DATENSCHUTZ - REGLEMENT UKBB

Universitäts-Kinderspital beider Basel

Inhaltsverzeichnis

1 Grundsätze und Geltungsbereich ... 3
1.1 Grundsätze ... 3
1.2 Geltungsbereich ... 4

2 Rechtliche Grundlagen und ergänzende Weisungen ... 4

3 Berufsgeheimnis ... 5
3.1 Auskunft und Herausgabe von Daten ... 5
3.2 Datenbearbeitung ... 7
3.3 Arbeitsplatz ... 7
3.4 Archivierung / Entsorgung ... 8

4 Einsatz von Informatikmitteln ... 8
4.1 Bearbeiten von schützenswerten Daten ... 8
4.2 Systemanmeldung und -abmeldung (Login und Logout) ... 8
4.3 Datenspeicherung ... 9
4.4 Datenaustausch ... 9
4.5 Organisation ... 10
4.6 Verhalten der Benutzer ... 10

5 Nutzung von Soft- und Hardware ... 11
5.1 Nutzung von Software ... 11
5.2 Nutzung von Hardware ... 12

6 Ergänzende Regelungen ... 12
6.1 Schriftliche Genehmigung für Ausnahmebewilligungen ... 12
6.2 Qualitätssicherung ... 12
6.3 Verantwortlichkeit und Meldepflicht ... 13

7 Organisation Datenschutz UKBB ... 13

8 Schlussbestimmungen ... 14

1 Grundsätze und Geltungsbereich

1.1 Grundsätze

Datenschutz ist Persönlichkeitsschutz. Gemäss

- Art. 13 Abs. 2 der Schweizerischen Bundesverfassung,
- § 11 Abs. 1 lit. j der Verfassung des Kantons Basel-Stadt vom 23.3.2005,
- Informations- und Datenschutzgesetz (IDG, SG 153.260) des Kantons Basel-Stadt vom 9. Juni 2010,

hat jede Person Anspruch auf Schutz ihrer persönlichen Daten.

Als schützenswerte Daten gelten Personendaten sowie Daten und Dokumente, an deren vertraulicher Behandlung ein erhebliches öffentliches Interesse besteht.

Aufgrund der Besonderheit der Arzt-Patienten-Beziehung und der dabei erhobenen sensitiven Gesundheitsdaten (besondere Personendaten), gelten im Bereich der Medizin noch weitere Geheimhaltungsvorschriften, wie das Arzt-/Patientengeheimnis, das im Strafgesetzbuch geregelt ist.[1]

Bei der Bearbeitung von Daten sind gemäss den gesetzlichen Vorgaben folgende Grundsätze einzuhalten:

- Rechtmässige Datenbeschaffung,
- Bearbeitung nach Treu und Glauben und der Verhältnismässigkeit,
- Bearbeitung nur zum vorgesehenen Zweck,
- Daten müssen wahrheitsgetreu sein,
- Daten müssen gegen unbefugtes Bearbeiten geschützt sein.

Da Daten auch elektronisch verarbeitet werden, kommt aus Sicht des Datenschutzes der Informationssicherheit eine bedeutende Rolle zu. Regeln des ISMS (Information Security Management System) sind ebenfalls im vorliegenden Reglement enthalten.

Bei der Beschaffung und der Verwendung von Personendaten gilt zur Wahrung des Datenschutzes generell die Regel:

So wenig wie möglich – so viel wie nötig
So kurz wie möglich – so ausführlich wie nötig

Jeder Mitarbeitende des Universitäts-Kinderspitals beider Basel (UKBB) darf Daten ausschliesslich zur Erfüllung der ihm vom UKBB übertragenen Aufgaben beschaffen, einsehen und bearbeiten. Jeder Mitarbeitende ist persönlich für den Datenschutz verantwortlich und muss die Daten vor unberechtigtem Zugriff schützen.

Datenschutz ist auch eine Führungsaufgabe. Jeder Vorgesetze ist dafür zuständig und verantwortlich, dass der Datenschutz durch die Mitarbeitenden gewährleistet ist und die Bestimmungen dieses Reglements eingehalten werden.

[1] Um das Papier lesbarer zu gestalten, wird auf die doppelte Nennung der männlichen und der weiblichen Form verzichtet. Die Ausführungen gelten selbstverständlich immer für beide Geschlechter. Die Ausdrücke Daten, sensitive Daten und besonders schützenswerte Daten werden in diesem Reglement gleichbedeutend verwendet.

Die unberechtigte Einsichtnahme in Daten (elektronisch oder in Papierform), muss unverzüglich dem Datenschutzbeauftragten des UKBB mitgeteilt werden. Es darf nur auf Daten zugegriffen werden, die zur Bewältigung der gestellten Aufgaben benötigt werden.

1.2 Geltungsbereich

Dieses Reglement gilt für alle Bereiche des UKBB, alle Mitarbeitenden und alle den UKBB-Mitarbeitenden gleichgestellten Personen. Es regelt den Umgang mit Personendaten (Patienten-, Angehörigen- und Personaldaten) in physischer und elektronischer Form. Es gilt für alle physischen und elektronischen Daten und Datensammlungen. Mitarbeitende des UKBB mit Führungsfunktion können bei Bedarf für einzelne Bereiche ergänzende Regelungen treffen.

2 Rechtliche Grundlagen und ergänzende Weisungen

Grundlagen für dieses Reglement sind:

- Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (insbesondere Art. 179novies und 320 f. StGB),
- Verordnung über die Information und den Datenschutz (IDV) des Kantons Basel-Stadt vom 9. August 2011,
- Leitfaden für die Bearbeitung von Patientendaten im medizinischen Bereich vom eidgenössischen Datenschutzbeauftragten (EDSB), 197, Ausgabe 2002,
- Informations- und Datenschutzgesetz (IDG, SG 153.260) des Kantons Basel-Stadt vom 9. Juni 2010.

Die nachfolgend aufgeführten Weisungen regeln einzelne Themenbereiche und sind Teil dieses Reglements. Die Weisungen sind im Intranet des UKBB einsehbar:

1. Datenschutz für Informationsverarbeitende Systeme, Kurzfassung, Stand 1.1.2014,
2. Weisung zur Durchführung von klinischen Studien am UKBB, welche einer Bewilligung durch die Ethische Kommission beider Basel (EKBB) bedürfen (inkl. Reglement zur Regelung des Zugriffs auf nicht anonymisierte Daten zu Forschungszwecken am UKBB und Reglement zur Anonymisierung personenbezogener Daten),
3. Weitere Weisungen/Reglemente (Reglungen in individuellen Verträgen, z.B. Berufsgeheimnis).

3 Berufsgeheimnis

Mitarbeitende, welche in einem Arbeitsverhältnis mit dem UKBB stehen (Vollzeit-Mitarbeitende, Teilzeit-Mitarbeitende, Aushilfen, Praktikanten, Mitarbeitende externer Firmen etc.), unterstehen der Geheimhaltungspflicht gemäss Art. 320 oder Art. 321 Ziffer 1, des StGB über das Berufsgeheimnis resp. § 26 des Gesundheitsgesetzes BS vom 21. September 2011 und müssen vor der Aufnahme einer Tätigkeit im UKBB ein entsprechendes Formular unterschreiben (vgl. Formular im Intranet, Stand 1.1.2014). Für den Bereich der medizinischen Forschung kommt zudem Art. 321bis StGB zur Anwendung.

Die Schweigepflicht über die anvertrauten Informationen gilt während und auch nach Beendigung des Arbeitsverhältnisses. Es gibt Situationen, in denen Gesundheitsfachpersonen von Gesetzes[2] wegen vom Berufsgeheimnis befreit sind. In unklaren Situationen wird das Gesundheitsdepartement des Kantons Basel- Stadt einbezogen.

Die Verantwortung dafür, dass Mitarbeitende externer Firmen das Formular „Geheimhaltung" vor ihrem Einsatz im UKBB unterschreiben, liegt bei der jeweiligen beauftragenden Stelle im UKBB. Die beauftragende Stelle archiviert die unterschriebenen Geheimhaltungs-Formulare. Werden Personendaten durch Externe bearbeitet, auch nur als Nebeneffekt (bspw. wenn ein Unternehmen mit der Wartung eines medizinischen Gerätes betraut wird und dadurch quasi beiläufig auf die darin gespeicherten Patientendaten zugreifen kann), hat das UKBB sicherzustellen, dass dieser Externe die Daten nur so bearbeitet, wie es dies selbst auch tun darf (§ 7 IDG).

Das Geheimhaltungsformular ist von der tatsächlich die Leistungen ausführenden Person zu unterschreiben.

3.1 Auskunft und Herausgabe von Daten

3.1.1 An Patienten und Eltern

In den „Informationen für Eltern" wird über den Datenschutz im UKBB informiert. Erwähnt wird darin die Möglichkeit, die Information an die nachbehandelnden Ärzte zu sperren.

Jede Person kann bei ihrem Arzt den Zugang zu ihren Daten[3] verlangen. Dies gilt auch noch dann, wenn diese nach der gesetzlichen Aufbewahrungspflicht noch vorhanden sein sollten. Hierzu sind die urteilsfähigen Kinder und Jugendlichen (im Folgenden immer Patienten genannt) und die Inhaber der elterlichen Gewalt von noch nicht urteilsfähigen Kindern berechtigt. Andere Personen sind nur mit einer dokumentierten Einwilligung oder einer schriftlichen Vollmacht des Patienten resp. der Inhaber der elterlichen Gewalt berechtigt. Gegebenenfalls wird die Einsicht eingeschränkt, wenn überwiegende Interessen anderer Personen betroffen sind.

Die um Auskunft ersuchende Person hat das Recht auf Zugang zu ihren eigenen Daten. Die Auskunft erfolgt mündlich oder schriftlich. Die direkte Einsicht in das eigene Patientendossier am Bildschirm wird nicht gewährt. Der verantwortliche Arzt, ab Stufe Oberarzt, prüft und visiert die herauszugebenen Dokumente und ist dafür verantwortlich, dass eine Kopie der herausgegebenen Akten mit seinem Visum im Patientendossier abgelegt wird.

In ausgewählten Fällen werden Daten nur nach einem persönlichen Gespräch in schriftlicher Form herausgegeben (Bsp. psychiatrische Patienten).

Auskünfte in ihrem Kompetenzbereich erteilen, unter Einhaltung der datenschutzrechtlichen Bestimmungen, auch weitere Bereiche im UKBB, wie die Therapien (Physio-, Logo- und Ergotherapie).

[2] § 27 Gesundheitsgesetz BS

[3] Daten können Arztberichte, Laborbefunde, Röntgenbilder, Therapieverläufe u.a. sein

3.1.2 An Externe und an der Behandlung Beteiligte

Externe erhalten nur dann Daten, wenn dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist oder eine Entbindung vom Berufsgeheimnis durch die Aufsichtsbehörde vorliegt. Ansonsten unterliegt die Bekanntgabe von Patientendaten an Ärzte, Therapeuten oder andere Personen der Einwilligung der Patienten. Bei der unmittelbaren Zusammenarbeit zwischen verschiedenen Gesundheitsfachpersonen geht das UKBB von der stillschweigenden Zustimmung des Patienten zur Datenbekanntgabe aus, sofern dieser von der Zusammenarbeit weiss und soweit nur jene Daten ausgetauscht werden, die für die Zusammenarbeit im konkreten Fall auch tatsächlich nötig sind. In Zweifelsfällen ist, die schriftliche Einwilligung des Patienten einzuholen.

Die Auskunft kann telefonisch, per Fax, per Post oder per Mail erfolgen. In allen Fällen müssen Identität und Legitimität der anfordernden Stelle gesichert feststehen. Die Übermittlung erfolgt ausschliesslich über gesicherte Kommunikationswege. Mailverkehr mit sensitiven Personendaten ist Mitarbeitenden des UKBB nur dann erlaubt, wenn eine sichere und zertifizierte Verbindung mit der Kommunikationsadresse besteht, wie z.B. HIN (vgl. dazu 4.1.4).

Auch Auskünfte an die Angehörigen sind grundsätzlich nur mit Einwilligung des Patienten zulässig. Wann immer möglich, soll dieser seine Nächsten selbst informieren. Bei bewusstlosen Patienten geht das UKBB von deren mutmasslicher Einwilligung zur Auskunftserteilung an die nächsten Angehörigen aus, sofern keine gegenteiligen Indizien vorhanden sind.

3.1.3 An Versicherungen

Krankenversicherer dürfen sich nur jene Daten beschaffen, die zur Erfüllung ihrer gesetzlichen Aufgaben unentbehrlich sind. Insbesondere geht es dabei um die Prüfung der Leistungspflicht und die Einschätzung der Wirtschaftlichkeit der Behandlung.

Im Normalfall genügen dem Krankenversicherer die Angaben, welche auf dem Rechnungsformular enthalten sind. Benötigt der Krankenversicherer im Einzelfall zusätzliche Angaben, welche nicht auf der Rechnung ersichtlich sind, hat er dem UKBB schriftlich, spezifische und auf den konkreten Fall bezogene Fragen zu stellen. Diese Fragen werden durch den behandelnden Arzt schriftlich beantwortet. Üblicherweise wird vom UKBB ein separater Bericht, der auf die spezifischen Fragen des Krankenversicherers eingeht, erstellt. Nur in Ausnahmefällen wird eine Kopie des Austrittsberichts zugestellt.

Sind die Angaben ausnahmsweise nicht ausreichend, kann der Krankenversicherer weitere Informationen einholen. Der behandelnde Arzt erstellt nach Rücksprache mit einem Oberarzt einen Bericht an den Vertrauensarzt des Krankenversicherers (persönlich und nicht an eine Sammeladresse wie z. B. „vertrauensärztlicher Dienst“).

Die Auskunftspflicht gegenüber der Unfall- und Invaliditätsversicherung ist gesetzlich weiter gefasst als bei den Krankenversicherern. Die Invalidenversicherung hat von Gesetzes wegen das Recht auf eine Kopie des Austrittsberichts.

3.1.4 An die Staatsanwaltschaft

Auskünfte an die Staatsanwaltschaft und die Herausgabe von Dokumenten haben ausschliesslich über den ärztlichen Direktor des UKBB zu erfolgen.

3.2 Datenbearbeitung

3.2.1 Patientendaten

Die Bearbeitung von Daten hat immer nach den Grundsätzen dieses Reglements zu erfolgen. Die Datenbearbeitung zu Forschungszwecken ist in einer ergänzenden Weisung des UKBB geregelt.

Die Bearbeitung von sensitiven Daten hat grundsätzlich in den Räumen des UKBB stattzufinden. Die Entfernung von Papierakten aus den Räumlichkeiten des UKBB ist nur dann zulässig, wenn dies zur Erfüllung der Aufgaben erforderlich ist. Dem Schutz vor Verlust und vor unbefugter Einsichtnahme ist besondere Beachtung zu schenken.

Vor der Verwendung von Bildmaterial oder namentlich gekennzeichneten Aussagen von Patienten und Mitarbeitenden in internen und externen Publikationen, ist in jedem Fall vorgängig das schriftliche Einverständnis der Betroffenen einzuholen.

3.2.2 Personaldaten

Die Zugriffsberechtigungen für Daten von Mitarbeitenden im SAP werden durch die Personalabteilung festgelegt. Die Regeln betreffend Geheimhaltung, Auskünfte und Datenbearbeitung gelten für Personaldaten sinngemäss wie für Patientendaten.

Physisch vorliegende Personal- und Bewerbungsdossiers dürfen nur im verschlossenen, persönlich adressierten Umschlag mit der internen Post verschickt werden. Elektronisch vorliegende Personal- und Bewerbungsdossiers werden elektronisch an die Bereiche im UKBB weitergeleitet und müssen dort spätestens nach 3 Monaten gelöscht werden. Gehaltsauskünfte werden nur an Mitarbeitende persönlich und an amtliche Stellen (Steueramt, AHV) erteilt.

Das zentral geführte Personaldossier umfasst folgende Teile: Austritt (Abschlusszeugnis, Austrittsunterlagen); Administration (Stellenbeschreibung, Beurteilungen/Personalgespräche, Probezeitberichte, div. Korrespondenz); Fortbildung; Disziplinarisches; Sozialversicherung; Arbeitsvertrag (inkl. Beförderungen, Vertragsänderungen, Vereinbarungen); Bewerbungsunterlagen.

Vorgesetzte haben das Einsichtsrecht in Personaldossiers ihrer Mitarbeitenden. Es dürfen keine „Schatten"-Personaldossiers geführt werden.

Mitarbeitende haben das Recht in ihr Personaldossier Einsicht zu nehmen. Gemäss den Richtlinien zur Aufbewahrung und Archivierung von Akten[4] sind Personaldaten während 10 Jahren nach Austritt aufzubewahren.

Referenzauskünfte über Stellenbewerber sind nur nach Absprache und Einwilligung mit dem jeweiligen Stellenbewerber einzuholen oder zu erteilen.

3.3 Arbeitsplatz

Sensitive Daten (Patientendaten und Personaldaten, sensible Daten des UKBB) dürfen bei Abwesenheit vom Arbeitsplatz für Dritte nicht einsehbar sein.

Zum Schutz von Dokumenten sind diese ausserhalb der Arbeitszeit und auch bei kurzen Abwesenheiten vom Arbeitsplatz so aufzubewahren, dass kein unbefugter Zugriff erfolgen kann.

[4] Departement für Wirtschaft, Soziales und Umwelt des Kantons Basel-Stadt, Amt für Sozialbeiträge, (Ausgabe 07.2013)

Bildschirme von Computern sind so aufzustellen, dass sie von Patienten und Dritten nicht eingesehen werden können.

Ausdrucke sensitiver Daten auf Netzwerkdruckern müssen unmittelbar nach dem Ausdruck dem Drucker entnommen werden. Auf Kopierern und Faxgeräten dürfen keine Ausdrucke liegen bleiben.

Auf die Vertraulichkeit von Informationen ist auch in Gesprächen zu achten. Unfreiwillig Zuhörende dürfen nicht mit ihnen nicht zustehenden Informationen bedacht werden. Dies ist insbesondere auch in der Cafeteria und andern öffentlichen Räumen zu beachten.

3.4 Archivierung / Entsorgung

Die administrativen Daten werden im UKBB physisch 10 Jahre aufbewahrt und dann dem Staatsarchiv des Kantons Basel-Stadt resp. Baselland zur Aufbewahrung angeboten (Anbietungspflicht). Die vom Staatsarchiv nicht benötigten oder gewünschten Daten werden mittels Aktenvernichter oder mit dem internen, gesicherten Verfahren des UKBB entsorgt.

Es ist dafür zu sorgen, dass unbefugte Personen die Archive nicht betreten können.

4 Einsatz von Informatikmitteln

Zum Schutz der Persönlichkeit der Patienten und der Mitarbeitenden im UKBB gilt im Umgang mit Daten, Geräten und Programmen Folgendes[5]:

Datensicherheit kann nicht nur durch Technik garantiert werden. Die Mitarbeitenden sind für ihre Daten verantwortlich.

4.1 Bearbeiten von schützenswerten Daten

Schützenswerte Daten von Patienten und von Mitarbeitenden des UKBB dürfen von den Mitarbeitenden ausschliesslich zur Erledigung der ihnen vom UKBB übertragenen Aufgaben bearbeitet werden. Als Bearbeiten gilt insbesondere das Erheben und Beschaffen, Aufzeichnen, Sammeln und Aufbewahren, Verwenden, Verändern, Austauschen, Zusammenführen, Bekanntgeben, Einsehen, Archivieren und Vernichten von Daten.

4.2 Systemanmeldung und -abmeldung (Login und Logout)

Jeder Mitarbeitende erhält einen persönlichen Zugang zu den Systemen des UKBB. Der Besitzer dieser Zugangsdaten haftet für die damit durchgeführten Aktionen und ist zur Geheimhaltung von Benutzernamen und Kennwörter verpflichtet.

Computer dürfen grundsätzlich nur in abgemeldetem Zustand oder nur mit Kennwort geschütztem Bildschirmschoner verlassen werden. Benutzererkennungen müssen einer Person zugeordnet sein, sind persönlich und müssen vertraulich behandelt werden. Das Weitergeben von Identifikationsmerkmalen (beispielsweise Passwort) ist untersagt.

[5] Die Datenschutzvereinbarung gilt für alle Mitarbeitenden des UKBB und Mitarbeitenden gleichgestellte Personen.

4.3 Datenspeicherung

Daten sind bei vernetzten Rechnern stets auf dem Laufwerk des Ihnen zur Verfügung stehenden Datenservers zu speichern.

Lokale Daten (C:\ und USB-Speichermedien) werden nicht gesichert. Daher ist es nicht erlaubt, auf diesen Laufwerken geschäftsrelevante Daten zu speichern. Die Daten auf UKBB-Fileablagen (Word, Excel, Powerpoint u.a.) können in der Regel bis zu einem Monat wiederhergestellt werden. Nach dieser Zeit werden die Daten auf den Sicherungsmedien überschrieben. Das gleiche gilt bei UKBB-Mailpostfächern.

Datenbanken (z.B. SAP, Phoenix, Polypoint, EKG, EEG u.a.) werden täglich gesichert. Nach einer Woche werden diese Daten auf den Sicherungsmedien überschrieben. Bei Programmanpassungen werden die Daten, je nach Wichtigkeit, vor und nach einem Update speziell gesichert.

Auf UKBB Medien gespeicherte Daten können bei groben internen Verstössen gesichtet werden. Bei strafbaren Handlungen ausserhalb des UKBB werden die Daten an die Untersuchungsbehörden (Staatsanwaltschaft) weitergegeben. Die Information der betroffenen Personen ist die Angelegenheit der oben erwähnten Organe. Das Vorgehen der IT-Abteilung bei einer solchen Untersuchung legt die Geschäftsleitung des UKBB fest.

Einsicht in die persönlichen Daten eines Anwenders sind nur bei einem Mehraugenprinzip möglich (Geschäftsleitung, Personalabteilung und den von Behördenseite zuständigen Datenschutzverantwortlichen).

Grundlage für ein solches Verfahren sind grobe Verstösse gegen das UKBB oder strafbare Handlungen die von Behörden verfolgt werden.

4.4 Datenaustausch

Datenübertragung

Ungesicherter Datentransfer an Dritte ist nicht gestattet. Die üblichen Kommunikationskanäle sind ungesichert. Dadurch kann die Integrität, Vertraulichkeit und Authentizität der übertragenen Daten, der Kommunikation und der Kommunikationspartner nicht sichergestellt werden.

Als Ausnahme gilt die verschlüsselte Übertragung über zertifizierte und gesicherte Verbindungen z.B. HIN (Health Info Net).

Für das Versenden von Datenträgern (Diskette, CD/DVD, USB-Datenträger) können diese von der IT-Abteilung verschlüsselt werden (Anfragen via HelpDesk). Die Übertragung anonymisierter Daten über unverschlüsselte Kommunikationskanäle ist zulässig.

Datennutzung

Das Benutzen von heruntergeladenen Daten aus dem Internet ist nur gestattet, nachdem diese mit dem vom UKBB eingesetzten Virenscanner geprüft worden sind. Software darf nur durch die IT-Abteilung des UKBB installiert werden. Dadurch wird sichergestellt, dass keine Schadsoftware ins lokale Netzwerk gelangen und nur benötigte und lizenzierte Software installiert wird.

Internet

Die IT-Abteilung des UKBB sperrt unsichere und nicht benötigte Internetdienste (z.B. Facebook, Skype, usw.) und protokolliert die Internetaktivitäten.

Im Unternehmensnetzwerk ist Skype oder Lync mit Enterprise Voice verboten. Für die Kommunikation mit zuweisenden und nachbehandelnden Ärzten stehen gesicherte Portale, VPN-Zugängen in der DMZ zur Verfügung.

Bei gravierendem Fehlverhalten, z.B. einem übermässigen privaten Emailverkehr oder nicht tolerierbaren Aktivitäten im Internet (Gefährdung der Daten- und Anwendungssicherheit durch Einschleusen von Viren o.ä.), können regelmässige mitarbeiterbezogene Kontrollen durchgeführt werden. Die zuständigen Vorgesetzten werden informiert.

4.5 Organisation

Die technische Ausführung und Überwachung des Internet-Zuganges ist die IT-Abteilung des UKBB zuständig. Diese stellt die notwendigen sicherheitstechnischen Sachmittel zur Verfügung und überwacht deren Einsatz.

Die IT-Abteilung des UKBB führt das von der Datenschutzgruppe und der Geschäftsleitung des UKBB bewilligte Monitoring durch. Die entsprechenden IT-Konzepte dazu sind ihnen vorzulegen.

Die IT-Abteilung analysiert fortlaufend online den gesamten Datenverkehr von und zum Internet nach schädlichen Codes. Bei Erkennen von kritischen Ereignissen werden entsprechende Massnahmen eingeleitet.

Massenversand von E-Mails, intern wie auch extern (z.B. an „Alle“) ist untersagt oder bedarf der ausdrücklichen Bewilligung durch die Geschäftsleitung.

Allen Mitarbeitenden des UKBB steht ein eigener Email Account zur Verfügung.

Vorgesetzte können für externe Mitarbeitende, die regelmässig im UKBB tätig sind, bei der IT-Abteilung einen Email Account beantragen. Diese Accounts sind auf den UKBB-internen Emailverkehr beschränkt.

4.6 Verhalten der Benutzer

Private Nutzung von Internet und von E-Mail im UKBB dürfen nicht mit der Pflicht zur Erfüllung der übertragenen Aufgaben in Konflikt geraten.

Der Benutzer verwendet ausschliesslich sein persönliches Konto (Account) und ein sicheres, nicht rückschliessbares Kennwort. Er tritt so mit seiner eigenen Identität gegenüber Dritten auf.

Repräsentation nach aussen

Nur Befugte repräsentieren das UKBB im Internet nach aussen. Dabei gelten die bestehenden Unterschriftenregelungen und entsprechenden Vorschriften des UKBB.

Das Eintragen in Newsletter-Listen und ähnlichem ist erlaubt, sofern keine bindenden Verträge abgeschlossen werden, keine Kosten entstehen und Newsletter für das UKBB nützlich sind.

Sicherheit

Schutzvorrichtungen (wie z.B. Virenschutzsoftware, Software Agents) dürfen nicht deaktiviert, umgangen oder verändert werden. Es dürfen keine unerlaubten Kommunikationsmittel an das Netzwerk oder die Computer angeschlossen werden. Dies gilt insbesondere für Kommunikationsgeräte zur Erstellung von Verbindung nach aussen wie Modem oder Router.

Internet / E-Mails / SPAM

Daten, welche vom und zum Internet übermittelt werden, können jederzeit ausserhalb der vom UKBB kontrollierten Netze mitgelesen werden. Es ist grundsätzlich untersagt, besonders schützenswerte Personendaten (Patienten- oder Mitarbeitenden-Daten) via Internet unverschlüsselt zu übermitteln.

Urheberrechte, Copyrights und Lizenzbestimmungen werden vom UKBB vollumfänglich anerkannt und berücksichtigt.

SPAM hat meistens keine Sicherheitsproblematik. Leider gehen dabei aber immer wieder relevante Mails „unter". Die IT-Abteilung des UKBB ist dauernd bestrebt, die Benutzer von dieser Problematik zu entlasten. Um SPAM möglichst zu vermeiden, sollten folgende Punkte beachtet werden:

- Email-Adresse nur an seriöse Kontakte weiter geben (keine Newsletter usw.),
- Öffnen von Links in Mails nur, wenn der Absender bekannt ist,
- Niemals ein Passwort bekannt geben,
- Nie auf SPAM antworten (auch automatische Lesebestätigung ausschalten),
- Email-Adresse nie als Text im Internet präsentieren (Artikel usw.).

5 Nutzung von Soft- und Hardware

5.1 Nutzung von Software

Installation von Programmen

Die im UKBB eingesetzten Softwareprodukte werden zentral verwaltet und deshalb ausschliesslich durch die IT-Abteilung des UKBB installiert. Diese prüft, ob die Software virenfrei und lizenziert ist

Für die Installation von speziellen – nicht in der Grundinstallation vorgesehenen - Programmen hat der jeweilige Vorgesetzte ein „IT-Mittelantrag" an die IT-Abteilung zu erstellen.

Disketten / USB-Sticks

Die von den Mitarbeitenden verwendeten Disketten / CD / DVD / USB-Sticks dürfen nur eingelesen werden, nachdem sie mit dem im UKBB eingesetzten Virenscanner geprüft worden sind.

Kopieren/Weitergabe von Software

Das Kopieren und die Weitergabe von am UKBB eingesetzter Software, auch zu privaten Zwecken, ist illegal und somit untersagt.

Von Mitarbeitern entwickelte Software

Sämtliche Software, die im Auftrag des UKBB oder als Bestandteil des Aufgabengebiets am Arbeitsplatz oder zu Hause durch Mitarbeitende entwickelt wurde, ist Eigentum des UKBB.

5.2 Nutzung von Hardware

Verwendung privater Computern und -zubehör

Für die Erledigung geschäftlicher Aufgaben am Arbeitsplatz sind nur UKBB Computer erlaubt. Private Computer dürfen nur an speziell gekennzeichnete Netzwerkanschlüsse (Anwendernetz) angeschlossen werden. Private Peripheriegeräte (Geräte über einen Steckerkontakt, Bluetooth oder WLAN) dürfen nicht an einen UKBB-Computer angeschlossen werden.

Die Verwendung von privatem Computerzubehör (Lautsprecher, Fotoapparat, Videokameras, MP3-Player, Spielzubehör usw.) ist untersagt. Die Verwendung von privat gekauften und dem ergonomischen Arbeiten dienlichen Tastaturen und Mäusen ist erlaubt. Die Verwendung muss der IT-Abteilung des UKBB gemeldet werden.

Tragbare Personalcomputer (Laptops, Notebooks, PDAs)

Bei sämtlichen tragbaren Personalcomputern muss das Systemkennwort aktiviert werden. Das Kennwort ist nur der IT-Abteilung bekannt. Tragbare Geräte müssen im eingeschalteten Zustand bei Nichtbenutzung mit einem Kennwort oder PIN geschützt sein. Auch Mobilegeräte werden zentral verwaltet. Die Sicherheitsregeln sind den Standard Clients, soweit als möglich angeglichen.

Diebstahlschutz Hardware

Es ist notwendig, dass speziell exponierte Geräte mittels technischen Massnahmen geschützt werden. Die IT-Abteilung des UKBB hilft bei Bedarf weiter.

6 Ergänzende Regelungen

6.1 Schriftliche Genehmigung für Ausnahmebewilligungen

Ausnahmebewilligungen bedürfen eines begründeten Antrages, der vom jeweiligen Vorgesetzten an den internen Datenschutzbeauftragten eingereicht wird. Dieser prüft allenfalls mit dem Leiter IT die Machbarkeit. Der CEO entscheidet abschliessend.

6.2 Qualitätssicherung

Die Abteilung IPE hat von der Geschäftsleitung des UKBB den Auftrag laufend qualitätssichernde Massnahmen durchzuführen. Dazu gehören:

- die zentrale und standardisierte Verwaltung der Clients,
- Sicherheits- und Performance Kontrollen im LAN/WLAN,
- Kontrolle der Schnittstellen (USB-Ports, DVD-Laufwerke, Sticks),
- Kontrolle autorisierter und nicht autorisierter Domain Zugriffe,
- Kontrolle der Regelverstösse im Umgang mit Emails und Internet.

6.3 Verantwortlichkeit und Meldepflicht

Bei Zuwiderhandlung gegen dieses Reglement und der entsprechenden Weisungen des UKBB oder gegen das Datenschutzgesetz werden die notwendigen arbeits-, zivilrechtlichen bzw. personalrechtlichen Massnahmen bis hin zur Kündigung eingeleitet.

Jeder Mitarbeitende ist verpflichtet, sicherheitsrelevante Vorkommnisse, Missbräuche oder Sicherheitslücken welche den Datenschutz gefährden, dem Datenschutzbeauftragten des UKBB zu melden. Diese Meldungen können auch anonym erfolgen.

7 Organisation Datenschutz UKBB

Um die Verantwortung im Umgang mit besonders schützenswerten Daten wahrzunehmen, besteht im UKBB folgende Organisation:

Interner Datenschutzbeauftragter UKBB

Aufgaben des internen Datenschutzbeauftragten:

- Sicherstellung, dass die datenschutzrelevanten Reglemente und Verfahren allen interessierten und betroffenen Personen zugänglich sind,
- Entwicklung und Betreuung von Reglementen und Weisungen betr. dem Umgang mit besonders schützenswerten Daten; regelmässige Vorschläge zur Anpassung der Reglemente gemäss den sich ändernden gesetzlichen und betrieblichen Bestimmungen,
- Beratungs-, Informations- und Dokumentationsdienst für alle datenschutzrelevanten Anfragen sowohl von intern wie extern,
- Schulung, Information und Sensibilisierung der Mitarbeitenden in Zusammenarbeit mit dem kantonalen Datenschutzbeauftragten,
- Beobachtung der Entwicklung auf dem Gebiet des Datenschutzes,
- Information der Geschäftsleitung über seine Tätigkeit und die Aktivitäten der Datenschutzgruppe

Datenschutzgruppe UKBB

Aufgaben der Datenschutzgruppe:

- Zusammentragen von datenschutzrelevanten Fragestellungen,
- Unterstützung des Datenschutzbeauftragten bei seinen Aufgaben,
- Förderung der Einhaltung des Datenschutzes im UKBB,
- Vorschläge zuhanden der Geschäftsleitung UKBB zur Verbesserung des Datenschutzes.

Folgende Personengruppen sind in der Datenschutzgruppe vertreten: Therapien, Pflege, Arztdienst, Sekretariate, Informatik, Personalabteilung, Qualitäts- und Risikomanagement und Facilitymanagement. Die Wahl der Mitglieder erfolgt durch die Geschäftsleitung. Die Datenschutzgruppe trifft sich mindestens 4 Mal im Jahr. Sie führt ein Beschlussprotokoll.

8 Schlussbestimmungen

Dieses Reglement ersetzt folgende Dokumente: Vereinbarung über die Benutzung von Internet und E-Mail am Universitäts-Kinderspital beider Basel (UKBB) vom 17. Januar 2003 und vom 19.08.2011, die Datenschutzvereinbarung vom 01.01.2012 und das Datenschutzreglement vom 01.01.2012.

Das Datenschutz-Reglement des UKBB wurde vom Verwaltungsrat an der Sitzung vom 29.09.2014 genehmigt. Es tritt per sofort in Kraft.

Basel, 29.09.2014

Manfred Manser
Präsident des Verwaltungsrates

Dr. Conrad E. Müller
Sekretär des Verwaltungsrates