordnungen von Heilbehelfen.

Beinhaltet auch: Einholung von Chefarztbewilligungen

6.2. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage

6.3. Beschreibung der **Kategorien betroffener Personen**: Patienten

6.4. Verarbeitung durch **Auftragsverarbeiter: Dr. Martina Binder/ MS Access basiert**

6.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: Zugriff ausschließlich mit Passwort möglich, verschlüsselt

Betroffene Personengruppe: Patienten (besondere Kategorien personenbezogener Daten)					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax)	13, 16, 17		gemäß der gesetzlichen Aufbewahrungspflicht (mindestens 10 Jahre)	
2	Rezeptdaten	13, 16, 17			
3	Verordnungsdaten	13, 16, 17			

7. Datenanwendung: Hausapotheke

7.1. **Zweck** der Verarbeitung: Betrieb, Verwaltung, Abrechnung und Organisation einer Hausapotheke einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

7.2. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage

7.3. Beschreibung der **Kategorien betroffener Personen**: Patienten

7.4. Verarbeitung durch **Auftragsverarbeiter: KEINE**

7.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**:

Betroffene Personengruppe: Patienten (besondere Kategorien personenbezogener Daten)					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel, Mail, Fax)	9, 13, 16		gemäß der gesetzlichen Aufbewahrungspflicht (mindestens 10 Jahre)	
2	Rezeptdaten	9, 13, 16			

8. Datenanwendung: ELGA

8.1. **Zweck** der Verarbeitung: Speicherung von Gesundheitsdaten im Rahmen von ELGA als ELGA-Gesundheitsdiensteanbieter (im Sinne des § 2 Z 10 Gesundheitstelematikgesetz 2012) einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

8.2. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage

8.3. Beschreibung der **Kategorien betroffener Personen**: Patienten

8.4. Verarbeitung**: KEINE**

8.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**:

Betroffene Personengruppe: Patienten (besondere Kategorien personenbezogener Daten)					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax)	Elektronische Gesundheitsakte („ELGA“) gemäß § 2 Z 6 GTelG		10 Jahre	
2	Laborbefunde				
3	Befunde der bildgebenden Diagnostik				
4	Medikationsdaten				
5	weitere Befunde				

9. Datenanwendung: Information an eigene Patienten

9.1. **Zweck** der Verarbeitung: Übersendung von Informationen und Erinnerungen an eigene Patienten, um Vorsorge und Kontrolluntersuchungen wahrzunehmen, Impftermine einzuhalten, Befundbesprechungen etc. einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten.

9.2. **Rechtsgrundlage** der Verarbeitung: gesetzliche Grundlage, Erfüllung eines Vertragsverhältnisses

9.3. Beschreibung der **Kategorien betroffener Personen**: Patienten (besondere Kategorien personenbezogener Daten)

9.4. Verarbeitung durch **Auftragsverarbeiter: Dr. Martina Binder**

9.5. Allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen**: nur nach schriftlicher Einwilligung des Patienten

Betroffene Personengruppe: Patienten (besondere Kategorien personenbezogener Daten)					
Nr.	**Kategorien**				
	von personenbezogenen Daten:	**an Empfänger**	**Übermittlung an ein Drittland**	**Speicherdauer**	**Anmerkung**
1	Stammdaten inkl. Kontaktinformationen (etwa Adresse, Tel., Mail, Fax)			2 Jahre	
2	Patienteninformationen (etwa Befunde, Diagnosen)				
3	Impfdaten				
4	Informationen über Vorsorge und Kontrolluntersuchungen				

III. Technische und organisatorische Maßnahmen

HINWEIS: DIE HIER VORGESCHLAGENEN MASSNAHMEN SIND UNVERBINDLICH UND MÜSSEN MIT DEM ZUSTÄNDIGEN SYSTEMADMINISTRATOR ABGESTIMMT WERDEN!

Gemäß Art 32 DSGVO sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs und der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Diese Maßnahmen schließen unter anderem Folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Jeder Verantwortliche ist somit verpflichtet, geeignete technische und organisatorische Datensicherheitsmaßnahmen zu ergreifen.

Technische und organisatorische Maßnahmen sind verpflichtend von jedem Verantwortlichen umzusetzen, um den unberechtigten Zugriff durch Dritte auf personenbezogene Daten zu verhindern.

Die vorliegenden technischen und organisatorischen Maßnahmen (TOM) sind ein Beispiel für einen Mindestschutz, um die Wiederherstellbarkeit von personenbezogenen Daten zu gewährleisten. Bitte beachten Sie, dass es sich hierbei um ein Beispiel handelt und im Einzelfall weitere Maßnahmen notwendig sein können.

Die technische Umsetzung kann dabei durch beauftragte Unternehmen (etwa einen IT-Dienstleister) erfolgen.

In Entsprechung des Art 32 DSGVO trifft der Verantwortliche folgende technische und organisatorische Maßnahmen:

1. Hinsichtlich Benutzer

1.1. Technische Maßnahmen

1.1.1. Bildschirmsperre:

Der Verantwortliche stellt sicher, dass sämtliche Nutzer verpflichtet sind, beim Verlassen des Arbeitsplatzes den Computer so zu sperren, dass er durch Dritte nicht genutzt werden kann (Stichwort: Bildschirmsperre). Es sind sämtliche Geräte so einzustellen, dass eine Bildschirmsperre nach spätestens 10 Minuten Nichtbenutzung des Computers diesen automatisch sperrt, sodass dieser erst wieder nach Eingabe eines Kennworts verwendet werden kann.

1.1.2. Umgang mit Speichermedien:

Der Verantwortliche stellt sicher, dass sämtliche Computer so gesperrt sind, dass Speichermedien nur nach Eingabe eines Passworts verwendet werden können.

1.1.3. Sichere Nutzung des Internets:

Der Verantwortliche stellt sicher, dass Benutzer eine Schulung zum sicheren Umgang mit dem Internet erhalten. Die Schulung der Mitarbeiter erfolgt einmal im Jahr.

1.1.4. Technische Maßnahmen zum Sichern von Arbeitsplatzrechnern:

Der Verantwortliche stellt sicher, dass sämtliche Arbeitsplatzrechner so gesichert sind, dass Rechnermikrofone und Kameras gegen unberechtigten Zugriff gesperrt sind. Sämtliche Arbeitsplatzrechner erhalten regelmäßig Sicherheitsupdates und werden regelmäßig auf Viren untersucht. Die Grundkonfiguration der Rechner sieht vor, dass die Rechner vor unberechtigtem Zugang geschützt sind (die Nutzung des Rechners ist nur nach Eingabe eines Passworts möglich).

Folgende technische Maßnahmen werden je Arbeitsplatzrechner ergriffen:

Zugriff nur mit Passwort

1.1.5. Datensicherung der Clients:

Der Verantwortliche stellt sicher, dass sämtliche lokal auf den Arbeitsplatzrechnern gespeicherten Daten regelmäßig gesichert werden.

Die Rechner werden wie folgt gesichert:

Externe Festplatte

1.2. Organisatorische Maßnahmen

1.2.1. Mitarbeiterschulung:

Der Verantwortliche stellt sicher, dass sämtliche Mitarbeiter regelmäßig geschult werden. Im Rahmen der Schulung werden die Mitarbeiter aufgeklärt, auf welche Art und Weise personenbezogene Daten verarbeitet werden dürfen und welche Datensicherheitsmaßnahmen zu ergreifen sind. Der Verantwortliche stellt sicher, dass ein entsprechender Nachweis der Schulung im Personalakt des jeweiligen Mitarbeiters abgelegt wird.

Im Rahmen der Schulung werden die Mitarbeiter auch über die sichere Nutzung von Browsern, die sichere Nutzung von sozialen Netzwerken sowie über die Zulässigkeit der Nutzung von Kommunikationsmedien informiert.

Der Verantwortliche hat seine Mitarbeiter darüber aufgeklärt, dass die Nutzung von Onlinespeichern („Cloud-Dienste“) – ohne ausdrückliche Genehmigung des Verantwortlichen – nicht zulässig ist.

Die Mitarbeiter werden dahingehend geschult, dass diese umgehend bekannt geben müssen, sollte ein genutztes Endgerät – egal aus welchem Grund – nicht mehr nutzbar sein (Defekt, Verlust, Diebstahl).

Sofern eine private Nutzung der IT-Infrastruktur gestattet wird, stellt der Verantwortliche sicher, dass mit den Mitarbeitern eine Vereinbarung hinsichtlich der privaten Nutzung der IT-Infrastruktur mit folgendem Inhalt geschlossen wird:

„*Dem Dienstnehmer ist das Benutzen der IT-Anlage für private Zwecke bis auf Widerruf nach Maßgabe der folgenden Bestimmungen gestattet:*

1. *Der Dienstnehmer darf die IT-Systeme nur in einem solchen Maße in Anspruch nehmen, dass dadurch die betriebliche Nutzung der IT-Systeme nicht beeinträchtigt wird; dies betrifft insbesondere die Menge der abgelegten Daten.*

2. *Der Dienstnehmer ist verpflichtet, die für private Zwecke eingerichteten Ordner ständig von nicht mehr benötigten Daten zu räumen, um Speicherplatz zu sparen. Dateien, die besonders viel Speicherkapazität in Anspruch nehmen (Grafiken, Video- und Tondateien), wird er nicht speichern.*

3. *Der Dienstnehmer ist verpflichtet, spätestens am letzten Tag des Dienstverhältnisses sämtliche seiner privaten Dateien von den Speichern der Dienstgeberin zu entfernen. Sollte er für die von ihm angelegten Dateien ein Kennwort oder eine sonstige Zugangssperre verwendet und nicht alle Dateien entfernt haben, so setzt er die Dienstgeberin durch Bekanntgabe dieses Kennworts in die Lage, die Dateien selbst zu entfernen.*

4. *Nach Beendigung des Dienstverhältnisses muss die Dienstgeberin dem Dienstnehmer nicht mehr Gelegenheit geben, seine Dateien selbst zu entfernen; sie muss ihm auch keinen Zugang mehr zu seinen privaten Dateien ermöglichen.*

5. *Der Dienstnehmer nimmt zur Kenntnis, dass es möglich ist, dass seine privaten E-Mails von anderen Mitarbeitern gelesen werden, wenn er diese über das allgemeine E-Mail-System des Dienstgebers versendet und empfängt. Der Dienstnehmer darf die E-Mail-Funktion nur in einem solchen Maß in Anspruch nehmen, dass dadurch die betriebliche Nutzung der IT-Anlage sowie der Leitungen der Dienstgeberin nicht beeinträchtigt wird; dies betrifft insbesondere die Menge des Datentransfers.*

6. *Der Dienstnehmer wird genau darauf achten, keine verdächtigen Mails oder Attachments, insbesondere von ihm unbekannten Absendern, zu öffnen."*

1.2.2. Nutzung von Kommunikationsmitteln:

Der Verantwortliche klassifiziert Dokumente wie folgt:

1. Vertraulich
2. Nicht vertraulich
3. Öffentlich bekannt

Der Verantwortliche nutzt folgende Kommunikationsmedien:

1. Persönliche Übergabe
2. Versand per verschlüsselter elektronischer Kommunikation
3. Versand per eingeschriebenem Brief
4. Versand per Post
5. Versand per Fax
6. Versand per E-Mail
7. Telefonische Mitteilung
8. Versand per SMS
9. Versand per Messenger Dienst (etwa: Whatsapp)

Zur Einhaltung eines angemessenen Sicherheitsniveaus verpflichtet sich der Verantwortliche, Informationen ausschließlich wie folgt zu übermitteln bzw. zu übersenden:

Klassifizierung	**Kommunikationsmedium**
Vertraulich	Persönliche Übergabe Versand per verschlüsselter elektronischer Kommunikation Versand per Post
Nicht vertraulich	Jedes Medium
Öffentlich bekannt	Jedes Medium

Der Verantwortliche klassifiziert Informationen wie folgt:

Information	Klassifizierung
Informationen, die die Sozialversicherungsnummer enthalten	Vertraulich
Gesundheitsdaten	Vertraulich
Adressinformationen	Vertraulich
Kontaktinformationen	Vertraulich
Informationen über Patienten	Vertraulich
Befunde	Vertraulich

Die Weitergabe von Zugangsdaten und Passwörtern im Zusammenhang mittels verschlüsselter elektronischer Kommunikation erfolgt ausschließlich per Post, persönlich oder per SMS (nach vorheriger schriftlicher Einwilligungserklärung des Empfängers).

Zulässige Kommunikationsmedien

Der Arzt als datenschutzrechtlicher Verantwortlicher wird vertrauliche Informationen (etwa Gesundheitsdaten und Befunde) an Patienten mittels unverschlüsselter E-Mail nur senden, wenn der jeweilige Patient vorab in die unverschlüsselte Zusendung eingewilligt hat. Sollte keine schriftliche Einwilligung des Patienten vorliegen, hat der Arzt als datenschutzrechtlicher Verantwortliche die mündliche Einwilligung des Patienten in der Patientenakte zu dokumentieren.

Der Verantwortliche verpflichtet sich, vertrauliche Informationen (etwa Gesundheitsdaten) an zulässige Übermittlungsempfänger (etwa: Apotheken, Ärzte, Krankenhäuser, Pflegeheime, Krankenversicherungen) ausschließlich mittels verschlüsselter elektronischer Kommunikation oder mittels Fax zu senden.

1.2.3. Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung:

Der Verantwortliche stellt sicher, dass sämtliche Nutzer sich verpflichten, sich nach dem Erfüllen einer Aufgabe vom jeweiligen Arbeitsplatzrechner abzumelden.

1.2.4. Geeigneter Umgang mit Laufwerken für Wechselmedien und externe Datenträger (Handhabung, Entsorgung, Transport):

Den Mitarbeitern ist es ohne explizite Erlaubnis nicht gestattet, personenbezogene Daten, die der Verantwortliche verarbeitet, auf Datenträger zu speichern. Eine solche Speicherung wird der jeweilige Verantwortliche explizit anordnen und – für den Einzelfall – geeignete Sicherheitsmaßnahmen anordnen.

1.2.5. Clean Desk Policy:

Der Verantwortliche stellt sicher, dass jeder Mitarbeiter sich verpflichtet, Dokumente und Unterlagen vor Verlassen des Arbeitsplatzes entsprechend zu verstauen und einzuschließen, sodass ein unbefugter Dritter keinerlei Kenntnis über deren Inhalt erhalten kann. Das „Aufräumen und Abschließen“ beinhaltet sämtliche Unterlagen, Datenträger und sonstige Informationsmedien.

1.2.6. Regelungen zu Home-Office, mobiler Arbeitsplatz:

Der Verantwortliche stellt sicher, dass Mitarbeiter, welche einen mobilen Arbeitsplatz oder das Homeoffice nutzen, sich verpflichten, ausschließlich die vom Verantwortlichen bereit gestellten Systeme zu nutzen und sämtliche Zugangsdaten geheim zu halten. Das schriftliche Festhalten der Zugangsdaten ist nicht zulässig.

Der Verantwortliche stellt sicher, dass die Mitarbeiter dem Verantwortlichen umgehend mitteilen, sollten die Zugangsdaten des Mitarbeiters nicht mehr geheim sein.

1.2.7. Regelungen zu Bring your own device:

Sollte der Verantwortliche den Mitarbeitern gestatten, eigene Endgeräte (Smartphones, Tablets, Laptops) zu nutzen, wird der Verantwortliche eine entsprechende Richtlinie erlassen und den Mitarbeitern zur Kenntnis bringen.

1.2.8. Regeln zum Verlassen der Räumlichkeiten:

Der Verantwortliche stellt sicher, dass die Mitarbeiter dahingehend geschult werden, dass sämtliche Fenster und Türen bei Verlassen der Räumlichkeiten geschlossen bzw. abgeschlossen werden, sodass ein unbefugter Dritter keinen Zugang zu den Räumlichkeiten des Verantwortlichen bzw. zu personenbezogenen Daten hat.

1.2.9. Sicherung von physischen Dokumenten:

Der Verantwortliche stellt sicher, dass sämtliche Mitarbeiter dahingehend geschult werden, dass Dokumente der Kategorie „vertraulich“ in einem verschlossenen Aktenordner oder Aktenschrank verwahrt und unmittelbar nach dem Gebrauch wieder eingeschlossen werden müssen.

Der Verantwortliche hat mit den Mitarbeitern geeignete Maßnahmen zur Sicherung des Schlüssels getroffen.

1.2.10. Geheimhaltungsvereinbarung:

Der Verantwortliche stellt sicher, dass mit sämtlichen Mitarbeitern eine Geheimhaltungsvereinbarung mit folgendem Inhalt geschlossen worden ist:

„*Der Dienstnehmer ist verpflichtet, personenbezogene Daten aus Datenverarbeitungen, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anver-*

traut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (kurz: das Datengeheimnis).

Dienstnehmer dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung des Dienstgebers übermitteln.

Das Datengeheimnis besteht auch über das Ende des Dienstverhältnisses hinaus unbefristet fort."

2. Hinsichtlich IT-Infrastruktur:

2.1. Technische Maßnahmen

2.1.1. Arbeitsplatzrechner:

Der Verantwortliche stellt sicher, dass Computer vor unbefugtem Zugriff und unbefugter Nutzung geschützt sind. Darüber hinaus sind sämtliche Arbeitsplatzrechner so konfiguriert, dass sich Updates und Softwarekorrekturen, die Sicherheitslücken schließen, automatisch installieren. Bei Arbeitsplatzrechnern, auf denen besondere Kategorien von Daten gespeichert sind, sind die genutzten Speichermedien verschlüsselt.

2.1.2. Mobiltelefone:

Sofern auf mobilen Endgeräten (Mobiltelefone, Tablets oder Ähnliches) personenbezogene Daten gespeichert werden, wird der Verantwortliche Maßnahmen dahingehend ergreifen, dass der Zugriff auf die mobilen Endgeräte erst nach Eingabe eines Kennworts möglich ist. Mobile Endgeräte sind darüber hinaus so konfiguriert, dass sich der Bildschirm des mobilen Endgeräts nach spätestens 30 Sekunden sperrt, sodass das Endgerät erst nach Eingabe eines Kennworts wiederverwendet werden kann.

Darüber hinaus stellt der Verantwortliche sicher, dass der Speicher der mobilen Endgeräte verschlüsselt ist. Daten von und zu mobilen Endgeräten werden ausschließlich verschlüsselt übertragen.

Der Verantwortliche stellt sicher, dass die Daten auf Mobiltelefonen aus der Ferne („Remote") gelöscht werden können, wenn diese verloren gegangen sind.

2.1.3. Unterbrechungsfreie Stromversorgung:

Server und andere Komponenten sind mit einer unterbrechungsfreien Stromversorgung gesichert.

2.1.4. Sicherung von öffentlich zugänglichen Bereichen:

Sofern der Verantwortliche öffentlich zugängliche Netzwerke („WLAN“) betreibt, wird er diese so sichern, dass ein Zugriff auf nicht öffentlich zugängliche Systeme des Verantwortlichen nicht möglich ist.

Der Verantwortliche stellt ferner sicher, dass öffentlich zugängliche Netzwerkanschlüsse (etwa Netzwerkdosen) nicht genutzt werden können.

2.1.5. Softwaresicherheitsmaßnahmen:

Der Verantwortliche stellt sicher, dass sämtliche Endgeräte regelmäßig mit Updates versorgt werden und Softwarepakete, welche Sicherheitslücken schließen, automatisch und regelmäßig in die entsprechenden Systeme eingespielt werden. Er stellt darüber hinaus sicher, dass regelmäßig geprüft wird, ob das Einspielen ordnungsgemäß funktioniert hat.

Der Verantwortliche stellt sicher, dass der Zugriff auf Systeme nur nach Eingabe eines Passworts möglich ist, wobei Passwörter folgende Kriterien erfüllen müssen (Passwortrichtlinie):

8-stellig mit Sonderzeichen

Der Verantwortliche stellt sicher, dass Backups der Datenbestände in folgenden Abständen erstellt werden:

wöchentlich

Der Verantwortliche stellt sicher, dass Benutzer gelöscht oder gesperrt werden, sobald diese keinen Zugriff mehr auf das System benötigen (etwa: Löschen von Benutzer-Konten von ehemaligen Mitarbeitern).

Der Verantwortliche stellt sicher, dass sämtliche Systeme durch eine Firewall geschützt werden, um einen unberechtigten externen Zugriff zu verhindern. Der Verantwortliche stellt sicher, dass ein aktueller Viren- und Spamfilter installiert ist und gewartet wird.

2.1.6. Sicherung von Telekommunikationseinrichtungen:

Der Verantwortliche stellt sicher, dass sämtliche Telekommunikationseinrichtungen (etwa Telefonanlage, Fax, VPN, W-LAN, E-Mailserver, Firewalls) vor unberechtigtem Zugriff geschützt sind.

2.2. Organisatorische Maßnahmen

2.2.1. Maßnahmen bei Außerbetriebnahme eines Clients / Beendigung des Dienstverhält-

nisses:

Der Verantwortliche stellt sicher, dass sämtliche Rechner, welche nicht mehr genutzt werden sollen, ordnungsgemäß entsorgt werden und personenbezogene Daten auf den Rechnern vor unberechtigtem Zugriff geschützt werden.

2.2.2. Dokumentation der technischen Infrastruktur:

Der Verantwortliche stellt sicher, dass die gesamte technische Infrastruktur ausreichend dokumentiert ist. Dies beinhaltet auch die Dokumentation und Kennzeichnung der Verkabelung sowie relevanter baulicher Maßnahmen.

3. Bauseitig:

3.1. Organisatorische Maßnahmen:

3.1.1. Regelungen über das Aufrufen von Patienten und die Vertraulichkeit der persönlichen Kommunikation:

Der Verantwortliche stellt sicher, dass Patienten diskret aufgerufen werden. Dazu werden der Verantwortliche oder dessen Mitarbeiter lediglich den Nachnamen des Patienten aufrufen. Der Verantwortliche und dessen Mitarbeiter werden so mit dem Patienten kommunizieren, dass ein Dritter keine Kenntnis über den Inhalt der Kommunikation erhält.

3.1.2. Regelungen über den Zutritt zu Räumlichkeiten:

Der Verantwortliche stellt sicher, dass der Zutritt zu den Räumlichkeiten nur berechtigten Personen möglich ist. Mitarbeiter, welche Schlüssel oder Zutrittsberechtigungen zu den Räumlichkeiten erhalten haben, sind entsprechend geschult, dass diese den Verantwortlichen umgehend informieren müssen, sollte der Schlüssel abhandenkommen (Verlust, Diebstahl oder ähnliches).

3.1.3. Maßnahmen zum Schutz der Infrastruktur:

Der Verantwortliche stellt sicher, dass die Infrastruktur vor unberechtigtem Zutritt geschützt ist. Ferner hat der Verantwortliche Maßnahmen ergriffen, die Infrastruktur vor Zerstörung (etwa durch Feuer) zu schützen.

3.1.4. Serverraum:

Der Verantwortliche stellt sicher, dass Server vor unberechtigtem Zugriff geschützt (etwa versperrt) sind und eine Verfügbarkeit des Servers in ausreichendem Ausmaß sichergestellt ist.

3.1.5. Archiv:

Der Verantwortliche hat Maßnahmen dahingehend ergriffen, dass der Zutritt zum Archiv nur berechtigten Personen möglich ist.

4. Administrativ:

4.1. Definition von Prozessen:

Der Verantwortliche hat in Punkt V dieses Dokuments Prozesse zur Auskunft, Löschung und Richtigstellung von Daten definiert.

4.2. Behandlung von Sicherheitsvorfällen:

Der Verantwortliche hat Prozesse definiert, was im Fall eines Sicherheitsvorfalles passieren soll.

4.3. Überprüfung der Einhaltung:

Der Verantwortliche wird regelmäßig die hier beschriebenen technischen und organisatorischen Maßnahmen evaluieren und prüfen.