Begriffe

- Datenschutz
  Daten werden vor unberechtigtem Zugriff geschützt.
- Datensicherheit
  Daten werden vor Verlust oder unberechtigten Änderungen oder unberechtigtem Zugriff geschützt.
- Datensicherung
  Methode, um die Datensicherheit im Hinblick auf den Verlust von Daten zu gewährleisten.

Rechtliche Grundlagen des Datenschutzes

- EU-Datenschutzrichtlinie
  http://europa.eu.int/comm/internal_market/privacy/index_de.htm
  Regelt auf europäischer Ebene die Belange des Datenschutzes.
- Grundgesetz (GG)
  Art. 10 und Art. 73
  http://www.jura.uni-sb.de/BIJUS/grundgesetz/
  Regelt das Fernmeldegeheimis und die Hoheit des Bundes bzgl. Telekommunikationseinrichtungen.
- Bundesdatenschutzgesetz (BDSG)
  http://bundesrecht.juris.de/bundesrecht/bdsg_1990/index.html
  Regelt den Datenschutz in Betrieben sowie der öffentlichen Verwaltung.
- Berliner Datenschutzgesetz (BlnDSG)
  http://www.datenschutz-berlin.de/recht/bln/blndsg/blndsg_nichtamt.htm
  Regelt die lokalen Gegebenheiten in Berlin.

Rechtliche Grundlagen des Datenschutzes

- Sozialgesetzbuch (SGB)
  - SGB I §§ 35-37
    http://bundesrecht.juris.de/bundesrecht/sgb_1/index.html
    Regelt das Sozialgeheimnis und damit verbundene elektronische Datenübermittlung.
  - SGB X §§ 67-85
    http://bundesrecht.juris.de/bundesrecht/sgb_10/index.html
    Regelt den Schutz der Sozialdaten sowie deren Datenerhebung, -verarbeitung und -nutzung.
- Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste
  (Informations- und Kommunikationsdienste-Gesetz - IuKDG)
  http://www.datenschutz-bayern.de/recht/iukdg.htm
  Regelt das Zusammenspiel unterschiedlicher Gesetze im Bereich Information und Kommunikation.

Rechtliche Grundlagen des Datenschutzes

- Telekommunikationsgesetz (TKG)
  http://bundesrecht.juris.de/bundesrecht/tkg/index.html
  insb. TKG § 89
  Regelt den Datenschutz im Rahmen von Telekommunikationseinrichtungen.
- Signaturgesetz (SigG)
  http://bundesrecht.juris.de/bundesrecht/sigg_2001/index.html
  Regelt den Umgang mit verschüsselten Daten.
- Betriebsverfassungsgesetz (BetrVG)
  BetrVG § 87, Abs. 1, Nr. 6
  http://bundesrecht.juris.de/bundesrecht/betrvg/index.html
  Regelt die Mitbestimmungsrechte des Betriebsrates im Hinblick auf technische Überwachungsmaßnahmen der Mitarbeiter.

Wichtige Grundsätze der Gesetzgebung

- Personenbezogene Daten sind nach „Treu und Glauben“ zu behandeln.
  D.h. die Daten dürfen nur für **einen eindeutigen** und **rechtmäßigen Zweck** verwendet werden.
- Die Person deren Daten erhoben werden, muss ihre Einwilligung zur Speicherung und Verarbeitung der Daten geben.
  D.h. für die Praxis: Liegt eine Einwilligung zur elektronischen Datenverarbeitung nicht vor, so müssen die Daten weiterhin schriftlich erhoben werden!!!
- Die Person deren Daten erhoben werden, besitzt grundsätzlich ein Auskunftsrecht (Einsicht in die Daten).
  Ausnahme: Psychiatrische Erkrankungen.
- Die Person deren Daten erhoben werden, besitzt ein Widerspruchsrecht.
  D.h. eine Einwilligung kann zurück gezogen werden.

Wichtige Grundsätze der Gesetzgebung

- Personengebundene Daten dürfen ausschließlich auf Weisung durch einen Verantwortlichen verarbeitetet werden.
  D.h. auch ein authorisierter Mitarbeiter muss im Zweifelsfall die Weisung abwarten, um Daten auszuwerten, weiterzuleiten o.ä. Manipulationen vorzunehmen.
- Die Sicherheit der Daten muss durch technische und organisatorische Maßnahmen gewährleistet werden.
- Werden personenbezogene Daten gespeichert, so muss eine Meldung an eine Datenschutz-Kontrollstelle erfolgen.
  Diese Aufgabe übernimmt der Datenschutzbeauftragte des Hauses. Aber Achtung: In kleineren ambulanten Einrichtungen ist dies häufig nicht geregelt!

Folgen für die Praxis

Datenschutzbeauftragter

- Jede Veränderung der IT-Infrastruktur muss mit dem Datenschutzbeauftragten abgesprochen werden.
- Insbesondere Veränderungen an Datennetzen sollten zusätzlich mit externen Instanzen des Datenschutzes (Landesdatenschutzbeauftragter) abgestimmt werden.

Datenübertragung

- Die Art der zu übertragenden Daten ist auf ein Minimum zu beschränken (z.B. die Labordaten, nicht jedoch Name etc. des Patienten). Zur Wiedererkennung müssen Identifikationsnummern verwendet werden.
- Die Datenübertragung sollte verschlüsselt erfolgen. Dieses Vorgehen ist immer notwendig, sofern die Daten das eigene LAN verlassen (z.B. per Internet).

Folgen für die Praxis

Patientendaten

- Grundsatz 1:
  Der Patient muss der elektronischen Datenerhebung zustimmen. Andernfalls dürfen die Daten nicht gespeichert werden.
- Grundsatz 2:
  Es dürfen diejenigen Daten übertragen werden, die zur sachgerechten Behandlung des Patienten notwendig sind.
- Grundsatz 3:
  Der Datenaustausch mit externen Einrichtungen ist zulässig, sofern dies der sachgerechten Behandlung des Patienten dient.
  Eine Erneute Einwilligung des Patienten ist hierzu nicht erforderlich. Vielmehr gilt: Hat der Patient der elektronischen Datenerhebung grundsätzlich zugestimmt, so muss er die Weiterleitung der Daten an andere Behandlungseinheiten ausdrücklich verbieten.
  (siehe dazu auch: http://www.baden-wuerttemberg.datenschutz.de/material-lfd/gesundheitswesen.html)

Exkurs: Patienteninformation

„Im Bereich der Telemedizin ist es besonders wichtig, dass der Patient in allen Verarbeitungsphasen ausreichend informiert ist über die Verarbeitung seiner personenbezogenen Daten.

Dies setzt voraus, dass das ihn informierende Personal ebenfalls ausreichend informiert ist.

Es muss insbesondere auch gewährleistet sein, dass dem Patienten bei Vertragsabschluss bzw. Einwilligung Umfang, Zweck und Rechtsgrundlage der Verarbeitung seiner Daten sowie ggf. die Grundzüge des technischen Verfahrens der Verarbeitung (z.B. bei Chipkartenverfahren) bekannt gegeben worden sind."

Quelle: Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2002): Datenschutz und Telemedizin. Anforderungen an Medizinnetze.

Internet:

http://www.lfd.niedersachsen.de/functions/downloadObject/0,,c1231690_s20,00.pdf

Risiken der Datensicherheit

Risiken, welche die innerbetriebliche Datensicherheit gefährden können:

1. Zugriff durch unbefugte Personen
   - Mitarbeiter innerhalb des Betriebes (z.B. durch Passwortdiebstahl)
   - Daten, die von Mitarbeitern mitgenommen und auf den heimischen Rechner kopiert wurden.
2. Computerviren
   - Zerstörung von Daten
   - Spionage relevanter Daten
3. Fehler befugter Personen
   - Daten werden an Personen versandt, die nicht dem erwünschten Empfänger entsprechen (z.B. per unverschlüsselter E-Mail).
4. Entwenden der Hardware, z.B. durch
   - Diebstahl
   - Weiterverkauf einer Festplatte, die nicht sicher gelöscht wurde

Folgen für die Praxis

Zugriffssteuerung

Grundsätzlich gilt:

Jedes Datennetz im Gesundheitswesen muss vor unbefugtem Zugriff abgeschottet werden. D.h.

Alle Patientendaten müssen so gesichert sein, dass:

- Speicherung
- Nutzung
- Veränderung und
- Weitergabe

nur durch authorisierte Personen stattfinden. (siehe auch: http://info.imsd.uni-mainz.de/AGDatenschutz/Empfehlungen/Zugriff.html)

Zusätzlich müssen die Daten vor externen nicht authorisierten Personen geschützt werden. Dies geschieht durch eine Firewall sowie durch Virenschutz-Software.

Folgen für die Praxis

Auffinden von Sicherheitslücken

Grundsätzlich gilt:

Jedes Datennetz ist nur so sicher, wie dessen größte Schwachstelle!

Szenario:

Der Abteilungsserver wird morgens per automatischer Anmeldung (mit Benutzername und Passwort) gestartet, da nicht sichergestellt werden kann, dass die authorisierte Person (z.B. Abteilungsleitung) anwesend ist.

Folge:

Alle Rechner der Station sind sicher, bis auf den Server, der in einem nicht verschlossenen Nebenraum plaziert ist. **Jeder Besucher / Patient könnte in einem solchen Fall auf alle Daten zugreifen**!

Konsequenz:

Jede Führungskraft im Unternehmen ist für die Datensicherheit verantwortlich. D.h. sie muss über die Infrastruktur informiert sein und die notwendigen Maßnahmen zur Datensicherheit ggf. überprüfen.

Weitere Quellen: Datenschutzbeauftragte der Länder

- http://www.datenschutz-berlin.de/
- http://www.datenschutzzentrum.de/
- http://www.datenschutz.de/
- http://www.bfd.bund.de/
- Zeitschrift: Datenschutz und Datensicherheit
  http://www.dud.de/