1.1.060.4.01 Bearbeitungsreglement für die Datensammlung nach KVG

1. Inhaltsverzeichnis

2. Abkürzungen

AHV	Alters- und Hinterlassenenversicherung
ATSG	Bundesgesetz vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (SR 830.1)
BAG	Bundesamt für Gesundheit
BBTI	Versicherungssoftware BBT*Individual*
DRG	Diagnosis Related Groups (diagnosebezogene Fallgruppen)
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz (SR 235.1)
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
KKLH	Krankenkasse Luzerner Hinterland
KPMG	Wirtschaftsprüfungs- und Beratungsgesellschaft, auditiert das DSMS der KKLH
KVG	Bundesgesetz vom 18. März 1994 über die Krankenversicherung (SR 832.10)
KVV	Verordnung vom 27. Juni 1995 über die Krankenversicherung (SR 832.102)
MCD	Minimal Clinical Dataset
QM	Qualitätsmanagement (Handbuch)
SQL-Server	relationales Datenbanksystem, dessen Daten über die Abfragesprache SQL abgefragt und manipuliert werden können
SQS	Schweizerische Vereinigung für Qualitäts- und Managementsysteme, auditiert das QM der KKLH
VAD	Vertrauensärztlicher Dienst
VDSG	Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (SR 235.11)
zDAS	(zentrale) Datenannahmestelle

3. Ausgangslage

3.1 Rechtliche Grundlagen

Gestützt auf Art. 21 der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) und in Verbindung mit Art. 84 des Bundesgesetzes über die Krankenversicherung (KVG) hat die Krankenkasse Luzerner Hinterland (in diesem Dokument KKLH genannt) für die automatisierte Datensammlung, die besonders schützenswerte Daten oder Persönlichkeitsprofile beinhaltet, das vorliegende Bearbeitungsreglement erstellt.

3.2 Ziel des Bearbeitungsreglements

Das Bearbeitungsreglement umschreibt insbesondere die Datenbearbeitungs- und Kontrollverfahren sowie den Betrieb der Datenbearbeitung. Es enthält Angaben über das für den Datenschutz und die Datensicherheit verantwortliche Organ, die Herkunft der Daten, die Zwecke, für welche sie regelmässig bekannt gegeben werden und beschreibt das Verfahren für die Erteilung der Zugriffsberechtigung auf die Module der elektronischen Informatiksysteme.
Das vorliegende Reglement wird laufend den gesetzlichen, organisatorischen und betrieblichen Änderungen angepasst.

3.3 Zweck der Datenbearbeitung

Der Zweck der Datensammlung ist im Bundesgesetz über die Krankenversicherung (KVG) geregelt. Der Krankenversicherer ist verantwortlich für die Abwicklung der Krankenversicherung nach KVG.

Artikel 84 KVG bestimmt, dass die mit der Durchführung, der Kontrolle oder der Beaufsichtigung der Durchführung des Gesetzes betrauten Organe befugt sind, die Personendaten, einschliesslich besonders schützenswerte Daten und Persönlichkeitsprofile, zu bearbeiten, die sie benötigen, um die ihnen nach dem Gesetz übertragenen Aufgaben zu erfüllen.
Die kassenpflichtigen Leistungen müssen gemäss Art. 32 KVG wirksam, zweckmässig und wirtschaftlich sein und sich insbesondere auf das Mass beschränken, welches für den Behandlungszweck erforderlich ist. Der Versicherer ist nach Art. 56 KVG berechtigt und verpflichtet, die Wirtschaftlichkeit der Leistungen zu überprüfen.

3.4 Verantwortliche Stelle

Die KKLH ist verantwortlich für die Abwicklung der sozialen Krankenversicherung und somit Inhaberin der damit verbundenen Datensammlungen.

Gestützt auf Art. 59a KKV dürfen MCD-Files, die für die Beurteilung der stationären DRG-Rechnungen erforderlich sind, nur an eine zertifizierte Datenannahmestelle gesandt werden. Mit der Ernennung einer externen Datenannahmestelle wurde die MCD-Bearbeitung an die zertifizierte Datenannahmestelle der BBT Software AG ausgelagert. Aufgrund dessen gelten zusätzlich zu den vorliegenden Richtlinien der KKLH die Richtlinien gemäss Bearbeitungsreglement zDAS der BBT Software AG (1.1.062.4.01).

3.5 Schweigepflicht

Sämtliche Mitarbeiter der KKLH unterstehen der Schweigepflicht nach Art. 33 ATSG. Bei Verletzung der Schweigepflicht unterstehen sie spezialgesetzlich den Strafbestimmungen von Art. 92 KVG. Die Mitarbeitenden sind über die Sanktionen informiert.
Alle Mitarbeitenden müssen eine Geheimhaltungs- und Schweigepflichtvereinbarung unterzeichnen, zu deren Einhaltung sie sich sowohl für die Zeit während ihrer Anstellung, als auch nach Beendigung des Arbeitsverhältnisses verpflichten.

4. Struktur / Abgrenzung

4.1 Struktur des Infosystems

Die Hauptstruktur der KKLH besteht aus der Verwaltungssoftware BBTI der Firma BBT Software AG, Zermatt sowie diversen Umsystemen.

4.1.1 BBTI
Das BBTI wird ständig weiterentwickelt und den aktuellen Erfordernissen angepasst, so ist zum Beispiel das elektronische Einscannen von Arzt- und Spitalrechnungen sowie von weiteren Dokumenten aktuell ein Thema. Vor der Einführung des Programmes BBTI am 01.01.2014 benutzten wir als Hauptsoftware Valsana 5.5, ebenfalls von der BBT Software AG. Dieses dient uns aktuell nur noch als Archiv.

4.1.2 Zentrale Datenannahmestelle (zDAS)
Gestützt auf Art. 59a KVV müssen sämtliche Krankenversicherer über eine zentrale Datenannahmestelle für die MCD-Bearbeitung verfügen. Die KKLH hat die BBT Software AG als zertifizierte Datenannahmestelle verpflichtet. Die MCDs werden ausschliesslich an die zDAS gesandt. Die zDAS gewährt zur Rechnungsprüfung mittels eines Links Zugriff auf auffällige MCDs. Über die User-Berechtigung im BBTI Software Programm ist gewährleistet, dass nur die berechtigten DRG-Mitarbeiter sowie die VAD-Mitarbeiter Zugriff auf diesen Link erhalten.

4.1.3 Medikamentenprogramm SwissCDA
Um die Leistungspflicht von Medikamenten abklären zu können, wird mit dem Medikamentenprogramm SwissCDA gearbeitet. Dieses Programm wird regelmässig mit neuen Updates versehen, die Zugehörigkeit zu einer Medikamentengruppe ist eindeutig gekennzeichnet. Preisentwicklungen und Veränderungen können anhand von Reports aufgezeigt und ausgedruckt werden.

4.1.4 Vertragsdatenbank
Um die zum Teil komplexen Rechnungen korrekt abrechnen zu können, steht uns die Vertragsdatenbank ZVR der Santésuisse zur Verfügung. Sämtliche Verträge, Tarife, Taxen und Diagnosecodes können abgefragt werden.

4.1.5 Intranet
Eine interne Informationsquelle ist das Intranet. Dort werden Links, Hinweise und Internetadressen zu den verschiedensten Arbeitsgebieten gespeichert und verwaltet. Dieses Arbeitsmittel ist sehr interessant und deckt ein grosses Spektrum an Fachfragen ab. Die regelmässige Aktualisierung ist sehr wichtig, nur so kann auch ein stetes Interesse an diesem neuen Arbeitsinstrument erhalten und gefördert werden.

4.2 Schnittstellen
Der Anhang A zeigt die Datenverarbeitung mit externen Stellen in tabellarischer Form. Nach Wunsch kann dieser im Hauptsitz der KKLH in Zell eingesehen werden.

4.3 Interne Organisation
Die Gesamtverantwortung für den Datenschutz trägt das Leitungsorgan, also der Vorstand und der Geschäftsführer. Diese Verantwortung ist nicht übertragbar. Für die Umsetzung des Datenschutzes im Betrieb ist die Geschäftsleitung verantwortlich.

Jeder Mitarbeiter hat Zugriff auf die Haupt- und Umsysteme der KKLH, der Zugriff ist aber so eingeschränkt, dass jeder Mitarbeiter nur diejenigen Berechtigungen erhält, die er für seine tägliche Arbeit braucht.
Die Informatikabteilung bzw. der IT-Verantwortliche ist für das reibungslose Funktionieren der Haupt- und Umsysteme zuständig und hat dementsprechend auch bei allen Systemen Administratorrechte. Zusätzlich ist er verantwortlich für den Datenschutz in IT-relevanten Themen wie das Betriebssystem, Anwendungen, die Datenbank, das Netzwerk und die Datensicherheit.
Die Abteilung Mitgliedschaft ist für den Kundendienst sowie für die Vertragsverwaltung der Versicherten (Ein- und Austritte, Vertragsmutationen, etc.) zuständig. Für diese Aufgabe bearbeiten sie Daten im BBTI und den Umsystemen.
Die Leistungsabteilung kontrolliert, verarbeitet und erstattet eingehende ambulante Rechnungen des KVG sowie Zusatzleistungen. Alle ambulanten und stationären Spitalrechnungen werden von der Spitalabteilung verarbeitet und geprüft. Elektronisch eingehende stationäre Rechnungen werden von den DRG-Hilfspersonen verarbeitet. Direkt an den VAD übermittelte Rechnungen und Informationen werden im VAD durch die Vertrauensärzte und/oder die Hilfspersonen des VAD überprüft und zuhanden der Leistungsabteilung zur Zahlung freigegeben. Die medizinischen Informationen verbleiben im VAD.

Gestützt auf Art. 59a KVV hat die Krankenkasse Luzerner Hinterland für die MCD-Bearbeitung die BBT Software AG als zertifizierte Datenannahmestelle ernannt. In Bezug auf die damit verbundenen Prozesse und Handlungen gelten

die Bestimmungen gemäss Bearbeitungsreglement zDAS der BBT Software AG (1.1.062.4.01). Die Bearbeitung von Papier-MCDs obliegt ebenfalls der BBT. Sollten einmal MCDs in Papierform bei uns eingehen (bisher nicht eingetreten), würden diese mit Bitte um Zustellung an unsere DAS an den Leistungserbringer zurückgesendet.

Der betriebliche Datenschutzverantwortliche kontrolliert die Einhaltung des Datenschutzes, berät die Geschäftsleitung und die Mitarbeitenden und unterstützt bei der operativen Umsetzung des Datenschutzes im Betrieb.

4.4 Dateninhaber, Datenowner, Verwaltung der Datensammlungen

Die KKLH ist Inhaberin und somit verantwortlich für ihre Datensammlung. Gleichzeitig gilt aufgrund der engen Abhängigkeit zur BBT Software AG auch das Bearbeitungsreglement der BBT (1.1.062.4.01).

4.5 Applikation

Die Applikationsowner/Prozessverantwortlichen für das EDV-System der KKLH, resp. für die Umsysteme sorgen für die Datensicherheit und den Datenschutz im Allgemeinen sowie die Einhaltung von Bestimmungen, Weisungen und Reglementen zur Datenbearbeitung im Besonderen. Folgende Regelungen sind festgeschrieben:

- Zugriffskontrolle (Zugriffsrechte, -überwachung, -verwaltung) der Mitarbeitenden auf die Informatiksysteme bzw. Versichertendaten
- Datensicherung (Back-up, Archivierung)
- Netzwerksicherheit (vertrauenswürdige Netze, Verschlüsselung, Passwortschutz, Anschluss von Fremdunternehmen, Internetzugang).

5. Benutzer und Datenzugriff

5.1 Benutzer

Zugriffsberechtigt auf das EDV-System der KKLH und die Umsysteme sind:

- Mitarbeitende der KKLH, soweit sie dies zur Ausübung ihrer Aufgaben, der Durchführung der Kranken- und Unfallversicherung nach KVG, benötigen
- Systemadministratoren
- Mitarbeitende von externen Dienstleistungsunternehmen nach Erteilung des Zugriffsrechts

Zusatzberechtigungen DRG haben:

- DRG-Hilfspersonen
- VAD (Vertrauensärzte und deren Hilfspersonen)
- Systemadministratoren

5.2 Benutzerverwaltung

Zuständig für die Benutzerverwaltung ist die Informatik-Abteilung der KKLH. Jeder Mitarbeiter arbeitet auf einer eigenen, passwortgeschützten Benutzeroberfläche. Die Zugriffsberechtigungen (für das BBTI sowie andere Programme und Ordner) sind mit dem Benutzer gekoppelt. Die Benutzerverwaltung ist rollenbasiert organisiert, jedem Mitarbeiter wird eine Rolle mit bestimmten dazugehörigen Rechten zugewiesen.

5.3 Prozess Zugriffsberechtigungen

Es werden nur die notwendigsten Zugriffsrechte auf Netzwerke, Programme und Daten an Benutzer vergeben. Jeder Mitarbeitende erhält nur Zugriff auf diejenigen Daten, die er zur Erfüllung seiner Aufgabe braucht.
Der IT-Verantwortliche entscheidet gemäss den festgeschriebenen Regeln in den Weisungen und in Zusammenarbeit mit den Applikationsownern/Prozessverantwortlichen über die Vergabe und den Umfang der Zugriffsrechte. Die Zugriffrechte sind auf die Funktion und Tätigkeitsfelder jeder Person zugeschnitten. Zudem wird für jede Berechtigung entschieden, ob eine Leseberechtigung genügt, oder ob Änderungsberechtigungen vergeben werden müssen.
Die Zugriffsrechte sind im Detail in den Dokumenten „7.3.022.4.01 Zugangsberechtigungen“ sowie „1.1.064.5.01 Laufblatt Berechtigungen“ festgehalten. Zudem hat jeder Mitarbeitende eine persönliche Identifikation (Benutzername) und ein Passwort. Die Weitergabe des persönlichen Passworts ist untersagt. Weisungen bezüglich der Zusammensetzung der Passwörter (Anzahl Stellen, Sonderzeichen etc.) liegen schriftlich in den Informatik-Benutzerrichtlinien (7.3.042.4.01) vor und sind allen Mitarbeitenden bekannt.

5.4 Ausbildung der Benutzer

Die Benutzer werden betriebsintern für die verschiedenen Applikationen und Umsysteme geschult.

6. Bearbeitung der Daten

6.1 Datenbeschaffung

Die Daten stammen einerseits direkt von Leistungserbringern gemäss Art. 42 Abs. 2 KVG sowie andererseits von den Versicherten selbst oder den von ihnen ermächtigten Personen und Stellen (Versicherungen, Amtsstellen usw.). Es können gemäss Art. 32 ATSG auch Daten im Rahmen der Amts- und Verwaltungshilfe erhoben werden.

6.2 Datenkategorien

Im Anhang B sind die Datenkategorien der Datensammlung des EDV-Systems der KKLH aufgeführt und klassifiziert.

6.3 Datenweitergabe

Datenweitergabe nach Art. 84a KVG in Verbindung mit Art. 84 KVG.

Daten werden bekannt gegeben für:

- die Sicherstellung der Einhaltung der Versicherungspflicht (Art. 7 Abs. 5 KVG)
- die Abwicklung der Prämienverbilligung
- die Beurteilung von Leistungsansprüchen
- die Zuweisung und Verifikation der Versichertennummer an die AHV
- die Erstellung der Versichertenkarte und den online-Abfragedienst
- die Abwicklung der sozialen Krankenversicherung im Bereich Managed Care
- die Koordination mit Leistungen anderer Sozialversicherer (z.B. Art. 27 KVG)
- die Geltendmachung von Rückgriffrechten gegenüber haftpflichtigen Dritten
- Sicherstellung der Notfallzentrale (Assistance-Leistungen im Ausland)
- die Führung von Statistiken

Datenempfänger sind:

- Versicherte und von ihnen bevollmächtigte Dritte
- Leistungserbringer (Online-Versichertenkartenabfrage, Managed Care)
- Behörden (Prämienverbilligungsstellen der Kantone, BAG, IV-Stellen usw.)
- Sozialdienste
- Verbandsdienstleister der Krankenversicherer (RVK, BBT Software AG, Datenpool)
- Rechtsdienst
- Vertrauensärzte

6.4 Datenbearbeitung

6.4.1 Nach Art. 42 KVG

Die Datenbearbeitung für die Kontrolle von ambulanten und stationären Behandlungsrechnungen erfolgt auf der Grundlage von Art. 42 KVG. Diagnosedaten und zusätzliche medizinische Auskünfte, die aufgrund von Art. 42 Abs. 4 KVG verlangt werden, dürfen ausschliesslich im Rahmen der Rechnungskontrolle und zum durch in Art. 56 KVG vorgesehenen Recht zur Prüfung der Wirtschaftlichkeit bearbeitet werden.
Stationäre Behandlungen werden gemäss Art. 49 KVG mit leistungs- und diagnosebezogenen Fallpauschalen in Rechnung gestellt (SwissDRG). Die Leistungserbringer haben dem Versicherer, resp. einer zertifizierten Datenannahmestelle, zusammen mit der Rechnung Angaben über Haupt- und Nebendiagnosen, Behandlungen und Prozeduren mitzuteilen. Diese Informationen sind im sogenannten MCD enthalten (Minimal Clinical Dataset, auch Medizinischer Datensatz genannt). MCDs sind streng vertrauliche Daten und dürfen nur von den DRG- sowie den VAD-Hilfspersonen eingesehen werden. Gemäss Art. 59a KVV dürfen MCD-Files ausschliesslich an zertifizierte Datenannahmestellen übermittelt werden.

Die gesamtschweizerisch einheitliche Struktur des oben erwähnten Medizinischen Datensatzes und jene des Administrativen Datensatzes sind in der Verordnung des EDI über die Datensätze für die Datenweitergabe zwischen Leistungserbringern und Versicherern vom 20. November 2012 geregelt.

6.4.2 Grundsätze der Datenbearbeitung

Die Bearbeitung der Personendaten richtet sich nach den folgenden datenschutzrechtlichen Richtlinien:

Rechtmässigkeit
Die Bearbeitung der Personendaten erfolgt auf der Grundlage von KVG Artikel 84 und VVG Artikel 59a.

Treu und Glauben
Die Bearbeitung der Personendaten erfolgt nach Treu und Glauben.

Zweckmässigkeit
Die KKLH bearbeitet Personendaten ausschliesslich zum Zweck der Erfüllung der ihr durch das Gesetz übertragenen Aufgaben zur Durchführung der sozialen Krankenversicherung.

Verhältnismässigkeit
Es werden nur diejenigen Personendaten bearbeitet, die zur Erfüllung des gesetzlichen Auftrages gemäss Art. 84 KVG notwendig sind.

Erkennbarkeit
Gestützt auf Art. 84 KVG werden diese Daten für die Erfüllung nachfolgender Aufgaben benötigt:

- Beurteilung des Leistungsanspruches
- Berechnung der Leistung
- Gewährung der Leistung
- Koordination mit Leistungen anderer Sozialversicherer
- Überprüfung der Einhaltung der Versicherungspflicht
- Berechnung der Prämien
- Beurteilung des Anspruches auf Prämienverbilligung
- Ausübung der Aufsicht über die Durchführung dieses Gesetzes
- Erstellung von Statistiken
- Zuweisung und Verifizierung der Versichertennummer der AHV
- Berechnung des Risikoausgleiches

Informationssicherheit
Alle Personendaten werden durch angemessene technische und organisatorische Massnahmen gegen Verlust und unbefugtes Bearbeiten geschützt.

Grenzüberschreitende Bekanntgabe von Daten
Die KKLH hält bei der Datenbekanntgabe die gesetzlichen Regelungen von Artikel 6 DSG sowie der Artikel 5 und 7 VDSG ein.

6.5 Weitere Datenweitergabe

Die weitere Datenbekanntgabe ist abschliessend in Art. 84a KVG geregelt. So können im Einzelfall und auf schriftlich begründetes Gesuch hin Daten gemäss den spezifischen Anforderungen an Sozialhilfebehörden, Zivilgerichte, Strafgerichte und Strafuntersuchungsbehörden, Betreibungsämter, sowie mit schriftlicher Bewilligung an Dritte weitergegeben werden.

7. Archivierung und Vernichtung

Archivierungspflichtige Dokumente werden während der gesetzlich verlangten Dauer archiviert und vor Veränderungen oder unbefugten Zugriffen geschützt. Die Zutritte zum Archiv werden sehr restriktiv vergeben. Nach Ablauf der

gesetzlichen Archivierungsfrist werden die Dokumente vernichtet, da die rechtliche Grundlage (Zweckmässigkeit) wegfällt.

Die KKLH sorgt bei der Aufbewahrung und der Entsorgung dafür, dass unberechtigte Dritte keinerlei Zugang, Zugriff oder Einsicht in Personendaten von versicherten Personen haben.
Dies bedeutet insbesondere:

- Die KKLH sichert Räumlichkeiten, in denen Personendaten aufbewahrt werden, gegen unbefugten Zutritt oder bewahrt Personendaten unter Verschluss auf.
- Die KKLH achtet bei der Entsorgung von Papier darauf, dass besonders schützenswerte Personendaten weder dem gewöhnlichen Kehricht noch der Papiersammlung zugeführt werden. Diese Papiere werden entweder geschreddert oder unter Aufsicht des Versicherers vernichtet.
- Die KKLH beachtet bei der Entsorgung von elektronischen Datenträgern, dass sämtliche Informationen dauerhaft unlesbar gemacht werden.

Die Aufbewahrungsdauer für jede Datensammlung ist aus dem Dokument „1.1.060.4.03 Datensammlungen“ und dem darin integrierten Konformitätsnachweis ersichtlich (siehe auch Anhang C).

Bezüglich Archivierung und Vernichtung von MCD-Daten gelten die Bestimmungen gemäss dem Bearbeitungsreglement über die zDAS der BBT Software AG (1.1.062.4.01)

8. Technische und organisatorische Massnahmen nach Art. 9 VDSG

8.1 Zugangskontrolle

Der Hauptsitz der KKLH in Zell ist mit modernen Schliesssystemen manuell vor dem Zugang unbefugter Personen geschützt. Fenster und Türen werden abends und an den Wochenenden verschlossen.
Im Schalterraum im UG ist der Bürobereich zusätzlich durch eine Beratungstheke abgetrennt. Die Bildschirme, welche vom Schalter her eingesehen werden könnten, sind mit einer Verdunkelungsfolie abgedeckt. Zusätzlich beachten die Mitarbeiter am Schalter strikt die Clean Desk Policy.
Die VAD- und DRG-Büros, wo die MCDs eingesehen werden, sind zusätzlich gesichert. Während des Tages bleibt die Tür immer geschlossen. Zusätzlich wird die Tür mit Schlüssel abgeschlossen, wenn niemand im Büro ist. Einen Schlüssel dazu haben nur die DRG- und VAD-Hilfspersonen sowie der Geschäftsführer. Die Aktenschränke mit besonders schützenswerten Daten werden zusätzlich abgeschlossen.
Im Allgemeinen bewegen sich Besucher nie frei in den Räumlichkeiten der KKLH, sondern werden immer von jemandem begleitet. Für weitere Informationen siehe auch „1.1.061.3.01 Datenschutzleitbild“.

8.2 Personen- und Datenträgerkontrolle

Der Zugriff auf die zu bearbeitenden Daten erfolgt ausschliesslich remote. Alle Daten befinden sich im Rechenzentrum beim Hauptsitz in Zell. Zutritt haben nur die Mitarbeitenden der Informatik-Abteilung sowie der Geschäftsführer. Zweimal wöchentlich wird eine Datensicherung auf einer externen Festplatte von unserem IT-Verantwortlichen in ein Schliessfach auf der Bank gebracht. Ansonsten verlassen keine Datenträger mit Personendaten den Geschäftssitz der KKLH.
Der Zugriff auf die DRG- und VAD-relevanten Daten ist stark eingeschränkt. Nur die DRG- sowie die VAD-Hilfspersonen haben Zugriff auf die elektronischen Rechnungen und die auffälligen MCDs. Sind diese mit „vertraulich“ markiert, hat nur die VAD-Hilfsperson Zugriff darauf. Ausschliesslich die VAD-Hilfsperson kann auf die vertrauensärztlichen Entscheide auf dem Casenet des RVK zugreifen.

8.3 Authentifizierung und Benutzerkontrolle

Durch sicherheitstechnische Vorkehrungen ist es ausschliesslich berechtigten Personen möglich, Daten abzufragen oder zu bearbeiten. Nur berechtigte Personen erhalten Zugriff auf das Informationssystem der KKLH. Zugriff erhält man nur mit einer gültigen User-ID sowie dem korrekten Passwort. Einige der Umsysteme der KKLH verlangen einen zusätzlichen, vom Benutzer abweichenden Benutzernamen und Passwort.

8.4 Bekanntgabekontrolle

Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, werden über die Schnittstellen identifiziert. Die Übermittlung von Personendaten findet immer über einen verschlüsselten Kanal statt.

8.5 Chiffrierung

Die Daten der KKLH werden nicht chiffriert. Die MCDs befinden sich ausschliesslich in der zentralen Datenannahmestelle der BBT Software. Sie sind pseudonomisiert und werten als DataBlob gespeichert. Da in die zentrale Datenannahmestelle keine DRG-Rechnungen fliessen, ist die Pseudonomisierung gemäss den Vorgaben des Forums „Datenaustausch“ gewährleistet.

8.6 Speicherkontrolle

Durch die Zugangskontrolle sowie durch die Authentifizierung ist gewährleistet, dass Unbefugte weder auf den Speicher zugreifen und Änderungen vornehmen können, noch Einsicht in die Daten erhält.

8.7 Home Office

Home-Office wird bei der KKLH nur ganz beschränkt bewilligt. Genaue Informationen dazu sind in „1.1.061.3.01 Datenschutzleitbild“ zu finden.

8.8 Protokollierung

Die Hauptsoftware der KKLH, das BBTI, verfügt über eine Eingabekontrolle. Es kann also über das Protokoll rückverfolgt werden, welche Personendaten von wem und zu welcher Zeit eingegeben wurden. Die Zugriffe werden gemäss Art. 10 VDSG durchgeführt (siehe auch 10.4).

8.9 Programmentwicklung

In der KKLH werden keine Entwicklung von Programmen und auch keine Tests und Produktionen gemacht. Programme entwickelt, testet und produziert die BBT Software AG für uns, wir sind die Programmbezüger (z.B. des BBTI). Dementsprechend gelten auch die Bestimmungen des Bearbeitungsreglements der BBT Software AG (1.1.062.4.01) mit. Im Rahmen von Maintenance, Unterhalt, Wartung und Parametrierung dürfen nur definierte Aktionen vorgenommen werden.

8.10 Backup / Restore

Der IT-Verantwortliche führt eine tägliche Sicherungskopie der BBTI-Daten durch. Zusätzlich werden die Daten der Buchhaltung und des BBTI zweimal wöchentlich auf eine externe Festplatte gebrannt. Näheres dazu im Dokument „7.3.020.4.01 Datensicherung“.

8.11 Schulung

Alle Mitarbeiter der KKLH werden in regelmässigen Abständen bezüglich dem Umgang mit schützenswerten und besonders schützenswerten Daten geschult und dafür sensibilisiert. Weitere Informationen sind in „1.1.061.3.01 Datenschutzleitbild“ enthalten.

9. Datensicherheit

Für die Gewährleistung der Datensicherheit, d.h. dem Schutz von Daten während der Datenverarbeitung und Speicherung oder dem Datentransport vor Verlust, Zerstörung, Verfälschung, unbefugter Kenntnisnahme und unberechtigter Verarbeitung, werden folgende Massnahmen angewendet:

9.1 Organisatorische Massnahmen

- Es bestehen Informatik-Benutzerrichtlinien. Die Einhaltung wird durch die Geschäftsleitung jährlich geprüft.
- Erstellung von Sicherheitskopien auf einem separaten Speichermedium.
- Getrennte Aufbewahrung der Sicherheitskopien.

- Alle Computer sind passwortgeschützt.
- Automatische Bildschirmsperrung nach [5] Minuten ohne Aktivität.
- Clean Desk Policy
- Alle Mitarbeitenden werden laufend zu den Themen Datenschutz und Datensicherheit geschult.
- Die Mitarbeitenden der IT bilden sich regelmässig in Security Themen weiter.

9.2 Technische Massnahmen

- Es besteht ein Back-up-Konzept.
- Eine Firewall ist eingerichtet und wird mindestens monatlich aktualisiert.
- Virenprüfung: die IT-Abteilung ist verantwortlich, dass alle Computer immer über den aktuellsten Virenschutz verfügen.
- Plattenspiegelung: Der Datenbestand einer Festplatte wird nach jeder Veränderung auf eine zweite Festplatte kopiert.
- Vertrauliche Daten werden nur per Post oder Secure E-Mail (HIN-Adresse) übermittelt.
- Das Rechenzentrum befindet sich in einem gesicherten Raum.

10. Interne und externe Kontrollen

In Ergänzung zu Kapitel 9 „Datensicherheit“ sind folgende Massnahmen Kontrollen im Unternehmen implementiert:
Die Einhaltung der datenschutzrechtlichen Bestimmungen wird **intern** folgendermassen sichergestellt und kontrolliert:

10.1 Massnahmen auf Unternehmungsebene

- Schriftlich festgehaltene Datenschutzpolitik, die allen Mitarbeitenden bekannt ist
- Datenschutz- und Datensicherheitsrichtlinien resp. -konzept
- Regelungen von Aufgaben, Verantwortlichkeiten und Kompetenzen bezüglich Datenschutz und Datensicherheit in den Pflichtenheften der Mitarbeitenden
- Thematisierung des Datenschutzes und der Datensicherheit in allen Stellenbeschreibungen und Arbeitsverträgen
- Zugänge zu den Büros sowie zum Archiv sind gesichert
- Laufende Schulung aller Mitarbeitenden bezüglich Datenschutz und Datensicherheit
- Weisungen betreffend Umgang mit E-Mail und Telefon
- Das System zeichnet die Zugriffe auf Daten, den Zeitpunkt sowie den Umfang der Zugriffe (lesen, verändern etc.) auf.

10.2 Kontrollen durch das Management

Das Leitungsorgan und die Geschäftsleitung nehmen ihre Führungs- und Überwachungsaufgaben durch folgende Kontrollen war:

- Prüfen der Bereiche der internen Kontrolle und Ableiten von Massnahmen
- Prüfung der Umsetzung der Datenschutzpolitik
- Sorgfältige Auswahl und Instruktion aller externer Dienstleister, die auf Daten zugreifen müssen oder an die Daten weitergegeben werden
- Verfassen von Datenschutz- und Datensicherheits-Vertragsklauseln mit allen Dienstleistern, die auf Daten zugreifen können oder an denen Daten weitergegeben werden sowie Kontrolle, ob die Dienstleister die Vorschriften bezüglich Datenschutz und Datensicherheit einhalten
- Periodische Prüfung der Zugriffsrechte sowie des Umfangs der Zugriffsrechte jedes Mitarbeitenden anhand der Zugriffsliste

- Auswertung der Systemaufzeichnungen bezüglich Zugriffen auf Daten, Zeitpunkt sowie Umfang der Zugriffe und Abgleich mit der Zugriffsliste

Des Weiteren lebt das Management seine Vorbildfunktion aktiv und täglich und stellt die notwendigen Mittel für die kontinuierliche Verbesserung des Datenschutzes und der Datensicherheit bereit.

10.3 Kontrollen auf Prozessebene

- Prüfung der Konformität vor Einrichtung einer Datensammlung und Dokumentation im Konformitätsnachweis (siehe „1.1.060.4.01 Datensammlungen“)
- Jährliche Kontrolle des Konformitätsnachweises (Vollständigkeit, Korrektheit, Ist die Datenbearbeitung immer noch zweckmässig? Ist der Empfänger der Daten noch korrekt? etc.).
- Jährliche Prüfung der Personendaten auf Ihre Richtigkeit (Policenversand)

10.4 IT-Kontrollen

Der Grossteil der IT-Kontrollen wurde bereits unter „Datensicherheit“ erläutert. Hier sind nur noch die ergänzenden aufgelistet.

- Protokollierung der Eingaben und Veränderungen

10.5 Interne Audits

- Jährliche Kontrolle durch den betrieblichen Datenschutzbeauftragten.
- Jährliche Kontrolle durch die interne Revision.

Diese Kontrollen sind in das umfassende interne Kontrollsystem des Unternehmens integriert. Diese Kontrollen werden durch folgende externe Audits ergänzt.

- Audits im Rahmen der SQS
- Datenschutzaudits (zentrale Datenannahmestelle und MCD-Prozess) durch die KPMG

11. Rechte der Betroffenen

11.1 Informationspflicht nach Art. 14 DSG

Art. 14 DSG verlangt die Information der betroffenen Person, wenn besonders schützenswerte Personendaten oder Persönlichkeitsprofile beschafft werden. Aufgrund des gesetzlichen Auftrages nach KVG 84 und KVV 59a zur Bearbeitung von Gesundheitsdaten gilt die Ausnahmeregelung nach Art. 14 Abs. 4 lit. a DSG, wonach die Informationspflicht des Inhabers der Datensammlung entfällt, wenn die Speicherung oder die Bekanntgabe ausdrücklich durch das Gesetz vorgesehen ist.

11.2 Auskunftsrechte nach Art. 8 und 9 DSG und Art. 1 und 2 VDSG

11.2.1 Form, Inhalt und Anschrift

Auskunftsbegehren sind schriftlich zusammen mit einer Kopie der ID oder des Passes an folgende Adresse und Kontaktperson zu senden:

Krankenkasse Luzerner Hinterland
z. H. Datenschutzbeauftragter
Luzernstr. 19
6144 Zell LU

11.2.2 Auskunftsbegehren über die Gesundheit

Daten über die Gesundheit des Gesuchstellers werden an einen vom Gesuchsteller bestimmten Arzt übermittelt, nicht an den Gesuchsteller persönlich.

11.2.3 Prozessablauf

Der interne Prozessablauf ist im Prozess „1.1.060.1.00 Auskunftsbegehren“ geregelt.

Durch die Ernennung einer externen Datenannahmestelle wurde die MCD-Bearbeitung an die Datenannahmestelle der BBT Software AG ausgelagert. Aufgrund dessen gelten zusätzlich zu den vorliegenden Richtlinien bezüglich Auskunftsbegehren der KKLH die Richtlinien gemäss Bearbeitungsreglement der BBT Software AG (1.1.062.4.01).

11.3 Recht des Versicherten nach Art. 42 Abs. 5 KVG

Auf Verlangen der versicherten Person ist der Leistungserbringer in jedem Fall verpflichtet, die medizinischen Angaben nur dem Vertrauensarzt oder der Vertrauensärztin der KKLH bekannt zu geben. Ebenso ist der Leistungserbringer in begründeten Fällen berechtigt, dieses Verfahren auch ohne Antrag der versicherten Person anzuwenden.

11.4 Berichtigungs- und Löschrechte Art. 5 Abs. 2 und Art. 25 DSG

Die Berichtigungs- und Löschrechte betroffener Personen richten sich nach Art. 5 Abs. 2 und Art. 25 DSG. Die Gesuche sind an folgende Adresse und Kontaktperson zu senden:

Krankenkasse Luzerner Hinterland
z. H. Datenschutzbeauftragter
Luzernstr. 19
6144 Zell LU

Durch die Ernennung einer externen Datenannahmestelle wurde die MCD-Bearbeitung an die Datenannahmestelle der BBT Software AG ausgelagert. Aufgrund dessen gelten zusätzlich zu den vorliegenden Richtlinien bezüglich Berichtigungs- und Löschrechte der KKLH die Richtlinien gemäss Bearbeitungsreglement der BBT Software AG (1.1.062.4.01).

12. Abschliessende Bestimmungen

12.1 Anhänge

Die im vorliegenden Bearbeitungsreglement erwähnten Anhänge sind integrierender Bestandteil dieses Bearbeitungsreglements. Es sind dies:

Anhang A: Schnittstellen
Anhang B: Datenkategorien
Anhang C: Konformitätsnachweis
Anhang D: Wichtige Bildschirmmasken

Das Bearbeitungsreglement ist online auf unserer Website für die Öffentlichkeit zugänglich und kann dort heruntergeladen werden. In die Anhänge kann ausschliesslich vor Ort in der KKLH in Zell Einsicht genommen werden.

12.2 Zuständigkeit

Das Bearbeitungsreglement wird vom betrieblichen Datenschutzverantwortlichen verwaltet.

12.3 Änderungen des Reglements

Das Bearbeitungsreglement wird gemäss Art. 11 Abs. 2 VDSG regelmässig vom Inhaber der Datensammlung aktualisiert. Dieses Reglement kann jederzeit geändert werden. Änderungen bedürfen der Zustimmung der Geschäftsleitung.

12.4 Inkrafttreten

Dieses Reglement wurde dem EDÖB im Sinne von Art. 84b KVG vorgelegt. Es ersetzt die vorangehenden Reglemente und tritt per 01.09.2015 in Kraft.

Zell, im August 2015

Krankenkasse Luzerner Hinterland
Geschäftsführer

Bruno Peter