WEISUNG
INFORMATIONSSICHERHEIT UND DATENSCHUTZ

VOM 1. SEPTEMBER 2023

LINDENHOFGRUPPE

VORWORT

Sowohl unsere Patientinnen und Patienten als auch unsere Kundinnen und Kunden und nicht zuletzt auch Sie als Mitarbeitende dürfen darauf vertrauen, dass ihre persönlichen Informationen nur für den vorgesehenen Zweck erhoben, verarbeitet und genutzt werden und vor Missbrauch geschützt sind. Dazu reichen technische und organisatorische Sicherheitsmassnahmen nicht aus, sondern Ihr verantwortungsbewusster Umgang mit Informationen ist genauso wichtig.

Diese Weisung gibt Ihnen eine Übersicht über die in der Lindenhofgruppe geltenden Bestimmungen, damit Sie in Ihrem Arbeitsalltag sicher mit den Informations- und Kommunikationsmitteln umgehen und der Datenschutz gewährleistet ist.

INHALTSVERZEICHNIS

1. GELTUNGSBEREICH

Diese Weisung ist verbindlich für alle Mitarbeitenden, Ärztinnen und Ärzte sowie externe Beauftragte der Lindenhofgruppe.

Informations- und Kommunikationsmittel im Sinne dieser Weisung sind Hardware (Computer, Tablets, Smartphones, Datenträger usw.), Software (Applikation, Anwendungsprogramme) Netzwerke und Dienste.

Personendaten sind alle Informationen, die sich auf eine bestimmte oder auch nur bestimmbare Person beziehen. Darunter fallen alle Patientendaten, Mitarbeiterdaten, Partnerdaten (insbesondere Beleg-, Partner-, Fachärztinnen und -ärzte sowie externe Beauftragte) oder Kundendaten. Weil die Patientendaten die wichtigsten Daten in einem Spital sind, wird nachstehend von Personendaten und Patientendaten gesprochen.

2. PERSÖNLICHE VERANTWORTUNG UND INDIVIDUELLE VORSCHRIFTEN

Alle Mitarbeitenden, Ärztinnen und Ärzte sowie externe Beauftragte, die Zugang zu Informationen über Personen, Patientinnen und Patienten oder Geschäftsdaten haben, sind persönlich dafür verantwortlich, dass der Datenschutz beachtet und die Informationen sorgfältig bearbeitet werden.

Erkundigen Sie sich bei Ihren Vorgesetzten respektive Ansprechpersonen über die in Ihrem Bereich geltenden Datenschutz- und Sicherheitsbestimmungen.

In einzelnen Bereichen sind Abweichungen von dieser Weisung möglich. Diese bedürfen der vorgängigen Zustimmung durch das Informationssicherheits- und Datenschutzboard der Lindenhofgruppe.

3. BERUFLICHE SCHWEIGEPFLICHT (PATIENTENGEHEIMNIS)

Alle Mitarbeitenden, Ärztinnen und Ärzte sowie externen Beauftragten sind an die berufliche Schweigepflicht gebunden. Alle Informationen und Daten, die Sie im Rahmen Ihrer Tätigkeit für die Lindenhofgruppe über Patientinnen und Patienten erfahren, müssen geheim gehalten werden. Die berufliche Schweigepflicht gilt über das Ende Ihres Anstellungsverhältnisses respektive über Ihre Tätigkeit für die Lindenhofgruppe hinaus.

Die Befreiung von der beruflichen Schweigepflicht erfolgt durch den Patienten, durch die Patientin oder durch den kantonsärztlichen Dienst des Kantons Bern (KAD).

Die berufliche Schweigepflicht dauert über den Tod des Patienten, der Patientin hinaus.

4. GRUNDREGELN ZUM UMGANG MIT PERSONENDATEN

- Sagen Sie den Personen vorher, was wir mit ihren Daten machen und wem wir welche Informationen weitergeben.
- Verwenden Sie die erhobenen Daten nur für die Aufgabenerfüllung.
- Üben Sie sich in Datensparsamkeit und «need-to-know».
- Dokumentieren Sie in den dafür vorgesehenen Systemen und vernichten Sie rasch alle Handnotizen und Papierunterlagen, die Sie nicht mehr benötigen.
- Bearbeiten Sie keine Daten gegen den expliziten Willen der betroffenen Person (Vetorecht).
- Greifen Sie nur auf diejenigen Daten zu, die Sie für die Aufgabenerfüllung effektiv benötigen. Geben Sie keine Informationen an unberechtigte Dritte weiter.
- Prüfen Sie die Daten, ob sie richtig, aktuell und vollständig sind.
- Geben Sie sensitive Daten (besonders schützenswerte Daten: Art. 5 Bst. c revDSG) nicht für Zwecke Dritter weiter.
- Helfen Sie mit, alle Massnahmen zu treffen, damit die Personendaten bei uns sicher sind.

5. SICHERER UMGANG MIT INFORMATIONS- UND KOMMUNIKATIONSMITTELN

5. 1. GRUNDSÄTZE DER NUTZUNG

Behandeln Sie sämtliche durch die Lindenhofgruppe bereitgestellten Betriebsmittel sorgfältig und geben Sie diese nach Aufforderung oder bei Beendigung des Arbeitsverhältnisses oder des Auftrags vollständig und mängelfrei zurück.

Für alle durch die Lindenhofgruppe bereitgestellten IT-Systeme gilt zudem, dass die Umgehung von vorhandenen bzw. integrierten Sicherheitsmechanismen nicht erlaubt ist (z.B. Deaktivierung Virenschutz, eigene WLAN-Hotspots zum Internetsurfen auf unzulässigen Seiten usw.).

Die Inhalte dieser Weisung gelten auch bei Nutzung ausserhalb des Netzwerks bzw. der Räumlichkeiten der Lindenhofgruppe.

5. 2. VORSICHTSMASSNAHMEN AM ARBEITSPLATZ

Schützen Sie Computer, Tablets, Smartphones und Datenträger vor unberechtigtem Zugriff. Achten Sie darauf, dass in Bereichen mit Publikumsverkehr Monitore, Laptops, Tablets, Drucker und Faxgeräte so aufgestellt sind, dass das Risiko der Einsichtnahme durch Dritte möglichst ausgeschlossen ist.

Gewöhnen Sie sich an, beim Verlassen des Arbeitsplatzes den Desktop und das Notebook mit Passwort zu sperren und Büroräume abzuschliessen. Alle Dossiers mit Personendaten (Personaldossiers, Belegarztdossiers etc.) sowie Patientendossiers und vertrauliche / geheime Dokumente sind, wenn möglich, einzuschliessen.

Entfernen Sie Unterlagen mit Personen- oder Patientendaten sowie vertrauliche / geheime Dokumente umgehend aus Druckern oder Faxgeräten.

Achten Sie darauf, dass sich keine unbefugten Personen in Räumen aufhalten, die nicht allgemein zugänglich sind. Fordern Sie unbefugte Personen auf, den Raum sofort zu verlasen. Sofern erforderlich, informieren Sie den technische Dienst.

5. 3. GESPRÄCHE

Sprechen Sie nicht in öffentlichen Räumen (Korridor, Spitalrestaurant, Tea-Room, Tram etc.) über Patientinnen und Patienten; tauschen Sie keine vertraulichen / geheimen Informationen in der Öffentlichkeit aus.

Geben Sie keine Informationen über Personen, Patientinnen und Patienten oder vertrauliche / geheime Geschäfte an Ihnen unbekannte und unberechtigte Personen weiter.

5. 4. UMGANG MIT SOFTWARE

Änderungen an den Systemeinstellungen (Installation, Deinstallation, Änderung der Konfiguration usw.) dürfen nur von den dazu berechtigten IT-Administratoren vorgenommen werden. Es ist verboten, Sicherheitssoftware (Virenschutz, Firewall usw.) auszuschalten, zu blockieren oder sicherheitsrelevante Einstellungen an diesen zu verändern.

Es ist nicht erlaubt, eigenmächtig Software- und Hardware-Erweiterungen auf Informatikmitteln der Lindenhofgruppe zu installieren.

5. 5. UPDATES

Durch die Lindenhofgruppe bereitgestellte Notebooks oder PCs werden regelmässig mit sicherheitsrelevanten Updates versorgt. Damit diese auf den Geräten eingespielt werden können, starten Sie bitte die IT-Systeme regelmässig neu.

Mitarbeitende sowie Ärztinnen und Ärzte, die alternative Hard- oder Software betreiben (z.B. Linux, Apple), müssen eigenverantwortlich regelmässig sicherheitsrelevante Updates auf ihren Notebooks oder PCs einspielen.

5. 6. DATEN SICHER BEARBEITEN

Verwenden Sie nur ihre eigenen, persönlichen Benutzerkonten oder die Ihnen zugeteilten funktionellen IT-Konten. Sie sind für die mit Ihrer Benutzer-ID erfolgten Zugriffe verantwortlich.

Alle geschäftsbezogenen Daten müssen auf den dafür bestimmten Serverlaufwerken gespeichert werden. Die Speicherung solcher Daten auf den persönlichen Datenträgern oder Laufwerken ist verboten.

Es ist aus Sicherheitsgründen verboten, Personendaten, Patientendaten und vertrauliche / geheime Geschäftsdaten in Cloud-Diensten (DropBox, WhatsApp etc.) zu speichern oder zu verschicken.

Geschäftsdaten dürfen jederzeit von den Vorgesetzten und anderen berechtigten Mitarbeitenden eingesehen werden. Diese Zugriffsmöglichkeit müssen Sie auch bei Abwesenheit sicherstellen. Bei Aus- oder Übertritt müssen Sie alle Dokumente der vorgesetzten Stelle übergeben.

5. 7. PATIENTENINFORMATIONSSYSTEME, KLINIKINFORMATIONSSYSTEM (KISIM)

Sie dürfen nur diejenigen Daten aufrufen, welche Sie zur Aufgabenerfüllung benötigen. Alle Patientendaten sind streng vertraulich. Fremdzugriffe sind nur erlaubt, wenn Sie in den Behandlungs- und Dokumentationsprozess des Patienten, der Patientin involviert sind.

Alle Dossierzugriffe werden protokolliert und sind im Patientendossier ersichtlich.

5. 8. PASSWÖRTER UND PIN

Passwörter / PIN sind persönlich und vertraulich. Sie dürfen Passwörter / PIN nicht aufschreiben, unverschlüsselt auf Geräten abspeichern oder anderen Personen (auch nicht den Vorgesetzen, Stellvertretern usw.) bekannt geben.

Kombinieren Sie Buchstaben, Zahlen und Sonderzeichen für Ihr Passwort. Leicht erratbare Passwörter und solche, die einen Bezug zur eigenen Person aufweisen (z.B. Name, Name von Angehörigen, Geburtsdatum usw.), sind nicht erlaubt. Vermeiden Sie die Verwendung von gleichen oder ähnlichen Passwörtern / PIN für den geschäftlichen und den privaten Gebrauch.

Initialisierungspasswörter müssen sofort, andere Passwörter regelmässig gewechselt werden. Besteht der Verdacht, dass ein Passwort einem Dritten zur Kenntnis gelangt sein könnte, so müssen Sie dieses unverzüglich durch ein neues ersetzen.

Weiterführende Informationen
Infoblatt Passwortsicherheit →

5. 9. PRIVATE NUTZUNG DER INFORMATIKMITTEL

Die zur Verfügung gestellten IT-Systeme dienen der Erfüllung Ihrer geschäftlichen Aufgaben. Die Benützung der Informatikmittel für private Zwecke ist erlaubt, solange die Arbeitsleistung nicht beeinträchtigt wird und die beanspruchten Ressourcen (wie Netz-, System- und Speicherkapazität) gering sind.

Systemkomponenten und Peripheriegeräte dürfen nicht für private Zwecke vom Arbeitsplatz entfernt werden. Personendaten, Patientendaten oder Geschäftsdaten dürfen nicht privat genutzt oder in privaten Datenablagen oder auf den persönlichen, externen Laufwerken (USB-Stick, externe Harddisk) gespeichert werden.

Die private Nutzung der Informatikmittel zu kommerziellen Zwecken ist nicht erlaubt.

5. 10. EINSATZ MOBILER GERÄTE (SMARTPHONES, TABLETS)

Personendaten, Patientendaten und Geschäftsdaten auf firmeneigenen Smartphones müssen verschlüsselt abgespeichert sein (z.B. durch Container-Lösung oder durch Verschlüsselung des gesamten Geräts). Firmen-Smartphones werden, wenn möglich in das zentrale Managementsystem der Lindenhofgruppe eingebunden.

Es sind nur Smartphones mit Originalsoftware ohne Umgehung der Sicherheitsfunktionen (z.B. iPhone Jailbreak usw.) zugelassen. Durch die Integration in das zentrale Managementsystem besteht die Möglichkeit, das Smartphone im Bedarfsfall zu sperren oder vollständig zu löschen.

Es dürfen nur Apps aus vertrauenswürdigen Quellen (z.B. aus dem offiziellen App-Store) oder dem MDM-Store der Lindenhofgruppe installiert werden. Die Installation bestimmter Apps kann durch den Informationssicherheitsbeauftragten oder den Datenschutzbeauftragten aus sicherheits- oder datenschutzrelevanten Gründen untersagt werden.

Nicht benötigte Schnittstellen (z.B. WLAN, Bluetooth, GPS, NFC) sind zu deaktivieren und nur im Bedarfsfall zu aktivieren.

5. 11. EINSATZ PRIVATER GERÄTE

Es dürfen keine privaten Informatikmittel für geschäftliche Aufgaben eingesetzt oder mit dem produktiven Netzwerk der Lindenhofgruppe verbunden werden, die nicht den geltenden Standards der Lindenhofgruppe entsprechen und von der Informatik freigegeben wurden.

5. 12. FERNZUGRIFF

Der Fernzugriff auf das Netzwerk der Lindenhofgruppe wird von der Informatik den berechtigten Personen freigegeben, sofern die Voraussetzungen erfüllt und die Sicherheitsvorschriften eingehalten werden. Erfolgt der Fernzugriff aus privaten oder öffentlichen Räumen, sind folgende Vorkehrungen zu treffen, um die Offenlegung von Personendaten, Patientendaten oder vertraulichen / geheimen Geschäftsdaten gegenüber Dritten (Familienangehörige, Besucher etc.) zu vermeiden:

a. Bei jedem Verlassen des Arbeitsplatzes sowie bei jedem Unterbruch der Arbeit müssen Sie die Verbindung zum Server durch korrektes Abmelden beenden.

b. Platzieren Sie das Gerät ist so, dass keine ungewollte Einsichtnahme möglich ist.

c. Schützen Sie das Gerät mit Benutzername und Passwort und aktivieren Sie die automatische Computersperre.

Bewahren Sie die zur Verfügung gestellten IT-Systeme – insbesondere mobile IT-Systeme wie Notebooks, Tablets, Smartphones u. dgl. – sorgfältig auf. Achten Sie bei der Mitnahme von IT-Systemen darauf, dass diese nicht unbeobachtet bleiben und vor Diebstahl geschützt sind.

Weiterführende Informationen
Infoblatt Home-Office →

5. 13. SICHERER UMGANG MIT E-MAILS

5.13.1. Geschäftliche E-Mails

Verschicken Sie E-Mails mit Personen- und Patientendaten oder mit vertraulichem / geheimen Inhalt nur in verschlüsselter Form mit HIN-Mail Global[1]. Signieren Sie Ihre E-Mails, damit der Empfänger weiss, dass die E-Mail von Ihnen kommt.

Nicht erlaubt ist das automatische Weiterleiten von E-Mails und das Freigeben der persönlichen Mailbox an eine Drittperson ohne schriftliche Erlaubnis des oder der vorgesetzten Stelle. Nutzen Sie bei mehrtägigen Abwesenheiten die Funktion des Abwesenheitsassistenten.

Das Versenden von E-Mails mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt, Massen-Mails oder das Versenden von E-Mails mit der Aufforderung zum Weiterversand im Schneeballsystem ist verboten.

Es ist verboten, fremde E-Mailsysteme (beispiel@bluewin; @gmail; @yahoo etc.) für Personen- oder Patientendaten sowie vertrauliche / geheime Informationen zu verwenden.

Geschäftliche E-Mailarchive sind bei Aus- oder Übertritt der vorgesetzten Stelle zu übergeben.

5.13.2. Private Nutzung der Lindenhofgruppe E-Mail-Adresse

Private E-Mails müssen entweder gelöscht oder im persönlichen Ordner (mit «Privat» gekennzeichnet) abgelegt werden. In den nicht persönlichen Ordnern wird nicht unterschieden zwischen geschäftlichen und persönlichen Mails.

Alle von einer von der Lindenhofgruppe zur Verfügung gestellten E-Mail-Adresse ein- und ausgehenden E-Mails werden archiviert und können nicht individuell gelöscht werden. Dies gilt auch für private E-Mails.

1 Versand von E-Mails über HIN, d.h. von Vorname.Name@lindenhofgruppe.ch an Vorname.Name@lindenhofgruppe.ch oder an beispiel@hin.ch oder andere für HIN-Verschlüsselung registrierte Firmen-Adresse. Eine Überprüfung kann auf www.hin.ch vorgenommen werden.

Versand von E-Mails über HIN-Global, d.h. von Vorname.Name@lindenhofgruppe.ch an eine Nicht-HIN-E-Mailadresse (bspw. xy@bluewin.ch) mit dem Betreff (vertraulich). Betreff: Ihre Laborresultate (vertraulich).

Durch die Einrichtung von Filtern, durch Archivierung, das zeitlich begrenzte Zurückhalten oder Verändern von Nachrichten oder durch sonstige Eingriffe kann auch auf private E-Mails Eingriff genommen werden.

5.13.3. Verdächtige E-Mails, Phishing

Löschen Sie E-Mails mit unbekanntem Absender, verdächtigem Betreff oder unüblichem Inhalt; öffnen Sie keine angehängten Dateien, insbesondere solche, die ausführbare Programme enthalten. Antworten Sie nie auf verdächtige E-Mails.

Weiterführende Informationen
Infoblatt E-Mail-Sicherheit →

5. 14. SICHERE NUTZUNG DES INTERNETS

Übermitteln Sie Personen- oder Patientendaten sowie vertrauliche / geheime Geschäftsdaten nur verschlüsselt oder über eine geschützte Verbindung. Es ist verboten, externe Internetdienste (bspw. GoogleCalendar, Dropbox, ...) für Personen- und Patientendaten sowie vertrauliche / geheime Geschäftsdaten zu verwenden.

Geschäftsdaten der Lindenhofgruppe dürfen nur von den dazu durch die Geschäftsleitung ausdrücklich berechtigten Personen im Internet publiziert werden.

Der Zugriff auf Internet-Seiten mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt und die zu privaten Zwecken erfolgende Nutzung von Chatrooms, sowie Tauschbörsen ist verboten. Die Informatik kann im Auftrag der Geschäftsleitung den Zugriff auf bestimmte Online-Dienste sperren.

5. 15. UMGANG MIT SOZIALEN MEDIEN

Es ist nicht gestattet, in sozialen Medien (z.B. Facebook, Instagram) im Namen der Lindenhofgruppe aufzutreten, sofern es keinen offiziellen Auftrag dafür gibt. Imageschädigende Aussagen in Verbindung mit der Lindenhofgruppe sind untersagt und können personalrechtliche Folgen nach sich ziehen.

Geben Sie niemals Informationen über Personen, Patientinnen und Patienten oder vertrauliche/ geheime Geschäfte der Lindenhofgruppe auf sozialen Netzwerken preis. Verwenden Sie zur Registrierung nicht ihre Lindenhofgruppe E-Mail-Adresse.

Melden sich bei Ihnen Medienschaffende oder Social-Media-User wegen einer Auskunft, die die Lindenhofgruppe betrifft, antworten Sie nicht selbst, sondern verweisen Sie an die Kommunikationsstelle der Lindenhofgruppe.

Die private Nutzung sozialer Netzwerke (bspw. Facebook, XING) soll ausserhalb der Arbeitszeit erfolgen. Während der Arbeitszeit ist sie auf ein Minimum zu beschränken.

5. 16. FOTOS UND VIDEOS

Respektieren Sie die Privatsphäre unserer Patientinnen und Patienten sowie Ihrer Arbeitskolleginnen und -kollegen und machen Sie keine Fotos und Videos mit Ihren privaten Geräten.
Fotos und Videos mit Geräten der Lindenhofgruppe sind zu Überwachungs- und Dokumentationszwecken erlaubt, sofern die Einwilligungen der Betroffenen vorliegen.

5. 17. DATENLÖSCHUNG, REPARATUR UND ENTSORGUNG VON DATENTRÄGERN

Vernichten respektive löschen Sie Daten die nicht mehr gebraucht und auch nicht archiviert werden müssen.

Elektronische Datenträger (z.B. USB-Sticks, Speicherkarten, CDs, Geräte mit fest eingebauten Speichermedien) auf denen Personen-, Patientendaten oder vertrauliche / geheime Geschäftsdaten abgespeichert oder auf denen früher einmal solche Daten gespeichert worden sind, sind der Informatik zur Löschung oder Entsorgung zu übergeben. Diese entscheidet gemäss ihren Richtlinien über die weitere Verwendbarkeit oder die Entsorgung solcher Komponenten.

Nur die Informatik darf Informatikmittel in die Reparatur oder zur Entsorgung geben. Sie sorgt dafür, dass die Vertraulichkeit von Personen- und Patientendaten sowie vertraulichen / geheimen Geschäftsdaten gewährleistet bleibt.

Papierunterlagen mit Personen- oder Patientendaten sowie vertrauliche / geheime Dokumente sind entweder in den dafür bereitgestellten Containern oder in einem Aktenvernichter zu entsorgen.

Weiterführende Informationen
Infoblatt Social Engineering →
Infoblatt Schadsoftware & Computerviren →

6. MELDUNG VON SICHERHEITSRELEVANTEN EREIGNISSEN

6. 1. VERLUST UND DIEBSTAHL

Melden Sie den Verlust oder Diebstahl von Informatikmitteln der Lindenhofgruppe oder von geschäftlich benützten privaten Geräten unverzüglich dem ServiceDesk und der vorgesetzten Stelle. Besteht der Verdacht, dass Zugangs- oder Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden oder dass ein Informatikmittel mit schadenverursachender Software (Viren, Trojaner usw.) infiziert sein könnte, melden Sie dies umgehend dem ServiceDesk.

Umgehend zu melden ist auch der Verlust:
- von Schlüsseln dem Technischen Dienst;
- von Badges dem Human Resources.

6. 2. INFORMATIONSSICHERHEITSVORFÄLLE

Melden Sie alle (vermuteten) Informationssicherheitsvorfälle umgehend dem ServiceDesk. Beispiele für Informationssicherheitsvorfälle sind:

- Unerklärliches Systemverhalten (z.B. spontane Abstürze, Programme öffnen und schließen sich selbstständig, kryptische Dateinamen);
- Verdacht auf Missbrauch der eigenen Benutzerkennung (z.B. E-Mail-Versand im eigenen Namen);
- Ungewünschte Veröffentlichung von Daten im Internet;
- Verlust oder Diebstahl eines Datenträgers (z.B. USB-Stick) mit vertraulichen Daten;
- Öffnen eines verdächtigen E-Mail-Anhangs / Links;
- Weitergabe des eigenen Passworts (z.B. im Internet, per Telefon);
- usw.

6. 3. DATENSCHUTZRELEVANTE EREIGNISSE

Melden Sie alle datenschutzrelevanten Ereignisse dem Rechtsdienst der Lindenhofgruppe. Beispiele für datenschutzrelevante Ereignisse sind:

- Ungewünschte Veröffentlichung von personenbezogenen Daten im Internet;
- Versehentliches Versenden eines E-Mails an viele Empfänger (z.B. Interessenten einer Firmen-veranstaltung), in der alle Empfänger für jeden Empfänger ersichtlich sind;
- Verlust unverschlüsselter Datenträger an öffentlich zugänglichen Orten;
- Weitergabe personenbezogener Daten an unbefugte Dritte;
- usw.

7. SICHERER UMGANG MIT PATIENTENDATEN

7. 1. GRUNDREGELN ZUM UMGANG MIT PATIENTENDATEN

- Sagen Sie den Patientinnen und Patienten vorher, was wir mit ihren Daten machen und wem wir welche Informationen weitergeben.
- Verwenden Sie die für die Behandlung erhobenen Daten nur für die Behandlung.
- Erfassen Sie nur das, was für die Behandlung relevant ist.
- Dokumentieren Sie in den dafür vorgesehenen Systemen und vernichten Sie rasch alle Handnotizen und Papierunterlagen, die Sie nicht mehr benötigen.
- Bearbeiten Sie keine Daten gegen den expliziten Willen des Patienten, der Patientin (Vetorecht). Im Gegenzug dürfen Sie davon ausgehen, dass Patientinnen, Patienten damit einverstanden sind, dass ihre Daten zum Zwecke der Behandlung benutzt / bearbeitet werden.
- Informieren Sie sich nur über Patientinnen und Patienten, in deren Behandlung Sie involviert sind. Geben Sie keine Informationen an Mitarbeitende ausserhalb des Behandlungsteams weiter.
- Prüfen Sie die Daten, ob sie richtig, aktuell und vollständig sind.
- Patientendaten werden nur mit Einwilligung der betroffenen Person oder aufgrund gesetzlicher Regelung an Aussenstehende weitergegeben.
- Helfen Sie mit, alle Massnahmen zu treffen, damit die Patientendaten bei uns sicher sind.

7. 2. EINSICHTS- UND AUSKUNFTSRECHT DER PATIENTIN, DES PATIENTEN

Patientinnen und Patienten haben das Recht auf Einsicht in und Auskunft über ihre Behandlungsunterlagen. Verlangt eine Patientin, ein Patient Kopien ihrer / seiner Patientenakten, muss sie / er das Gesuch schriftlich an das Direktionssekretariat Pflege richten. Das Gesuch muss nicht begründet werden.

Im Patientendossier ist immer zu vermerken, wem was wann herausgegeben wurde.

Weiterführende Informationen
Merkblatt Herausgabe Patientendokumentation →

7. 3. BERICHTIGUNGSRECHT UND BESTREITUNGSVERMERK

Werden Patientendaten rechtswidrig bearbeitet, können Patientinnen und Patienten verlangen, dass das weitere Bearbeiten unterlassen wird oder in einer rechtmässigen Form erfolgt.

Jede betroffene Person hat das Recht, Einschätzungen der Behandelnden in den Behandlungsunterlagen mit einem Bestreitungsvermerk versehen zu lassen.

7. 4. AUSKÜNFTE AN ANGEHÖRIGE UND NAHESTEHENDE PERSONEN

Die berufliche Schweigepflicht gilt auch gegenüber den Angehörigen, den angegebenen Kontaktpersonen sowie den in einer Patientenverfügung eingesetzten Vertretungspersonen. Der urteilsfähige Patient, die urteilsfähige Patientin entscheidet, wer welche Informationen erhalten darf. Die Patientenverfügung tritt erst bei Urteilsunfähigkeit der Patientin, des Patienten in Kraft.

Verlangen Angehörige Auskünfte zur Diagnose oder detailliert Auskünfte zum Gesundheitszustand, muss vorgängig das Einverständnis der Patientin, des Patienten eingeholt werden. Dies kann auch mündlich erfolgen.

Allgemeine Auskünfte zum Spitalaufenthalt (bspw. Patient hat gut geschlafen, Patientin ist schmerzfrei, Patient ist in Therapie) dürfen Angehörigen und nahestehenden Personen gegeben werden. Verweigert die Patientin, der Patient auch diese allgemeinen Auskünfte, muss sich das Spitalpersonal daran halten.

Bei urteilsunfähigen Patientinnen und Patienten werden die Informationen gemäss ihrem mutmasslichen Willen weitergegeben. Dies bedeutet, dass Angehörige, die mit der Patientin, dem Patienten unter einem Dach leben, über den Aufenthalt informiert werden, ausser es liegen Hinweise vor (u.a. in einer Patientenverfügung), dass dies die Patientin, der Patient nicht wünscht.

Kann die Patientin, der Patient nicht mehr selber entscheiden und hat sie resp. er in einer Patientenverfügung oder in einem Vorsorgeauftrag eine Vertretung in medizinischen Angelegenheiten bestimmt, wird diese kontaktiert, und sie entscheidet über das weitere Vorgehen.

Weiterführende Informationen
Merkblatt Telefonische Auskunft über Patienten →

7. 5. WEITERGABE VON INFORMATIONEN AN ZUWEISENDE ODER NACHBEHANDELNDE FACHPERSONEN

Die Patientin, der Patient muss vor der Übermittlung von Informationen (Austrittsbericht, Pflegebericht etc.) an die zuweisenden und nachbehandelnden Ärztinnen und Ärzte sowie andere Fachpersonen und Institutionen (z.B. Spitex, Heime), welche die Behandlung und Betreuung unmittelbar übernehmen, informiert werden. Die Patientin, der Patient muss mit der Informationsweitergabe einverstanden sein.

7. 6. AUSKÜNFTE ÜBER VERSTORBENE PATIENTEN, PATIENTINNEN

Der Schutz des Patientengeheimnisses sowie die berufliche Schweigepflicht werden mit dem Tod der Patientin, des Patienten nicht aufgehoben, sondern dauern fort. Weil die verstorbene Person nicht mehr in die Datenweitergabe einwilligen

kann, muss vor einer Datenweitergabe beim kantonsärztlichen Dienst des Kantons Bern um Entbindung von der Schweigepflicht ersucht werden.

7. 7. BEFREIUNG VON DER BERUFLICHEN SCHWEIGEPFLICHT DURCH DEN KANTONSÄRZTLICHEN DIENST

In der Praxis braucht es in folgenden Fällen eine Einbindung durch den kantonsärztlichen Dienst:

- Gefährdungsmeldung an die KESB;
- Auskünfte im Rahmen von Strafverfahren (ausser es besteht eine Meldepflicht oder ein Melderecht);
- Auskünfte über verstorbene Patienten, Patientinnen (bspw. in Haftpflichtverfahren, Aktenherausgabe an Angehörige).

7. 8. GESETZLICHE MELDEPFLICHTEN UND MELDERECHTE

Liegt eine gesetzliche Meldepflicht oder ein gesetzliches Melderecht vor, braucht die an die Schweigepflicht gebundene Fachperson die betroffene Patientin, den betroffenen Patienten nicht vorgängig um eine Einwilligung zu ersuchen.

Liegt eine gesetzliche Meldepflicht vor, muss die Fachperson den Vorfall zwingend und unverzüglich innerhalb der vorgeschriebenen Fristen der zuständigen Behörde melden.

Bei einem gesetzlichen Melderecht kann die Fachperson die zuständige Stelle informieren, muss dies aber nicht zwingend tun.

Weiterführende Informationen
Merkblatt Gesetzliche Meldepflichten & Melderechte →

7. 9. BERICHTVERSAND AN SOZIALVERSICHERUNGEN

Die Sozialversicherungsgesetze sehen Auskunftspflichten von Leistungserbringern gegenüber Sozialversicherern (Krankenkassen, Unfall- und Invalidenversicherung) vor. Auskünfte werden nur auf Anfrage hin erteilt; der Umfang wird von der anfragenden Sozialversicherung bestimmt.

Weiterführende Informationen
Merkblatt Berichtversand an Krankenkassen →

8. KONTROLLMÖGLICHKEITEN

Es wird darauf hingewiesen, dass Benutzeraktivitäten auf IT-Systemen (z.B. Zugriffe, aufgerufene Webseiten, Metadaten des E-Mail-Verkehrs etc.) mitprotokolliert werden. Eine Einsicht in diese Aufzeichnungen erfolgt jedoch ausschließlich bei konkretem und begründetem Verdacht der missbräuchlichen Nutzung.

9. EINHALTUNG DER WEISUNG

Die Einhaltung der vorliegenden Weisung wird u.a. anhand von automatisch erstellten Aufzeichnungen überprüft (Protokollierung der Benutzeraktivitäten). Für Kontrollen werden die Empfehlungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sinn- und sachgemäss angewandt.

Verstösse gegen diese Weisung können disziplinarische und / oder personalrechtliche Massnahmen zur Folge haben.

10. INKRAFTTRETEN

Die Weisung tritt am 1. September 2023 in Kraft und ersetzt das Reglement Informationssicherheit und Datenschutz vom 1. Juni 2018 und die Weisung für den sicheren Umgang mit Informations- und Kommunikationsmitteln vom 1. Juni 2018 sowie alle früheren Regelungen und Bestimmungen der Lindenhofgruppe AG respektive deren Spitäler, welche zu dieser Weisung im Widerspruch stehen.

2 Ausnahme Kindeswohlgefährdungsmeldung: **der behandelnde Arzt** braucht für die Meldung einer **Kindeswohlgefährdung** an die KESB keine Entbindung von der Schweigepflicht (gesetzliches Melderecht).

Ausnahme akute Notsituation bei Erwachsenen: besteht für eine erwachsene Person eine erhebliche Gefahr, darf sofort und ohne vorgängige Entbindung von der Schweigepflicht eine Gefährdungsmeldung an die KESB gemacht werden.

Lindenhofgruppe
Postfach | 3001 Bern

lindenhofgruppe.ch

PASSWORTSICHERHEIT

INFORMATIONSSICHERHEIT UND DATENSCHUTZ

Informationssicherheit (IS) und Datenschutz (DS) sind für das Verhalten im beruflichen Alltag jeder Mitarbeiterin und jedes Mitarbeiters der Lindenhofgruppe wichtig und auch vom Gesetzgeber gefordert. In dieser Ausgabe behandeln wir den korrekten und sicheren Umgang mit Passwörtern.

PASSWORTRICHTLINIEN

Passwörter müssen mindestens 10-stellig sein. Ausserdem müssen sie mindestens drei der folgenden Kriterien enthalten:

- Grossbuchstaben
- Kleinbuchstaben
- Zahlen
- Sonderzeichen, wie: !, $, ?, @ usw.

GRUNDSÄTZLICH UND WICHTIG

Passwörter...

- sind geheim und dürfen nicht schriftlich aufbewahrt werden.
- sind persönlich und dürfen nicht an Dritte weitergegeben werden.
- dürfen auch keinem Support-Mitarbeiter, weder intern noch extern, mitgeteilt werden.
- sollten in regelmässigen Abständen, spätestens nach sechs Monaten, geändert werden.
- Bei Passwort-Missbrauch ist die IT-Abteilung umgehend zu kontaktieren.

WIE ERSTELLE ICH EIN SICHERES PASSWORT?

1. Verwenden Sie keine Begriffe aus Wörterbüchern, Ortsnamen oder Namen.
2. Nicht zu verwenden sind: Teile Ihres Namens, Ihr Login oder Ihre E-Mail-Adresse, Ihre Personal- oder Telefonnummer.
3. Meiden Sie persönliche Daten von sich oder Ihren Verwandten, wie z. B. Geburtsdaten oder Postadressen.
4. Vermeiden Sie Standardschreibweisen. Beispiele:
   a. Ersetzen Sie korrekte Schreibweisen durch Zahlen und Sonderzeichen, so wird aus Passwort = P@55w0rth
   b. Verwenden Sie eine spezielle Taktik beim Tippen des Passworts, indem Sie jeweils eine Taste nach rechts rutschen. So wird aus Passwort = Qsddeptz
   c. Streuen Sie zufällig Zahlen und Sonderzeichen ein, so kann aus Passwort z. B. P8s6w.rt werden
5. Es gibt zwei Alternativen zu einem Passwort, die einfach zu merken, aber sicher sind:
   a. Satzkürzel. Mit diesem System benutzen Sie die Anfangsbuchstaben und die passenden Zahlen eines für Sie einfach zu merkenden Satzes.
   Beispiel: Ich habe ein sicheres Passwort = iH1sP
   b. Passphrase. Ein leicht zu merkender Satz wird, durch die Vermeidung von Standardschreibweisen, zum Passwort. Beispiel: Ich liebe meine Tastatur = !Ich!ebeme!neT@5t@tur

Lindenhofgruppe | Informatik
Tel. + 41 31 366 90 09 | servicedesk@lindenhofgruppe.ch

lindenhofgruppe.ch

Im Sinne eines Archivs bündeln wir alle gegebenen Informationen im Intranet.
Auf diesen beiden Seiten finden Sie die entsprechenden Beiträge sowie weiterführende Informationen:
Services/Rechtsdienst/Datenschutz und Services/Informatik/Informationssicherheit.
Sollten Sie Fragen zu diesen Themen oder akuten Handlungsbedarf haben, wenden Sie sich an den IT-Service-Desk der Lindenhofgruppe: servicedesk@lindenhofgruppe.ch

LINDENHOFGRUPPE

07.2023

HOME-OFFICE

INFORMATIONSSICHERHEIT UND DATENSCHUTZ

Mitarbeiterinnen und Mitarbeiter, die im Home-Office arbeiten, sind attraktive Ziele für Cyber-Kriminelle. Die Angreifer nutzen die Situation aus, um Zugriff auf Unternehmensnetzwerke zu erhalten. Auch in der Lindenhofgruppe nutzt eine steigende Zahl von Personal den Fernzugriff auf unsere IT-Systeme. Deshalb erinnern wir Sie an einige wichtige Grundsätze, deren Einhaltung zur Sicherheit der Lindenhofgruppe-Netzwerke beiträgt. Hier nennen wir Ihnen einige Beispiele für derartige Angriffsversuche.

Phishing-Versuche
E-Mails, mit denen versucht wird an vertrauliche Daten zu gelangen, indem man den Empfänger dazu verleitet aufgrund eines vorgetäuschten Problems eine Antwort zu senden oder einen Anhang bzw. Link zu öffnen. Oft scheinen solche E-Mails von einer vertrauenswürdigen Quelle (z. B. Bank, Mitarbeiter) zu stammen.

→ Mehr bei Sicherheit bei E-Mails

Angriffe, um beim Remote-Login Passwörter abzufangen
Gefälschte Login-Seiten, Aufforderung zur Änderung Ihrer Passwörter.

→ Mehr bei Passwortsicherheit

Angriffe mit Malware über den privaten Internet-Anschluss

→ Mehr bei Schadsoftware und Computerviren

Wichtig – auch im Home-Office
Die geltenden Datenschutz- und Nutzungsbestimmungen der Lindenhofgruppe für die ICT-Infrastruktur sind durch geeignete technische und/oder organisatorische Massnahmen durchgehend sicherzustellen.

→ Mehr Tipps für den ICT-Schutz im Home-Office

TIPPS

Schutz von Daten und Computer

- Halten Sie die Einstellungen auf Ihrem privaten Computer immer aktuell und installieren Sie regelmässig Udpates. (Windows Updates, aktueller Virenschutz, Aktivierung Windows-Firewall).
- Nutzen Sie Ihren geschäftlichen Computer nicht für private Zwecke und machen Sie diesen nicht zugänglich für Kinder oder Familienangehörige.
- Aktivieren Sie auch zu Hause bei jedem Verlassen des Computers die Bildschirmsperre.
- Versenden Sie keine sensiblen Daten unverschlüsselt oder ungeschützt per E-Mail.
- Versenden Sie keine geschäftlichen Informationen über private E-Mail-Konten.
- Überprüfen Sie die Richtigkeit von Login-Seiten, z.B.: portal.lindenhofgruppe.ch

Telefon- und Videokonferenzen

- Bei Nichtverwendung: Mikrofon stumm schalten.
- Deaktivieren Sie standardmässig Ihre Kamera. Decken Sie das Objekt ab.
- Führen Sie keine geschäftlichen Gespräche im Freien (Balkon / Öffentlichkeit).
- Vorsicht beim Screen-Sharing. Achten Sie darauf, welche Inhalte Sie für andere Teilnehmer sichtbar machen.

Lindenhofgruppe | Informatik
Tel. + 41 31 366 90 09 | servicedesk@lindenhofgruppe.ch

lindenhofgruppe.ch

Im Sinne eines Archivs bündeln wir alle gegebenen Informationen im Intranet.
Auf diesen beiden Seiten finden Sie die entsprechenden Beiträge sowie weiterführende Informationen:
Services/Rechtsdienst/Datenschutz und Services/Informatik/Informationssicherheit.
Sollten Sie Fragen zu diesen Themen oder akuten Handlungsbedarf haben, wenden Sie sich an den IT-Service-Desk der Lindenhofgruppe: servicedesk@lindenhofgruppe.ch

LINDENHOFGRUPPE

07.2023

SICHERHEIT BEI E-MAILS

INFORMATIONSSICHERHEIT UND DATENSCHUTZ

GRUNDREGELN FÜR E-MAILS

- Die geschäftliche E-Mail-Adresse darf ausschliesslich für geschäftliche Zwecke genutzt werden.
- Vertrauliche Daten (z. B. Patientendaten) dürfen nur verschlüsselt versendet werden. Dazu muss der HIN-Gateway verwendet werden.
- E-Mails aus zweifelhafter Quelle dürfen nicht geöffnet und müssen unverzüglich gelöscht werden.
- Öffnen Sie keine Anhänge / Links in E-Mails aus unbekannter Quelle bzw. bei Zweifeln an der Echtheit.
- Die korrekte Adressierung und Richtigkeit der Anhänge sollte vor Versand nochmals überprüft werden.

SICHERHEITSRISIKEN IM ZUSAMMENHANG MIT E-MAILS

- Falscher Empfänger / Anhang
- Unverschlüsselter Datenversand
- Links / Anhänge, hinter denen sich Viren, Trojaner oder andere Malware verbergen

BEKANNTE ANGRIFFSTAKTIKEN

Phishing

E-Mails, mit denen versucht wird an vertrauliche Daten zu gelangen, indem man den Empfänger dazu verleitet aufgrund eines vorgetäuschten Problems eine Antwort zu senden oder einen Anhang bzw. Link zu öffnen. Oft scheinen solche E-Mails von einer vertrauenswürdigen Quelle (z. B. Bank, Mitarbeiter) zu stammen.

Spoofing

Die richtige Absender- bzw. Linkadresse wird hinter einer legitimen Adresse verborgen, d.h. der Empfänger sieht auf den ersten Blick nur die vorgetäuschte Adresse.

WIE ERKENNEN SIE SOLCHE ANGRIFFE?

- Achten Sie auf fehlerhafte Schreibweisen und Grammatik.
- Überprüfen Sie, ob die E-Mail-Adresse des Absenders stimmt, indem Sie auf dem Absendernamen doppelklicken.
- Überprüfen Sie, ob ein Link stimmt, indem Sie **(ohne zu klicken!)** mit der Maus über dem Link verweilen.
- Es sind Anhänge vorhanden, deren Existenz im E-Mail nicht plausibel begründet wird.

Sollten Ihnen bei diesen Punkten Unstimmigkeiten auffallen, öffnen Sie keine Links / Anhänge und löschen Sie die E-Mail unverzüglich.

Lindenhofgruppe | Informatik
Tel. + 41 31 366 90 09 | servicedesk@lindenhofgruppe.ch

lindenhofgruppe.ch

Im Sinne eines Archivs bündeln wir alle gegebenen Informationen im Intranet.
Auf diesen beiden Seiten finden Sie die entsprechenden Beiträge sowie weiterführende Informationen:
Services/Rechtsdienst/Datenschutz und Services/Informatik/Informationssicherheit.
Sollten Sie Fragen zu diesen Themen oder akuten Handlungsbedarf haben, wenden Sie sich an den IT-Service-Desk der Lindenhofgruppe: servicedesk@lindenhofgruppe.ch

LINDENHOFGRUPPE

07.2023

SOCIAL ENGINEERING

INFORMATIONSSICHERHEIT UND DATENSCHUTZ

Was ist Social Engineering? Social Engineering ist eine gezielte IT-Security-Attacke, die auf das Personal einer Unternehmung ausgerichtet ist. Die Angreifer versuchen, durch Manipulation und Tricks, Mitarbeiterinnen und Mitarbeiter der Unternehmung dazu zu bewegen, ihnen beim Erreichen ihrer Ziele zu helfen. Ziele sind zum Beispiel: Zugang zu Patientendaten, Login-Daten oder Geldüberweisungen zu erhalten. Technische Sicherheitsmassnahmen sind bei Social Engineering in der Regel nutzlos. Einzig das Verhalten der betroffenen Mitarbeiterinnen und Mitarbeiter kann den Erfolg einer solchen Attacke wirkungsvoll verhindern.

WAS KÖNNEN SIE TUN?

- Geben Sie niemals Ihre Login-Daten bekannt. Auch nicht an IT-Support-Mitarbeiterinnen oder -Mitarbeiter.
- Achten Sie auf das Verhalten der Personen um Sie herum. Schaut Ihnen jemand beim Einloggen in Ihren PC zu?
- Konfrontieren Sie unbekannte Personen, die sich in einem Raum oder Bereich aufhalten, der nicht der Öffentlichkeit zugänglich ist.
  Denken Sie daran: Ausweise können leicht gefälscht werden. Klären Sie im Zweifelsfall ab, ob die entsprechende Person wirklich von der Lindenhofgruppe aufgeboten wurde.
- Seien Sie vorsichtig bei wichtigen Anweisungen, die Sie per E-Mail oder Telefon erhalten. Insbesondere, wenn Sie als «dringend» eingestuft sind und kurz vor dem Wochenende erteilt werden. Überprüfen Sie die Richtigkeit der Anweisung, indem Sie über einen anderen Kommunikationskanal bei der entsprechenden Person nachfragen.
- Schliessen Sie keine unbekannten Wechseldatenträger (z. B. USB-Sticks) an Ihren Computer an.
- Öffnen Sie keine Links in E-Mails aus unbekannter Quelle bzw. bei Zweifeln an der Echtheit.
- Melden Sie verdächtige Vorfälle und Hardware-Diebstähle umgehend der IT-Abteilung.

BEISPIELE VON SOCIAL ENGINEERING

Der Angreifer…

- folgt Ihnen durch eine Tür, die Sie mit Ihrem Badge aufgeschlossen haben.
- gibt sich als Lieferant aus und bittet Sie, ihm Zugang zu einem abgeschlossenen Raum oder Bereich zu verschaffen.
- gibt sich am Telefon als IT-Support-Mitarbeiter aus und bittet Sie, ihm Ihre Login-Daten zu nennen.
- lässt an einer offensichtlichen Stelle einen manipulierten USB-Stick zurück. Der Finder schliesst diesen USB-Stick am Computer an und infiziert so den Computer.
- sendet Ihnen per E-Mail, unter falschem Namen (z. B. CEO), die Bitte für eine umgehende Geldüberweisung.

Lindenhofgruppe | Informatik
Tel. + 41 31 366 90 09 | servicedesk@lindenhofgruppe.ch

lindenhofgruppe.ch

Im Sinne eines Archivs bündeln wir alle gegebenen Informationen im Intranet.
Auf diesen beiden Seiten finden Sie die entsprechenden Beiträge sowie weiterführende Informationen:
Services/Rechtsdienst/Datenschutz und Services/Informatik/Informationssicherheit.
Sollten Sie Fragen zu diesen Themen oder akuten Handlungsbedarf haben, wenden Sie sich an den IT-Service-Desk der Lindenhofgruppe: servicedesk@lindenhofgruppe.ch

LINDENHOFGRUPPE

07.2023

SCHADSOFTWARE UND COMPUTERVIREN

INFORMATIONSSICHERHEIT UND DATENSCHUTZ

Was bedeutet Schadsoftware? Benutzerinnen und Benutzer von Desktop-Computern (PC / Mac) und Smart Devices (Smartphones / Tablets) sind ständig der Bedrohung durch neue Computerviren und Schadsoftware (sogenannte Malware) ausgesetzt. Diese Programme werden ohne Zustimmung der Nutzerin oder des Nutzers installiert und können eine Reihe unangenehmer Folgen haben: Sie können die Systemleistung reduzieren, innerhalb Ihres Systems nach persönlichen Daten suchen, Informationen löschen oder sogar den Betrieb computergesteuerter Hardware beeinträchtigen. Hacker entwickeln immer raffiniertere Methoden, um in Systeme einzudringen.

DAS KÖNNEN SIE PRÄVENTIV TUN

Im geschäftlichen Umfeld übernimmt die ICT der Lindenhofgruppe folgende Arbeiten:

- Netzwerk mit einer Firewall schützen
- E-Mailverkehr durch einen Spam- und Antivirus /Malware-Filter schützen
- Endgeräte (PCs, Notebooks mit einer aktuellen Antivirus- und Malware-Software schützen
- Antivirus-Software stets aktiv und aktuell halten (Updates regelmässig installieren)
- Die verfügbaren (Sicherheits-)Updates von Betriebssystemen (z. B. Windows, Android) und Software zeitnah installieren

Sie als Benutzer unterstützen uns, indem Sie:

- Keine unbekannten Wechseldatenträger (z. B. USB-Sticks) benutzen
- Keine Links in E-Mails von unbekannten Absendern oder Quellen anklicken. Das gilt auch, wenn Sie die Echtheit einer E-Mail bezweifeln
- Private Endgeräte (Notebooks, Smartphones, Tablets) mit einer aktuellen Antivirus-Software schützen (Weitere Informationen → av-test.org)
- Melden Sie verdächtige Vorfälle und Hardware-Diebstähle umgehend der IT-Abteilung

ARTEN VON SCHADSOFTWARE UND VIREN

- **Computerviren:** Infizierung von Dateien und Weiterverbreitung per E-Mail oder USB-Sticks
- **Würmer:** Infektion von Geräten und selbständige Verbreitung über das Netzwerk
- **Adware:** Automatische Anzeige von nichterwünschten Werbeanzeigen
- **Spyware:** Spionagesoftware zur illegalen Erfassung von Daten auf Ihrem Endgerät
- **Ransomware:** Infizierung von Geräten und Verschlüsselung Ihrer gespeicherten Dokumente (dient häufig der Erpressung)
- **Bots:** Programme zur Ausführung von Aktionen auf Ihren Computern
- **Rootkits:** Für Fernzugriff auf Ihren Computer
- **Trojanische Pferde:** Programme, die schädliche Änderungen an Ihrem Computer vornehmen
- **Bugs:** Fehler im Softwarecode, die Hacker für Attacken missbrauchen

Lindenhofgruppe | Informatik
Tel. + 41 31 366 90 09 | servicedesk@lindenhofgruppe.ch

lindenhofgruppe.ch

Im Sinne eines Archivs bündeln wir alle gegebenen Informationen im Intranet.
Auf diesen beiden Seiten finden Sie die entsprechenden Beiträge sowie weiterführende Informationen:
Services/Rechtsdienst/Datenschutz und Services/Informatik/Informationssicherheit.
Sollten Sie Fragen zu diesen Themen oder akuten Handlungsbedarf haben, wenden Sie sich an den IT-Service-Desk der Lindenhofgruppe: servicedesk@lindenhofgruppe.ch

LINDENHOFGRUPPE

07.2023

HERAUSGABE DER PATIENTENDOKUMENTATION

INFORMATIONSSICHERHEIT UND DATENSCHUTZ

GRUNDSATZ

Patientinnen und Patienten haben ein Recht auf Auskunft über den Inhalt ihrer Krankengeschichte und dürfen auch Kopien und Ausdrucke verlangen. Dieses Auskunftsrecht ist umfassend und schliesst alle vorhandenen Dokumente mit ein (Papierunterlagen, elektronische Aufzeichnungen, Pflegebericht, Geburts- und Wochenbettverlauf, Labordaten etc.). Das Einsichtsrecht umfasst auch Schreiben von anderen Ärzten, die in der Krankengeschichte figurieren, selbst wenn diese verletzende Bemerkungen enthalten sollten. Die Auskunft und die Herausgabe von Kopien und Ausdrucken ist grundsätzlich kostenlos (Ausnahmen sind denkbar, wenn eine Person bereits zum zweiten oder dritten Mal Kopien der gesamten KG verlangt).

HERAUSGABE VON KOPIEN UND AUSDRUCKEN

Zuständig zur Aktenherausgabe sind die Direktions- und Spitalleitungssekretariate (Standortsekretariat) sowie die Geburtensekretariate. Es gilt folgendes zu beachten:

1) Die Patientin/der Patient reicht ein schriftliches Gesuch ein, indem sie/er mitteilt, welche Akten sie/er benötigt. Zur Identifizierung brauchen wir eine Kopie der ID/Pass und die Adresse. EineBegründung ist nicht erforderlich.
2) Der fallführende Arzt wird durch das Standortsekretariat über die Aktenherausgabe informiert,insbesondere dann, wenn die Herausgabe des OP- und Austrittsberichts oder der gesamtenKrankengeschichte verlangt wird.
3) Im Patientendossier wird immer dokumentiert, wer was wem wann herausgegeben hat.
4) Die Unterlagen müssen von der Patientin oder vom Patienten persönlich abgeholt werden; Postversand ist nur in Ausnahmefällen und mit Einschreiben zulässig.
5) Der Versand von Patientendaten per eMail ist nur an eine HIN-verschlüsselte Adresse erlaubt.

EINSICHTNAHME VOR ORT

Die Einsichtnahme vor Ort stellt eine besondere Form des Auskunftsrechts dar. Beim Auskunftsrecht werden normalerweise Kopien oder Ausdrucke der Gesuchstellerin oder dem Gesuchsteller persönlich abgegeben.
Bei der Einsichtnahme hingegen wird die Krankengeschichte nur eingesehen und mit der Ärztin oder dem Arzt besprochen. Die Einsichtnahme vor Ort kann zur Verarbeitung beispielsweise einer schweren Krankheit oder bei Schicksalsschlägen mehr beitragen als die Herausgabe von Kopien. Die betroffene Person kann dennoch die Herausgabe von Kopien und Ausdrucken verlangen.

SCHUTZ DER PATIENTIN ODER DES PATIENTEN VOR DER WAHRHEIT (therapeutisches Privileg)

Die betroffene Person hat immer ein Recht auf Akteneinsicht. Wenn jedoch die Gefahr besteht, dass der Patientin oder dem Patienten durch die unmittelbare und unvorbereitete Einsicht in seine Gesundheitsdaten ein Schaden erwachsen könnte, kann die Ärztin oder der Arzt die Daten einem vom Patienten bestimmten Vertrauensarzt, beispielsweise dem Hausarzt, weitergeben.

HERAUSGABE DER ORIGINALE

Die Original-Behandlungsdokumentation wird nur herausgegeben, wenn die Patientin oder der Patient die Lindenhofgruppe schriftlich (mit Datum und Unterschrift) von der Aufbewahrungspflicht befreit. Vor der Herausgabe muss immer eine Kopie des gesamten Patientendossiers erstellt werden. Im Patientendossier wird vermerkt, wem wann was herausgegeben wurde.

→ Mehr zum Ablauf → Zur Checkliste

TELEFONISCHE AUSKUNFT ÜBER PATIENTEN[1]

INFORMATIONSSICHERHEIT UND DATENSCHUTZ

1 Zur besseren Lesbarkeit wird im Text nur die männliche Form verwendet.
2 Als Angehörige gelten Ehepartner, eingetragene Partner, Lebenspartner im gemeinsamen Haushalt sowie nahe Verwandte (Eltern, Kinder, Geschwister, Grosseltern, Enkel).
3 VIP sind bekannte Persönlichkeiten wie Sportler, Schauspieler, Musiker, Politiker und andere Prominente.
4 Bedrohte Personen sind Personen in einer Gefährdungslage wie bspw. Opfer von häuslicher Gewalt oder von Gewaltverbrechen (Täter auf der Flucht könnte das Opfer erneut aufsuchen wollen).

Normalfall: Fragen sie den Patienten, welche Informationen sie wem weitergeben dürfen. Diese Einwilligung kann der Patient mündlich erteilen. Dokumentieren sie seinen Willen in der Patientenakte. Notieren sie die Telefonnummer der Person, welcher sie mit Einwilligung des Patienten Auskunft geben dürfen. Rufen sie die Angehörigen/Vertrauensperson an, statt auf ihren Anruf zu warten. Bei Notfall-Eintritten und Verlegungen (in ein anderes Spital oder Psychiatrie) werden die Angehörigen durch den Arzt informiert. Dies kann auch telefonisch erfolgen.

Bei erstmaligen oder spontanen Anrufen auf der Station, die sie vorgängig nicht mit dem Patienten besprechen konnten, gehen sie nach Folgendem Raster vor.

Wer ruft an?	Informationen zur Behandlung/Gesundheit	Allgemeine Informationen
Angehörige[2]	Keine Informationen zur Behandlung/zum Gesundheitszustand am Telefon. Ausnahme: Sie kennen die Person und wissen, dass der Patient will, dass sie informiert wird.	Nach Identitätsprüfung durch Sicherheitsfragen* dürfen ohne Rücksprache mit Patient folgende Auskünfte gegeben werden: • Besuchszeiten • Zimmernummer • direkte Telefonnummer • Austritt erfolgt wann Bei VIP[3] oder bedrohten Personen[4] nur nach Rücksprache mit Pat.
Angehörige[2] und Vertretungspersonen, wenn Patient urteilsunfähig ist (bspw. Notfall-Eintritt)	Keine Informationen zur Behandlung/zum Gesundheitszustand am Telefon. Nach Identitätsprüfung durch Sicherheitsfragen* dürfen folgende Auskünfte gegeben werden: • Spitaleintritt • Allgemeine Auskunft zum Zustand; ab wann ist Besuch möglich etc. • Todesfall, situationsgerecht (durch Arzt) • Verlegung (nicht Psychiatrie)	Nach Identitätsprüfung durch Sicherheitsfragen* dürfen folgende Auskünfte gegeben werden: • Besuchszeiten • Zimmernummer • direkte Telefonnummer • Austritt erfolgt wann Bei VIP[3] oder bedrohten Personen[4] besser keine Auskunft geben oder nur nach einer sehr genauen Identitätsprüfung.
Besucher, Freunde, Nachbarn und andere Dritte	Keine Auskunft zur Behandlung/zum Gesundheitszustand. Der Anrufer muss sich an den Patienten wenden; ist dieser urteilsunfähig, an die Angehörigen.	Nach Identitätsprüfung durch Sicherheitsfragen* dürfen ohne Rücksprache mit Patient folgende Auskünfte gegeben werden: • Besuchszeiten • Zimmernummer • direkte Telefonnummer • Austritt erfolgt wann Bei VIP[3] oder bedrohten Personen[4] nur nach Rücksprache mit Pat.
Behörde (Polizei, Gemeinde etc.)	Keine Auskunft am Telefon.	Keine Auskunft am Telefon.

*** Es muss überprüft werden, ob es sich wirklich um Angehörige[2] des Patienten handelt. Beispiele für Sicherheitsfragen:**

- In welcher Beziehung stehen sie zum Patienten?
- Können sie mir das Geburtsdatum des Patienten sagen?
- Warum befindet sich der Patient im Spital?
- Bei Notfällen: Wie haben sie von der Spitaleinweisung erfahren?
- Im Zweifelsfall: Telefonnummer aufnehmen, zusätzliche Abklärungen tätigen (Patient fragen, Tel.-Nummer googeln etc.) und zurückrufen.

LINDENHOFGRUPPE

07.2023

BERICHTSVERSAND AN KRANKENKASSEN

INFORMATIONSSICHERHEIT UND DATENSCHUTZ

Die Krankenkassen sind im Bereich der obligatorischen Krankenpflegeversicherung berechtigt und verpflichtet, zu prüfen, ob die erbrachten Leistungen das Wirtschaftlichkeitsgebot erfüllen. Die zu Lasten der obligatorischen Krankenversicherung erbrachten Leistungen müssen wirksam, zweckmässig und wirtschaftlich sein (Art. 32 Abs. 1 KVG).

Häufig verlangen die Krankenkassen von den Spitälern die Herausgabe der vollständigen Austritts- und Operationsberichte. Diese enthalten besonders schützenswerte Personendaten und teilweise auch Informationen über die Patienten, welche nicht Grund für die Spitalbehandlung waren. Hier stehen der Datenschutz und das Berufsgeheimnis im Spannungsfeld zur Pflicht der Krankenkassen, im Bereich der obligatorischen Krankenversicherung zu prüfen, ob die erbrachten Leistungen wirksam, zweckmässig und wirtschaftlich sind. Die folgenden Ausführungen stützen sich auf die Empfehlungen des Eidgenössischen Datenschutzbeauftragten. Sie zeigen Ihnen, wie Sie bei der Herausgabe von Austritts- und Operationsberichten an die Krankenkassen vorgehen sollen.

BERICHTVERSAND UND AUSKÜNFTE IM OKP-BEREICH

Bezüglich der Weitergabe von Austritts- und Operationsberichten empfiehlt der Eidgenössische Datenschutzbeauftragte ein 3-stufiges Vorgehen:

1. Stufe: Die Spitäler stellen eine detaillierte und verständliche Rechnung.

2. Stufe: Benötigt der Versicherer im Einzelfall zusätzliche Angaben, kann er demLeistungserbringer schriftlich auf den konkreten Fall bezogene, spezifische Fragen stellen. Der Versicherer stellt der versicherten Person zur Information eine Kopie der Anfrage zu.

3. Stufe: Sind diese Angaben ausnahmsweise nicht ausreichend, kann der Versicherer einenAustritts- oder Operationsbericht (oder Notfallbericht) einholen. Er stellt der versichertenPerson die Informationen in Kopie zu.

Die Daten der 2. und 3. Stufe werden ausschliesslich dem Vertrauensarzt mitgeteilt. Eine persönliche Einwilligung des Patienten für die Datenherausgabe ist nicht erforderlich, weil eine gesetzliche Auskunftspflicht besteht (Art. 42 KVG).

Gemäss Rechtsprechung des Bundesgerichts entscheidet der Vertrauensarzt, welche Unterlagen er zur Überprüfung der Kostenübernahmepflicht benötigt. Kommt der Vertrauensarzt zum Schluss, dass die Beantwortung von Fragen nicht genügt, kann er weitere Unterlagen anfordern wie bspw. die Austritts- und Operationsberichte. Der Vertrauensarzt resp. die Krankenkasse ist jedoch verpflichtet, den Patienten vorgängig auf seine Wahlmöglichkeit hinzuweisen, dass die Unterlagen ausschliesslich dem Vertrauensarzt zugestellt werden (Art. 59a Abs. 5 KVV). Es widerspricht hingegen dem Verhältnismässigkeitsprinzip, wenn ein KVG-Versicherer systematisch Austritts- und Operationsberichte verlangt.

BERICHTVERSAND UND AUSKÜNFTE IM VVG-BEREICH

Im Zusatzversicherungsbereich fehlt eine gesetzliche Regelung, wonach der Patient verlangen kann, dass Gesundheitsdaten nur dem Vertrauensarzt bekannt gegeben werden dürfen. Es fehlt auch eine gesetzliche Entbindung von der ärztlichen Schweigepflicht, d.h. es bedarf der ausdrücklichen Einwilligung des Patienten, bevor der Austritts- und Operationsbericht an die Krankenkasse verschickt werden darf. Diese Einwilligung wird in der Regel mit dem Versicherungsvertrag erteilt. Es empfiehlt sich jedoch auch hier die Zustellung ausschliesslich an den Vertrauensarzt, insbesondere dann, wenn der Patient beim gleichen Versicherer grund- und zusatzversichert ist.

LINDENHOFGRUPPE

07.2023

GESETZLICHE MELDE-PFLICHTEN & MELDERECHTE

INFORMATIONSSICHERHEIT UND DATENSCHUTZ

1 VORBEMERKUNG

Gesetzliche Meldepflichten und Melderechte bestehen sowohl auf Ebene des Bundes als auch auf jener der Kantone (hier des Kantons Bern). Besteht eine gesetzliche Pflicht, einer Behörde eine Meldung zu machen, oder ist der Arzt[1] dazu von Gesetzes wegen berechtigt, so muss er weder die Einwilligung des Patienten einholen noch durch das Kantonsarztamt von der ärztlichen Schweigepflicht entbunden werden.
ACHTUNG: Die nachfolgende Aufzählung ist nicht abschliessend.

2 MELDEPFLICHTEN

Liegt eine gesetzliche Meldepflicht vor, muss der Arzt den Vorfall zwingend und unverzüglich innerhalb der vorgeschriebenen Fristen der zuständigen Behörde melden. Unterlässt er die Meldung, macht er sich strafbar (gegebenenfalls auch wegen Begünstigung).

2.1 Aussergewöhnliche Todesfälle (Art. 28 Abs. 1 Gesundheitsgesetz[2], Art. 253 StPO[3])

[1] Ärzte sind gemäss Gesundheitsgesetz verpflichtet, aussergewöhnliche Todesfälle (AgT) zu melden. Aussergewöhnliche Todesfälle sind alle plötzlich und unerwartet eintretenden sowie gewaltsamen Todesfälle und solche, die vielleicht gewaltsam verursacht sein könnten. Meldepflichtig sind auch Fälle, bei denen der Tod erst nach mehreren Tagen oder sogar Wochen eintritt, der Vorfall / Unfall aber das für die Hospitalisation ausschlaggebende Ereignis war (z.B. Myokardinfarkt mehrere Tage nach einem Verkehrsunfall mit Verletzungen und Blutverlust).

[2] Definition Aussergewöhnlicher Todesfall:
→ Siehe Checkliste

[3] Im Zweifelsfall ist immer eine Meldung zu machen. Es kann auch der Dienstarzt des Instituts für Rechtsmedizin Bern (IRM) informell um Rat gefragt werden (anonyme Schilderung des Falls).

[4] Eine Meldung an die Polizei kann auch zu Lebzeiten einer Person erfolgen, wenn der Exitus einen kaum zu vermeidbaren Ausgang darstellt oder – beispielsweise nach Stürzen zu Hause – Zweifel darüber herrschen, ob Dritte beteiligt waren. Es besteht im kantonalen Gesundheitsgesetz ein Melderecht bei Verdacht auf ein Verbrechen oder Vergehen gegen Leib und Leben, die öffentliche Gesundheit oder die sexuelle Integrität (siehe Ziffer 3.1).

[5] **Meldepflicht:** Das Vorgehen bei Meldungen von aussergewöhnlichen Todesfällen in der Lindenhofgruppe richtet sich nach dem Notfall- und Krisenmanagement. → Siehe Intranet

1 Die in diesem Merkblatt verwendeten Bezeichnungen beziehen sich auf Personen beider Geschlechter.
2 Bernisches Gesundheitsgesetz vom 2. Dezember 1984 (GesG; BSG 811.01)
3 Schweizerische Strafprozessordnung vom 5. Oktober 2007 (stopp; SR 312.0)
4 Bundesgesetz über die Bekämpfung übertragbarer Krankheiten am Menschen vom 18. Dezember 1970 (SR 818.101)
5 Verordnung vom 13. Januar 1999 über die Meldung übertragbarer Krankheiten des Menschen (Melde-Verordnung; SR 818.141.1)

07.2023

2.2 Spezialfall: Tod unter medizinsicher Behandlung (Art. 28 Abs. 1 GesG, Art. 253 StPO)

[1] Der Todesfall unter ärztlicher Behandlung ist dann ein aussergewöhnlicher Todesfall und unterliegt der Meldepflicht, wenn der Todeseintritt nicht eine 'nach der ärztlichen Erfahrung" zu erwartende Situation darstellt. Wenn also ein an und für sich gesunder Patient während oder nach einem ärztlichen Eingriff unerwartet plötzlich verstirbt.

[2] Im Zweifelsfall ist immer eine Meldung zu machen, statt sich dann Vertuschungsvorwürfen auszusetzen. Bei unklaren Fällen kann auch der Dienstarzt des Instituts für Rechtsmedizin Bern (IRM) informell um Rat gefragt werden (anonyme Schilderung des Falls). Falsche Angaben auf der Todesbescheinigung können den Straftatbestand des falschen ärztlichen Zeugnisses erfüllen (Art. 318 StGB), wobei sowohl die vorsätzliche als auch die fahrlässige Begehung strafbar sind.

[3] Meldepflicht: Das Vorgehen bei Meldungen von aussergewöhnlichen Todesfällen in der Lindenhofgruppe richtet sich nach dem Notfall- und Krisenmanagement. → Siehe Intranet

2.3 Übertragbare Krankheiten (Art. 12 Abs. 1 und 2 Epidemiengesetz[4]; Meldeverordnung[5, 6])

[1] Ärzte, Spitäler und Laboratorien sind gemäss Epidemiengesetz verpflichtet, Beobachtungen zu bestimmten übertragbaren Krankheiten des Menschen zu melden. Welche übertragbaren Krankheiten mit welchen Angaben meldepflichtig sind und in welchen Fällen Ergänzungsmeldungen oder Meldungen von Personalien erforderlich sind, können unter Bundesamt für Gesundheit BAG → admin.ch abgerufen werden: → Melden

[2] **Meldepflicht:** Die vom BAG bezeichneten übertragbaren Krankheiten des Menschen müssen dem Kantonsarzt gemeldet werden. Je nach Diagnose gibt es unterschiedliche gesetzliche „Meldefristen" und Meldeformen, die vom behandelnden Arzt („wer diagnostiziert, meldet") eingehalten werden müssen („Meldefristen" und Formulare sind im Internet unter obiger Adresse abrufbar).

2.4 Unerwünschte Wirkungen und Vorkommnisse im Zusammenhang mit Heilmitteln

2.4.1 Pharmakovigilanz, unerwünschte Arzneimittelwirkung (UAW) (Art. 59 Heilmittelgesetz[7]; Art. 63 Arzneimittelverordnung[8])

[1] Ärzte, Apotheker, Hersteller und Fachpersonen, die Heilmittel anwenden oder abgeben sind gemäss Heilmittelgesetz verpflichtet, unerwünschte Arzneimittelwirkungen zu melden. Alle schwerwiegenden, bisher unbekannten oder in der Fachinformation des betreffenden Arzneimittels ungenügend erwähnten sowie alle weiteren medizinisch wichtigen unerwünschten Wirkungen müssen gemeldet werden. Der Kausalzusammenhang zwischen einem Ereignis und einem Arzneimittel muss nicht nachgewiesen werden, der Verdacht alleine reicht.

[2] Schwerwiegende unerwünschte Wirkungen sind solche, die
- tödlich verlaufen;
- lebensbedrohlich sind;
- zu einer Hospitalisation oder deren Verlängerung führen;
- schwere oder bleibende Schäden verursachen;
- sonst als medizinisch wichtig zu beurteilen sind (z. B. wenn durch eine rechtzeitige medizinische Intervention eine der oben erwähnten Situationen hätte vermieden werden können).

[3] **Meldepflicht:** Schwerwiegende unerwünschte Wirkungen müssen innert 15 Tagen nach Kenntnis, nicht schwerwiegende unerwünschte Wirkungen innert 60 Tagen nach Kenntnis gemeldet werden. Alle Meldung müssen via Intranet erfasst werden: → Meldung erfassen

6 Verordnung des EDI vom 13. Januar 1999 über Arzt- und Labormeldungen (SR 818.141.11)
7 Bundesgesetz über Arzneimittel und Medizinprodukte vom 15. Dezember 2000 (HMG; SR 812.21)
8 Verordnung vom 17. Oktober 2001 über die Arzneimittel (VAM; SR 812.212.21)

2.4.2 Materiovigilanz, schwerwiegende Vorkommnisse mit Medizinprodukten (Art. 66 Medizinprodukteverordnung[9]; Art. 60 Verordnung über In-vitro-Diagnostika[10])

[1] Ärzte, Spitäler und Gesundheitsfachpersonen sind verpflichtet, die aufgrund von Vorkommnissen festgestellten Probleme oder Risiken von Medizinprodukten zu melden.

[2] Unter den Begriff «schwerwiegende Auswirkungen» fallen folgende Ereignisse:

- der Tod eines Patienten, Anwenders oder einer Drittperson
- eine Krankheit oder Verletzung, die zum Tod führen könnte
- eine ständige Beeinträchtigung einer Körperfunktion oder ständige Schädigung eines Körperteils
- die Notwendigkeit einer medizinischen Behandlung um schwerwiegende Auswirkungen auf die Gesundheit zu verhindern (Medikation, neuer oder verlängerter Spitalaufenthalt, usw.)
- schwerwiegende Auswirkungen auf die Gesundheit aufgrund von Fehldiagnosen (z. B. bei In-vitro-Diagnostika)

[3] **Meldepflicht:** Ärzte und Gesundheitsfachpersonen, die bei der Anwendung von Produkten ein schwerwiegendes Vorkommnis feststellen, müssen dieses dem Lieferanten und Swissmedic melden. Die Meldefrist beträgt je nach Risiko 2, 10 oder 15 Tage. Alle Meldung müssen via Intranet erfasst werden: → Meldung erfassen

2.4.3 Hämovigilanz, unerwünschte Reaktionen bei Transfusionen von labilen Blutprodukten (Art. 59 Heilmittelgesetz; Art. 16 Arzneimittel-Bewilligungsverordnung[11]; Art. 37 Arzneimittelverordnung)

[1] Alle an der Transfusionskette beteiligten Personen (z.B. Ärzte und Gesundheitsfachpersonen, die labile Blutprodukte anwenden oder dazu berechtigt sind) sind verpflichtet, unerwünschte Transfusionsreaktionen, Fehler sowie verhinderte Transfusionsfehler (near miss) Swissmedic zu melden. Das Haemovigilance Meldesystem in der Schweiz – Grundlagen → swissmedic.ch sowie die meldepflichtigen Reaktionen, Fehler und Beinahe Fehler sind aufgelistet auf der Website von Swissmedic unter → Was melden?

[3] **Meldepflicht:** Alle unerwünschten Transfusionsreaktionen, Fehler und Beinahe Fehler (near miss) müssen Swissmedic gemeldet werden. Die Meldung bei Todesfällen und Häufungen von Ereignissen sowie bei schwerwiegenden Transfusionsreaktionen sollte sofort erfolgen, spätestens innert 15 Tagen. Für alle anderen Meldungen beträgt die Frist maximal 60 Tage. Alle Meldung müssen via Intranet erfasst werden: → Meldung erfassen

2.5 Schwangerschaftsabbruch (Art. 119 Abs. 5 Strafgesetzbuch[12])

[1] Der Arzt, der einen Schwangerschaftsabbruch vornimmt, ist gemäss Art. 120 Abs. 2 Strafgesetzbuch unter Strafandrohung verpflichtet, den Schwangerschaftsabbruch zu melden. Selbstverständlich dürfen nur straflose Schwangerschaftsabbrüche durchgeführt werden (bis zur 12. Schwangerschaftswoche auf schriftliches Gesuch der schwangeren Frau und ausführlicher Aufklärung durch den Arzt; ab der 13. Schwangerschaftswoche bei medizinischer Indikation).
→ Informationen und das Meldeformular

[2] **Meldepflicht:** Schwangerschaftsabbrüche müssen unter Wahrung der Anonymität der Frau innert einer Woche seit dem Eingriff dem Kantonsarztamt Bern[13] gemeldet werden. Alle Informationen sowie das Meldeformular sind abrufbar unter obiger Adresse.

9 Medizinprodukteverordnung (MepV; SR 812.213
10 Verordnung über In-vitro-Diagnostika (InDV; SR 812.219)
11 Verordnung über die Bewilligung im Arzneimittelbereich vom 14. November 2018 (AMBV; SR 812.212.1)
12 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB; SR 311.0)
13 Art. 15 Abs. 2 lit. n Organisationsverordnung GEF vom 29. November 2000 (OrV GEF; BSG 152.221.121)

2.6 Vorfälle mit Hunden (Art. 78 Tierschutzverordnung[14])

[1] Der behandelnde Arzt ist gemäss Tierschutzverordnung verpflichtet, Vorfälle zu melden, bei denen ein Hund Menschen (oder Tiere) erheblich verletzt hat oder Anzeichen eines übermässigen Aggressionsverhaltens zeigt (und zwar auch dann, wenn der Patient vom eigenen Hund erheblich verletzt wurde und mit der Meldung nicht einverstanden ist).

[2] **Meldepflicht:** Erhebliche Verletzungen durch Hunde müssen dem kantonalen Veterinärdienst des Kantons Bern gemeldet werden.
→ Vorfälle mit Hunden melden

2.7 Gesundheitsschädigung mit möglichem Zusammenhang zum Militärdienst (Art. 84 Militärversicherungsgesetz[15])

[1] Der behandelnde Arzt ist gemäss Militärversicherungsgesetz verpflichtet, die Gesundheitsschädigung sofort der Militärversicherung anzumelden, wenn ein Zusammenhang mit dem Dienst in Betracht kommt oder wenn es der / die Versicherte verlangt. Unter Dienst sind alle der Militärversicherung unterstellten Anlässe und Tätigkeiten (z. B. Militär-, Zivilschutz- oder Zivildienst, Bundesdienst der beruflich Versicherten, Teilnahme an friedenserhaltenden Aktionen und Guten Dienste des Bundes, Angehörige des Schweiz. Korps für humanitäre Hilfe) zu verstehen.

[2] **Meldepflicht:** Gesundheitsschädigungen mit möglichem Zusammenhang zum Militärdienst müssen sofort der Militärversicherung (SUVA) gemeldet werden. → Informationen & Meldeformular

2.8 Entlassung aus fürsorgerischer Unterbringung (Art. 31 Kindes- und Erwachsenenschutzgesetz[16])

[1] Bei einer Entlassung aus einer fürsorgerischen Unterbringung kann eine Nachbetreuung bzw. können von der zuständigen Kindes- und Erwachsenenschutzbehörde (KESB) ambulante Massnahmen (Verhaltensweisen, Meldepflichten bzw. medizinisch indizierte Behandlungen, insbesondere kontrollierte Medikamenteneinnahme) angeordnet werden. Damit diese Nachbetreuung rechtzeitig organisiert werden kann, müssen die KESB und ein allfälliger Beistand vor Entlassung benachrichtigt werden.

[2] **Meldepflicht:** Die für die Entlassung zuständige Einrichtung hat die KESB und einen allfälligen Beistand rechtzeitig über die

3 MELDERECHTE

Der Arzt kann die zuständige Stelle informieren, muss dies aber nicht zwingend tun. Eine Nichtmeldung muss nachvollziehbar und objektiv begründet sein. Bei einem gesetzlichen Melderecht muss der Arzt weder die Einwilligung des Patienten einholen noch durch das Kantonsarztamt von der Schweigepflicht entbunden werden.

3.1 Verdacht auf eine gewisse Straftat (Art. 28 Abs. 2 Gesundheitsgesetz[17])

[1] Der behandelnde Arzt und die behandelnden Gesundheitsfachpersonen sind berechtigt, der Strafverfolgungsbehörde folgende Wahrnehmungen zu melden:

Verdacht auf ein Verbrechen oder Vergehen gegen Leib und Leben

- Einfache und schwere Körperverletzung von Patienten, die durch Dritte herbeigeführt wurde (Kratz-, Schürf-, Schnitt- oder Bisswunde, Knochenbruch, Vergiftung, Gehirnerschütterung, Schädigung eines wichtigen Organs oder Glieds, andere Schädigung des Körpers oder der körperlichen oder geistigen Gesundheit etc.).

- Gefährdung des Lebens (Würgehandlung, Schussverletzung oder Bedrohung mit durchgeladener und entsicherter Schusswaffe etc.).

14 Tierschutzverordnung des Bundes vom 23. April 2008 (TschV; SR 455.1)
15 Bundesgesetz vom 19. Juni 1992 über die Militärversicherung (MVG; SR 833.1)
16 Gesetz über den Kindes- und Erwachsenenschutz vom 1. Februar 2012 (KESG; BGS 213.316)
17 Gesundheitsgesetz vom 2. Dezember 1984 (GesG; BSG 811.01)

- Die Verletzung oder Lebensgefährdung kann vorsätzlich oder fahrlässig, bei einem Raufhandel, Angriff oder Unfall oder Ähnlichem entstanden sein. Ein Melderecht besteht auch bei einem Verdacht auf Unterlassung der Nothilfe.

Verdacht auf eine strafbare Handlung gegen die sexuelle Integrität
Vergewaltigung, sexuelle Nötigung, sexuelle Handlung in Ausnützung einer Notlage oder eines Abhängigkeitsverhältnisses (Erziehungs-, Betreuungs- oder Arbeitsverhältnis oder andere Abhängigkeit wie Anstaltsinsassen, Gefangene, Verhaftete etc.), sexuelle Handlung mit einem Kind unter 16 Jahren, Schändung (Ausnützung der fehlenden Widerstands- oder Entscheidungs-fähigkeit) oder Förderung der Prostitution etc.

Verdacht auf ein Verbrechen oder Vergehen gegen die öffentliche Gesundheit
Verbreitung von übertragbaren menschlichen Krankheiten oder Tierseuchen oder die Verunreinigung von Trinkwasser etc.

[2] **Melderecht:** Der Arzt oder die Gesundheitsfachperson darf ohne Entbindung von der Schweigepflicht den Strafverfolgungsbehörden (Staatsanwaltschaft oder Polizei, schriftlich oder telefonisch) Wahrnehmungen melden, die auf ein Verbrechen oder Vergehen gegen Leib und Leben, die öffentliche Gesundheit oder die sexuelle Integrität schliessen lassen.

3.2 Gemeingefährlichkeit (Art. 28 Abs. 3 Gesundheitsgesetz)

[1] Gesundheitsfachpersonen dürfen den zuständigen Behörden Wahrnehmen melden, die bei einer im Rahmen des Straf- und Massnahmenvollzugs oder des Vollzugs der fürsorgerischen Unterbringung behandelten Person auf Gemeingefährlichkeit oder bei erkannter Gemeingefährlichkeit auf deren Veränderung schliessen lassen. Unter Gemeingefährlichkeit fällen z. B. Drohungen gegen Leib und Leben, bevorstehende Gewaltanwendungen, Vorbereitung eines Brandes oder einer Geiselnahme.

3.3 Kindeswohlgefährdung (Art. 314c Abs. 2 Zivilgesetzbuch)[18]

[1] Der behandelnde Arzt darf der Kindesschutzbehörde (KESB) Meldung erstatten, wenn die körperliche, psychische oder sexuelle Integrität eines Kindes (bis 18 Jahre) gefährdet erscheint und die Meldung im Interesse des Kindes liegt. Dieses Melderecht besteht nur für den behandelnden Arzt. Das übrige Spitalpersonal muss sich vor einer Gefährdungsmeldung durch das Kantonsarztamt von der Schweigepflicht entbinden lassen.

[2] Mögliche Formen einer Kindeswohlgefährdung:
- *Körperliche Gewalt:* Alle Handlungen, die dem Kind Schmerzen zufügen, wie Schlagen, Schütteln, Treten, an den Haaren ziehen, Verbrennen, Ohrfeigen, Klaps auf den Po, Zwicken.
- *Physische Gewalt:* zum Beispiel Ablehnung, Abwertung, Drohung, Beschimpfung, Demütigung, Verachtung, Isolation, mutwilliges Angstmachen, aber auch Erleben von Partnerschaftsgewalt (häuslicher Gewalt) und Instrumentalisierung des Kindes in Elternkonflikten.
- *Vernachlässigung:* Kindliche Bedürfnisse werden nicht oder nur ungenügend erfüllt, wie z. B. Ernährung, Pflege, Aufsicht aber auch emotionale Vernachlässigung.
- *Sexuelle Gewalt:* jede sexuelle Handlung, mit oder ohne Körperkontakt, die eine Person unter Ausnützung eines Machverhältnisses an einer anderen Person vornimmt.

[3] **Melderecht:** Der behandelnde Arzt darf ohne Entbindung von der Schweigepflicht der Kindes- und Erwachsenenschutzbehörde (KESB) eine Gefährdungsmeldung einreichen. Die Meldung muss dem Schutz und Wohl des Kindes / Jugendlichen dienen.

[4] Eine Meldung an die Staatsanwaltschaft oder Polizei ist nur zulässig, wenn es sich um ein Verbrechen oder Vergehen gegen Leib und Leben, die öffentliche Gesundheit oder die sexuelle Integrität handelt (vgl. Ziffer 3.1).

18 (ZGB; SR 210)

3.4 Selbst- und Fremdgefährdung hilfsbedürftiger Personen (Art. 453 Zivilgesetzbuch)

[1] Besteht die ernsthafte Gefahr, dass eine hilfsbedürftige Person sich selbst gefährdet oder ein Verbrechen oder Vergehen begeht, mit dem sie jemanden körperlich, seelisch oder materiell schwer schädigt, kann der behandelnde Arzt ohne Entbindung von der Schweigepflicht der KESB Meldung erstatten. Eine akute Notsituation liegt beispielsweise vor, bei Suizidalität, schweren Selbstverletzungen oder massiver Verwahrlosung. Eine ernsthafte Gefahr kann auch beispielsweise bei einer geistig behinderten Person bestehen, die von ihrem Umfeld wahrscheinlich schwerer Gewalt oder Missbrauch ausgesetzt ist.

[2] Handelt es sich nicht um eine akute Notsituation, muss sich der behandelnde Arzt entweder von dem Patienten oder durch den Kantonsärztlichen Dienst von der ärztlichen Schweigepflicht entbinden lassen, bevor er die Gefährdungsmeldung einreicht (Art. 443 ZGB). Beispielsweise bei einer dauerhaften Verwahrlosungssituation, wen die Post nicht geöffnet wird, bei drohenden Vermögensverlusten oder wenn eine notwendige Spitexbetreuung abgelehnt wird.

3.5 Betäubungsmittelmissbrauch (Art. 3c Abs. 1 Betäubungsmittelgesetz[19])

[1] Gesundheitsfachpersonen können Fälle von vorliegenden oder drohenden suchtbedingten Störungen, namentlich bei Kindern und Jugendlichen, der Kindes- und Erwachsenenschutzbehörde melden, wenn eine erhebliche Gefährdung der Betroffenen, ihrer Angehörigen oder der Allgemeinheit vorliegt und sie eine Betreuungsmassnahme als angezeigt erachten. Bei Minderjährigen muss immer auch der gesetzliche Vertreter informiert werden, sofern nicht wichtige Gründe dagegen sprechen.

[2] **Melderecht:** Die Gesundheitsfachpersonen dürfen ohne Entbindung von der Schweigepflicht der Kindes- und Erwachsenenschutzbehörde Fälle von Betäubungsmittelmissbrauch, insbesondere durch Kinder und Jugendliche, melden. Es besteht kein Melderecht an die Staatsanwaltschaft oder Polizei.

3.6 Hinweise auf Waffenmissbrauch (Art. 30b Waffengesetz[20], Kantonale Waffenverordnung[21])

[1] Der behandelnde Arzt[22] ist berechtigt, den Strafverfolgungsbehörden Personen zu melden, bei denen ein erhöhtes Risiko besteht, dass sie Waffen zur Gefährdung oder Drohung von sich selbst oder Dritten verwenden könnten. Eine Körperverletzung ist nicht Voraussetzung für eine Meldung, sondern es genügt die abstrakte Gefährdung einer Drittperson oder wenn die Person die Waffengewalt gegen sich selber richtet.

[2] Als Waffen gelten alle Arten von Feuerwaffen, Messer, Dolche, Wurfsterne, Elektroschockgeräte etc.

[3] Eine Gefährdungsmeldung ist beispielsweise möglich, wenn

- aufgrund des körperlichen oder geistigen Zustandes, allenfalls verbunden mit einer aktuellen Krisensituation, ein erhöhtes Risiko besteht, dass die betroffene Person Waffen zur Gefährdung oder Drohung verwendet hat oder verwenden könnte.
- im Rahmen von häuslicher Gewalt Waffen zur Gefährdung, Verletzung oder Einschüchterung und Drohung von Angehörigen verwendet werden.

[4] **Melderecht:** Der behandelnde Arzt darf ohne Entbindung von der Schweigepflicht den Strafverfolgungsbehörden (Staatsanwaltschaft oder Polizei, schriftlich oder telefonisch) Fälle von Waffenmissbrauch melden.

19 Bundesgesetz über die Betäubungsmittel und die psychotropen Stoffe vom 3. Oktober 1951 (BetmG; SR 812.121)
20 Bundesgesetz über Waffen, Waffenzubehör und Munition vom 20. Juni 1997 (WG; SR 514.54)
21 Verordnung über den Vollzug des eidgenössischen Waffenrechts vom 15. Dezember 2004 (BSG 943.511.1)
22 In Absprache mit dem behandelnden Arzt kann die Meldung ausnahmsweise auch durch andere Spitalmitarbeitende erfolgen.

3.7 Mangelnde Fahreignung (Art. 15d Abs. 3 Strassenverkehrsgesetz[23])

[1] Jeder Arzt kann Personen, die wegen körperlicher oder geistiger Krankheiten oder Gebrechen oder wegen Süchten zur sicheren Führung von Motorfahrzeugen nicht fähig sind, der Aufsichtsbehörde (im Kanton Bern dem Kantonsarztamt) und der für die Erteilung des Führerausweises zuständigen Behörde (im Kanton Bern dem Strassenverkehrsamt) melden.

[2] Fahreignung bedeutet, dass eine Person aufgrund ihrer psychischen und physischen Grundkonstellation grundsätzlich in der Lage sein sollte, ein Fahrzeug sicher zu führen. Die Fahreignung kann z. B. wegen einer Demenz, einer Suchterkrankung (z. B. Alkoholismus), einer psychischen Erkrankung, einer Anfallkrankheit, eines schlecht eingestellten Diabetes mellitus etc. abgesprochen werden.

[3] **Melderecht:** Der Arzt darf ohne Entbindung von der Schweigepflicht dem kantonalen Strassenverkehrsamt Personen mit mangelnder Fahreignung melden.

4 WEITERE MELDEPFLICHTEN UND MELDERECHTE

Auf kantonaler wie auf Bundesebene bestehen verschiedene weitere gesetzliche Meldepflichten und Melderechte (Bsp. Transplantationsgesetz, Chemikaliengesetz, Bundesstatistikgesetz, Meldepflicht zu Handen des Zivilstandsregisters und andere Register).

23 Strassenverkehrsgesetz vom 19. Dezember 1958 (SVG; SR 741.0)