HÔPITAUX ROBERT SCHUMAN

# Verhaltenskodex für das interne und externe Personal betreffend die Sicherheit der Informationen innerhalb von Hôpitaux Robert Schuman

# Inhaltsverzeichnis

Einleitung

Informationen betreffend die medizinischen, pflegerischen und administrativen Bereiche unterliegen der strikten Einhaltung der deontologischen und gesetzlichen Bestimmungen. Diese Bestimmungen gewährleisten die Sicherheit und den Schutz der Patienten- und Personaldaten sowie des Personals das in HRS beschäftigt ist.

## 1. ZIELSETZUNG DES VERHALTENSKODEX

Vorrangige Ziele dieses Verhaltenskodexes sind:

- Das Einbeziehen von Personal, die berechtigten medizinischen und paramedizinischen Partner in die Verantwortung für die Risiken, die mit der Sicherheit der Information verbunden sind
- die beteiligten Parteien von HRS über die bewährten Praktiken zur Informationsverwaltung in einem juristischen Rahmen zu informieren
- die Patienten und das interne und externe Personal vor einer Sicherheitsverletzung der persönlichen Daten zu schützen.

## 2. ANWENDUNGSGEBIETE

Dieser Verhaltenskodex gilt für alle Personen, die berechtigt sind die Systeme zur Informationsverwaltung der HRS nutzen (die Nutzer)

Die Nutzer sind z.B. :

- das Personal von HRS,
- die angestellten Ärzte von HRS
- die liberalen Ärzte die in HRS tätig sind
- das weitere externe Personal (Berater usw.)

Unter Information versteht man alle betreffenden Daten der Patienten und/oder des Personals, die im Informationssystem des HRS vorhanden sind, mündlicher oder schriftlicher Natur, in digitaler Form oder als Papierversion.

- Gesundheitsdaten werden vom Gesetz als sensible Daten* bezeichnet. Somit dürfen die innerhalb der HRS erstellten Daten nur von berechtigten Personen eingesehen werden, die im Rahmen der Ausübung ihrer Tätigkeiten dazu ermächtigt sind.

- Die Identifizierung sowie die Authentifizierung sind obligatorisch wenn es um die Verwaltung von vertraulichen Daten geht.

- Laut Gesetz hat Hôpitaux Robert Schuman die Pflicht, jeden unberechtigten Zugriff auf persönliche Gesundheitsdaten die in ihrem Informationssystem beinhaltet sind, zu unterbinden.

* *Anhang betreffend die in Luxemburg geltenden Texte und Verordnungen. Siehe auch den Ministerialerlass vom 7. Juli 2005 betreffend die* **Genehmigung des Verhaltenskodex** *der Ärzte und Zahnärzte des Ärztekollegiums.*

Das Informationssystem beinhaltet:

- Daten mündlicher oder schriftlicher Natur, in digitaler Form oder als Papierversion,
- Softwarekomponenten (Anwendungen und Datenbanken, die den Mitarbeitern im Gesundheitswesen zur Verfügung gestellt werden),
- Netzwerkkomponenten (Infrastruktur für Wifi, Netzwerke, Kabel usw.),
- Computerarbeitsplatz (Bildschirm, Tastatur, Maus, Zentraleinheit, Drucker, Laptop)

## 3. ZUSTÄNDIGKEIT

Juristische Definition des Verantwortlichen für die Verarbeitung:

Das Gesetz vom 2. August 2002 hält fest : Verantwortlich für die Datenverarbeitung ist jene natürliche oder juristische Person, Behörde, Abteilung oder jede andere Institution die alleine, oder zusammen mit anderen, die Zielsetzung und die Mittel der Verarbeitung von persönlichen Daten festlegt. HRS ist verantwortlich für die informatische Verarbeitung der Daten in ihrem Informationssystem.

Es obliegt also der Verantwortung der Direktion HRS die Sicherheit der Informationen die sie verwahrt zu gewährleisten und über die Einhaltung der Benutzerregeln des Informationssystems von HRS zu wachen.

Alle Personen die Zugriff auf das Informationssystem des HRS haben, und/oder dieses System benutzen, müssen die expliziten Benutzerregeln dieses Verhaltenskodexes berücksichtigen.

## 4. VERPFLICHTUNG ZUR SICHERHEIT

Das Gesetz vom 2. August 2002 hält in Art. 22(1) fest, dass jeder Verantwortliche für die Datenverarbeitung die Sicherheit und die Vertraulichkeit der Daten gewährleisten muss.

Die gesetzlichen Verpflichtungen im Bereich der Sicherheit sind folgende:

- Zutrittskontrolle (Gebäudesicherung)
- Zugangskontrolle (Sicherung des Zugriffs auf DV-Systeme)
- Datenspeicherkontrolle (Zugriffsbeschränkungen auf die Verwaltungssysteme)
- Nutzungskontrolle (Schutz des Netzwerkes – Firewalls, DMZ)
- Zugriffskontrolle (Verwaltung der Konten, Verlaufskontrolle)
- Weitergabekontrolle (Datenübertragungsmaßnahmen: VPN, Verschlüsselung bis hin zur elektronischen Unterschrift)
- Eingabekontrolle (Login/Passwort)
- Transportkontrolle (Verschlüsselung der Träger)

- Verfügbarkeitskontrolle (Backupkonzepte, Sicherungskopien))

## 5. PRAKTISCHE LEITLINIEN

- Die Nutzer müssen dem IT-Helpdesk alle Zwischenfälle melden, welche die Sicherheit anbelangen.
- Die Nutzer müssen sämtliche Vorsichtsmaßnahmen ergreifen um den Schutz der ihnen anvertrauten Daten zu gewährleisten.
- Die Nutzer sind für ihr Arbeitsumfeld verantwortlich. Dieses muss sauber, ordentlich und abgesichert sein.
- Die Nutzer sind weder berechtigt die Konfiguration der Systeme zur Informationsverwaltung zu verändern, noch deren Parameter, welche ihnen von HRS zur Verfügung gestellt werden.
- Der Zugriff auf sämtliche Systeme zur Datenverwaltung muss geschützt sein.
- Die Nutzer dürfen weder ihr Passwort noch ihre eigene Smartcard zur Authentifizierung an Drittpersonen weitergeben, auch nicht an ihre Vorgesetzten oder Assistenten.
- Die Nutzer müssen ihre Mailboxen verantwortungsbewusst verwalten.
- Es ist den Nutzern untersagt, medizinische Informationen, welche aus dem Informationssystem HRS stammen, weiterzuleiten oder auf externe Datenträger zu speichern (USB-Sticks, CD-ROM, usw.), es sei denn die Erlaubnis dazu wurde ausdrücklich und nachvollziehbar erteilt.

## 6. SICHERHEIT / PASSWÖRTER

Alle Passwörter müssen regelmässig erneuert werden und den Sicherheitsvorgaben des HRS entsprechen.

## 7. VERHALTENSREGELN

Im Falle der Nichteinhaltung dieses Verhaltenskodexes oder im Falle einer Zuwiderhandlung muß der Nutzer mit Konsequenzen rechnen. Die Sanktion richtet sich nach der Schwere des Vergehens unter Berücksichtigung des Kontextes und der geltenden Rechtsvorschriften. * *Anhang*

## 8. VERPFLICHTUNG

Der Mitarbeiter/in erklärt hiermit, dass er den Verhaltenskodex zur Kenntnis genommen hat und verpflichtet sich, diesen zu respektieren.

Name : _____ Vorname : _____

Titel : _____

Unterschrift : _____ Datum : _____/_____/20___

## 9. ANHANG ZU DEN GESETZESTEXTEN UND REFERENZVORSCHRIFTEN

Die Verarbeitung von **persönlichen/vertraulichen Daten** im Bereich der Überwachung von **e-mails**, der **Internetnutzung** und der **Netzwerke** fallen in den Anwendungsbereich verschiedener gesetzlicher Bestimmungen, die hier noch einmal in Erinnerung gerufen werden:

**Jede Veränderung des Verhaltenskodexes sowie jede Überwachungsmaßnahme müssen im Vorfeld im Rahmen des gemischten Ausschusses diskutiert werden. Der Arbeitgeber ist verpflichtet eine Erlaubnis bei der CNPD einzuholen.**

- die Direktive 95/46/CE des Europäischen Parlamentes und des Rates vom 24 Oktober 1995 betreffend den Schutz der natürlichen Personen gegenüber der Verarbeitung von persönlichen/vertraulichen Daten und den freien Verkehr dieser Daten (hier „Directive cadre" genannt);

- die Direktive 2002/58/CE des Europäischen Parlamentes und des Rates vom 12 Juli 2002 betreffend die Verarbeitung von persönlichen/vertraulichen Daten und den Schutz des Privatlebens im Bereich der elektronischen Kommunikation (hier «Directive vie privée et communications électroniques» genannt) ;

- Artikel 8, Absatz (1) der Europäischen Konvention zum Schutz der Menschenrechte;

- Artikel 7 der Charta der Grundrechte der Europäischen Union;

- Artikel 28 der Verfassung ;

- Gesetz vom 28 August 1998 betreffend die Krankenanstalten : Art. 38 : Rechte des Patienten im Hinblick auf den Schutz des Privatlebens;

- das veränderte Gesetz vom 2 August 2002 betreffend den Schutz der Personen im Hinblick auf die Verarbeitung von persönlichen/vertraulichen Daten (hier «la loi» genannt) ;

- das veränderte Gesetz vom 30 Mai 2005 betreffend die speziellen Bestimmungen zum Schutz der Personen im Hinblick auf die Verarbeitung von persönlichen/vertraulichen Daten im Bereich der elektronischen Kommunikation (hier «la loi du 30 mai 2005» genannt) ;

- das Gesetz vom 11 August 1982 betreffend den Schutz des Privatlebens (hier « la loi du 11 août 1982 » genannt);

- der Artikel 460 des Strafgesetzes;

- das Arbeitsgesetzbuch und besonders die Art. L.261-1, L.261-2 et L.423-1;

- der Ministerialerlass vom 7 Juli 2005 betreffend die Genehmigung des Verhaltenskodex der Ärzte und Zahnärzte des Ärztekollegiums;

- die Genehmigung des Verhaltenskodex der Ärzte und Zahnärzte des Ärztekollegiums: Artikel 4-6 betreffend das Berufsgeheimnis, Artikel 44-50 betreffend die Information des Patienten sowie seine Zustimmung, Artikel 60-65 betreffend die medizinische Patientenakte und die Zugriffsmodalitäten;

- Artikel 37, Anlage 8 „Liste des moyens informatiques et de télécommunication“ des Kollektivvertrages :

- Artikel 15, 16, 18, 19, 20, 21 des Règlement grand-ducal du 07 octobre 2010 établissant le code de déontologie de certaines professions de santé.