Empfehlungen zur Sicherheit des Intranets von Krankenhäusern

AG DGI der GMDS, 27. März 2011

0. Zusammenfassung (Management Summary)

0.1 Zielvorstellungen, Anforderungen und Risiken: Hohe Priorität für ein Krankenhaus hat die Sicherheit der Patienten und der Schutz der Patientendaten und anderer Ressourcen, insbesondere vor Gefahren aus dem Internet. Andererseits erfordern dienstliche Belange und die Unterstützung der Krankenversorgung und Forschung einen möglichst ungehinderten Zugang zum Internet aus dem Bereich des Krankenhauses heraus sowie in umgekehrter Richtung den Zugriff auf das Intranet des Krankenhauses, möglichst von überall in der Welt.

Diese beiden Zielvorstellungen (Sicherheit und ungehinderter Zugriff) *stehen in einem Konflikt miteinander, zu dessen Auflösung nicht zu vernachlässigende Anstrengungen und Ressourcen notwendig sind.*

Der Schutz der Patientendaten einschließlich dem Schutz von Medizingeräten[1] muss dabei höchste Priorität genießen

- wegen der gesetzlichen Anforderungen der ärztlichen Sorgfalts- und Schweigepflicht,
- wegen des Schutzes von Leben und Gesundheit der Patienten,
- wegen des Ansehens und der Glaubwürdigkeit des Krankenhauses in der Öffentlichkeit.

Die letztendliche Verantwortung hierfür liegt beim Vorstand. Damit dieser sie adäquat wahrnehmen kann, sind

- angemessene technische Maßnahmen nach Vorgaben der anerkannten guten Praxis,
- organisatorische Regelungen zum Abdecken verbleibender Sicherheitslücken

notwendig. Dazu muss die Sicherheitslage dem Vorstand nachvollziehbar dargestellt werden.

Daher sind für dringende Sicherheitsprobleme im Netz des Krankenhauses praktikable Lösungen zu entwickeln. Das betrifft die Sicherheit der Patientendaten vor Angriffen aus dem Internet, die Sicherheit des internen Netzes und der Server, Medizingeräte und Arbeitsplatzrechner und ergänzend dazu die abgesicherte Möglichkeit zum Zugriff für Mitarbeiter von außen auf interne Daten und das E-Mail-Konto.

0.2 Grundsätzliche Empfehlungen:

1. Ein IT-Sicherheitskonzept für das Krankenhaus ist dringend nötig. Dazu gehört eine vom Vorstand verabschiedete allgemeine Richtlinie (Policy), ein Grobkonzept (z. B. Anpassung dieser Empfehlung an die lokalen Gegebenheiten) sowie ein Feinkonzept, das auch eine Risikoanalyse einschließt.
2. Als wichtigste konkrete Maßnahme wird eine Trennung des Krankenhausnetzes in ein streng geschütztes klinisches Datennetz und ein allgemeines Krankenhausnetz (KH-Netz) mit erleichtertem Internetzugang, das z. B. in Universitätskliniken auch den Bereich „Forschung und Lehre“ umfasst, empfohlen. Von Arbeitsplatzrechnern aus dem allgemeinen KH-Netz sollte ein Zugriff auf das klinische Datennetz über virtuelle

[1] Nach dem 4. MPG-Novellierungsgesetz ist auch ein erheblicher Teil der Software im KIS rechtlich als Medizinprodukt einzuordnen.

Techniken ermöglicht werden[2]. Für Zugriffe von außen ist eine geeignete sichere Portal-Lösung anzustreben.

3. Eine Risikoabschätzung nach dem Kosten-Nutzen-Modell ist für ein Krankenhausnetz nicht sinnvoll durchführbar; statt dessen sind im Sinne der guten Praxis die Empfehlungen des BSI zu befolgen, wie sie in den IT-Grundschutzkatalogen definiert sind[3]. Wegen des hohen Schutzbedarfs von Patientendaten sind zusätzliche Maßnahmen nötig.
4. Die Gewährleistung der IT-Sicherheit im klinischen Datennetz ist als Serviceleistung der zentralen IT-Abteilung anzusehen; Anwender müssen von eigener Sorge um die Sicherheit dieses Netzes und ihrer Patientendaten so weit möglich durch technische Maßnahmen entlastet werden. Im Gegenzug ist eine weitgehende zentrale Administration der Arbeitsplatzrechner anzustreben.
5. Da technische Maßnahmen nicht ausreichen, um alle Sicherheitsprobleme zu lösen, sind ergänzende organisatorische Maßnahmen unerlässlich.

0.3 Empfehlungen für den Vorstand:

1. In Abstimmung mit dem Datenschutzbeauftragten Erlass einer Leitlinie („Policy“) zum Datenschutz und zur IT-Sicherheit, die für Mitarbeiter verpflichtend ist; hier sollten auch Zugriffsregelungen von extern und mögliche Ausnahmeregelungen bei nachgewiesener dienstlicher Notwendigkeit definiert sein.
2. Anforderung regelmäßiger schriftlicher Berichte der zentralen IT-Abteilung über bestehende Risiken und Schwachstellen.
3. Auftrag an die zentrale IT-Abteilung zur Erstellung eines Feinkonzepts zu den vorgesehenen Maßnahmen für Netzstruktur und Sicherheit der IT-Arbeitsplätze sowie zur Kostenplanung, Priorisierung und Umsetzung.
4. Bereitstellung der dafür notwendigen Ressourcen gemäß der von der zentralen IT-Abteilung vorgelegten Kostenplanung.
5. Auftrag an die zentrale IT-Abteilung zur Formulierung von SOPs für die Mitarbeiter zum Umgang mit Patientendaten, Medizingeräten, Internet, E-Mail und mobilen Geräten; hierzu soll auch der Datenschutzbeauftragte konsultiert werden.
6. Grundsätzlich ist zu empfehlen, die Stelle eines IT-Sicherheitsbeauftragten zu etablieren. Dieser sollte direkt dem Vorstand unterstellt und bezüglich Beratungs- und Weisungsbefugnis ähnlich dem Datenschutzbeauftragten eingeordnet sein. Für kleinere Krankenhäuser kann diese Aufgabe auch an vertrauenswürdige externe Dienstleister vergeben werden.

1. Anforderungen

Die besonderen Schutzanforderungen der klinischen Daten und Prozesse und der Medizingeräte geben sehr enge Rahmenbedingungen für den Betrieb des Intranets eines Krankenhauses und seiner Anbindung an das Internet vor. Ärztliche Sorgfalts- und Schweigepflicht sowie Datenschutz definieren für die Patientendaten aus der Krankenversorgung einen hohen[4] Schutzbedarf. Die ins Intranet eingebundenen Medizingeräte erfordern gleichfalls einen ho-

[2] Der entscheidende Aspekt hierbei ist, dass Daten nicht auf den Arbeitsplatzrechner herunter geladen, sondern nur auf dem Bildschirm dargestellt werden. Diese weitgehende Abschottung der Patientendaten ist Voraussetzung dafür, dass der Umgang mit dem Internet für das allgemeine KH-Netz erleichtert werden kann.
[3] Diese werden auch in der Rechtsprechung und bei Datenschutzprüfungen zu Grunde gelegt.
[4] Gemäß § 3 Abs. 9 i.V.m. § 4a Abs. 3, § 4d Abs.5 und § 28 Abs. 6 BDSG muss bei Patientendaten immer von einem hohen Schutzbedarf ausgegangen werden.

hen Schutz[5]; zu den Medizingeräten muss seit dem 4. MPG-Änderungsgesetz auch ein Teil der KIS-Software gezählt werden. Daneben sind aber auch dienstliche Daten wie Benchmarking- und Forschungsdaten, innerbetriebliche Verwaltungsdaten und Finanzdaten als Betriebskapital des Krankenhauses schützenswert.

Andererseits erfordern die Unterstützung der Forschung und die Optimierung der Versorgung einen möglichst ungehinderten Zugang zu den Ressourcen des Internets aus dem Bereich des Krankenhauses heraus sowie in umgekehrter Richtung den Zugriff auf Ressourcen des Krankenhauses von überall in der Welt. Insbesondere in Universitätskliniken haben die Bereiche „Forschung und Lehre“ und „Krankenversorgung“ sehr unterschiedliche Anforderungen an Informationsoffenheit und den gleichzeitig zu gewährleistenden Schutz klinischer Ressourcen.

Ein Bedarf an Fernzugriffen besteht auch im Bereich der Patientenversorgung, etwa durch den ärztlichen Hintergrunddienst, sowie für Zwecke der Fernwartung von Servern und Medizingeräten.

Diese beiden Anforderungen (Sicherheit und ungehinderter Zugriff) stehen in einem Zielkonflikt miteinander, zu dessen Auflösung erhebliche Anstrengungen notwendig sind. Die Sicherheit von Daten, Prozessen und Medizingeräten im Intranet und der freie Informationsaustausch im Internet können nicht gleichermaßen in einem gemeinsamen Netz ohne zusätzliche technische und organisatorische Maßnahmen garantiert werden.

2. Bisherige Empfehlungen

Bisherige Sicherheitsempfehlungen, auch dieser AG, beruhten auf der Annahme, dass das Intranet sicher ist und Gefährdungen im wesentlichen vom Internet ausgehen. Durch die Parallelität der Nutzung des Arbeitsplatzrechners für das Arbeiten im Intranet und im Internet hat sich die Problemlage für die Sicherheit der Daten im Intranet aber in den letzten Jahren zunehmend verschärft.

Die physikalische Trennung von Intranet und Internet mithilfe eines Sicherheitsgateways („Firewall“) und der Einsatz eines Remote-Controlled Browsers Systems (ReCoBS[6]) für den Zugriff auf das Internet – entsprechend dem Konzept des Bundesamtes für Sicherheit in der Informationstechnik (BSI) – wurden bislang als wesentlicher Beitrag zur Wahrung des notwendigen Sicherheitsniveaus für die im Intranet vorhandenen Ressourcen angesehen.

Die Verfügbarkeit neuer Techniken und deren unkontrollierter Einsatz haben deutliche Auswirkungen auf das Sicherheitsniveau des Intranets und zeigen die Unzulänglichkeit der bisherigen Empfehlungen. Hierzu gehören z. B. UMTS-Sticks, die den Internetzugriff aus dem Intranet des Krankenhauses heraus unter Umgehung des Sicherheitsgateways erlauben, mobile Speicher mit großem Speichervolumen zum Import und Export von Daten, unkontrollierter

[5] vgl. Norm E IEC / DIN EN 80001

[6] Unter einem Remote-Controlled Browsers System (ReCoBS) versteht das BSI den Web-Zugang mit Hilfe von speziell gesicherten Terminalserver-Systemen. Dabei laufen die Browser nicht auf den Arbeitsplatz-PC’s, sondern auf einem Terminalserver außerhalb des LAN und werden von den Arbeitsplätzen aus ferngesteuert. Im Browser auf dem Terminalserver werden alle Webinhalte ausgeführt, so dass bei Einhaltung entsprechender Sicherheitsanforderungen Aktive Inhalte nicht ins LAN gelangen können. Statt dessen werden grafische Informationen an die Arbeitsplätze übermittelt und dargestellt. Damit sind Ausführung und Darstellung Aktiver Inhalte voneinander getrennt. (Quelle: Remote-Controlled Browsers System (ReCoBS) - Grundlagen und Anforderungen, Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/cae/servlet/contentblob/478364/publicationFile/30920/recobslanginfo_pdf.pdf)

Einsatz von WLAN, unkontrollierte getunnelte VPN-Verbindungen mit Laufwerkzugriff, die Nutzung von Skype und Instant-Messaging, Teamviewer und ähnlicher Werkzeuge, die den Zugriff von außen über Tunnel durch das Sicherheitsgateway hindurch auf Rechner im Intranet erlauben. Dazu kommt ein stark verändertes und oft wenig sicherheitsbewusstes Nutzerverhalten, uneinheitlich gestaltete Vergabe der Administrationsrechte für die am Intranet angeschlossenen Rechner, der Einsatz privater Rechner im Intranet und insbesondere auch die mobilen Rechner (Laptops), die innerhalb und außerhalb des Intranets des Krankenhauses betrieben werden.

3. Sollkonzept

Aus den genannten Gründen muss ein auf den bisherigen Empfehlungen beruhendes Sicherheits- und Netzkonzept dringend überdacht und geändert werden. Ziel dabei ist es, das nicht verhinderbare Risiko für die Sicherheit der Daten auf ein vertretbares Maß zu reduzieren und gleichzeitig eine größere Freiheit für den Internetzugriff zu ermöglichen.

Zur grundsätzlichen Lösung der Problematik ist das gängige Verfahren[7] die Aufteilung des Intranets in zwei Ebenen mit unterschiedlichen Schutzprofilen – hier „**klinisches Datennetz**“ und „**allgemeines KH-Netz“** genannt[8]. Der Einsatz eines Netzwerkzugangskontrollsystems und die zentrale Administration aller Rechner sind dabei wesentliche Beiträge zur Netzsicherheit; die zentrale Administration sollte aber auch in Erwägung gezogen werden, um personelle Ressourcen wirtschaftlich einzusetzen. Eine weitere Segmentierung der beiden Teilnetze – wie im folgenden vorgeschlagen – ist notwendig und erhöht die Sicherheit in entscheidendem Ausmaß.

Das **klinische Datennetz** ist ein besonders geschützter innerer Netzbereich, in dem die Medizinprodukte und Daten mit besonderem Schutzwert (Patientendaten, Mitarbeiterdaten, Daten klinischer Studien, Wirtschaftsdaten) liegen. Dieses Netz untergliedert sich in einen *Kernbereich* und einen *erweiterten Bereich*. Der Kernbereich ist räumlich eng lokalisiert und durch physische Zugangskontrolle geschützt, umfasst die Serverräume, insbesondere der zentralen IT-Abteilung und möglicherweise anderer zentraler Leistungserbringer, und erfüllt hohe Sicherheitsanforderungen. Zum erweiterten Bereich gehören alle dezentralen Geräte, auf denen Patientendaten liegen bzw. akquiriert werden, z. B. PDMS, POCT, auch reine klinische Arbeitsplatzrechner mit gar keinem oder sehr eingeschränkten Zugang zum Internet. Zur Absicherung des erweiterten Bereiches wird die Umsetzung folgender Maßnahmen (nach sorgfältiger Prüfung und Detailplanung) empfohlen:

- zentrale Administration der Rechner mit Sperren von CD/DVD-Laufwerken und USB-Schnittstellen,
- Einführung von zentralen Lese- und Brennstationen für den Austausch von Daten, dort auch Virenprüfung der eingelesenen Daten,
- ergänzende organisatorische Regelungen.

Im erweiterten Bereich sollten Subnetze

- für evtl. vorhandene Server für klinische Studien mit Patientendaten,
- für nicht im Kernbereich betriebene Medizingeräte,
- für WLAN-Zugänge für klinische Applikationen

[7] vgl. auch DIN EN 60601-1 3rd

[8] Diese Teilnetze entsprechen den Sicherheitsklassen B und A nach DIN EN 60601-1 3rd sowie den Schutzklassen B und A der neuen Norm E IEC / DIN EN 80001 für Medizinprodukte.

geeignet abgegrenzt werden. Separate Netze für Medizingeräte mit höchstem Schutzbedarf nach DIN EN 60601-1 (3rd Ed.) oder DIN EN 80001, Klasse C, gehören auch zum klinischen Datennetz, sind aber bis auf eventuelle Wartungszugänge nicht mit diesem verbunden[9]. Erforderliche Datenexporte aus dem klinischen Datennetz zu bestimmten, explizit definierten und besonders geregelten Zwecken, müssen auf kontrollierte Weise möglich sein.

Im **allgemeinen KH-Netz** stehen die Arbeitsplatzrechner, die einerseits als Zugangsrechner zum klinischen Datennetz und andererseits als allgemeine Arbeitsplatzrechner dienen. Dieser Bereich kann weniger restriktiv gehandhabt werden. Datensicherheit bedeutet aber auch die Sicherstellung der Verfügbarkeit der Zugangsrechner. Daraus resultiert, dass ein zentraler Schutz durch ein Sicherheitsgateway auch für das allgemeine KH-Netz vorhanden sein muss, jedoch kann dieses Sicherheitsgateway weniger restriktiv betrieben werden bzgl. der Filterung aktiver Inhalte. WLAN-Zugänge (z. B. für Patienten, Gäste, in Universitätskliniken auch für Studenten) sollen in abgetrennten Bereichen des allgemeinen KH-Netzes angesiedelt sein, die keine unkontrollierte Verbindung mit den übrigen Bereichen des allgemeinen KH-Netzes, aber eine ungehinderte Nutzung der nötigen Ressourcen im Internet erlauben.

Die physikalische Trennung dieser beiden Netze durch den Einsatz von Sicherheitsgateways und der Einsatz von virtuellen Zugängen (Remote Controlled Applications, virtuellen Desktops und ähnlichen Techniken) analog zum ReCoBS-Ansatz für die Nutzung von Ressourcen des klinischen Datennetzes aus dem allgemeinen KH-Netz heraus erfolgt in analoger Weise wie bei der vom BSI empfohlenen Internetnutzung. Als Systeme dafür denkbar sind neben Microsoft Terminalserver auch Citrix XEN-Server und VMWare-Lösungen, gegebenenfalls in Kombination. Eine für den Nutzer einfache und praktikable Lösung sollte bevorzugt werden.

Der Zugriff von außen kann liberaler gestattet werden, wenn die Möglichkeit eines Durchgriffs (außen → allgemeines KH-Netz → klinisches Datennetz) kontrolliert werden kann. Die Empfehlungen des BSI sollten bei der VPN-Implementierung für das Erreichen des notwendigen Sicherheitsniveaus berücksichtigt werden. Über VPN in das Kliniknetz eingebundene Remote-Rechner (z. B. für den ärztlichen Hintergrunddienst) sollten als Rechner in ein separat abgetrenntes Segment des allgemeinen KH-Netzes eingehängt werden; der Zugriff auf die Daten erfolgt dabei in gleicher Weise wie bei den lokalen Rechnern über Remote Controlled Applications. Für manche Anwendungen (z. B. radiologische Befundung) ist gegebenenfalls aus Performanzgründen eine dedizierte Lösung einzurichten. Die aktuelle Marktentwicklung im Bereich von Zugriffsportalen ist eng zu beobachten; hier sind künftig möglicherweise kostengünstige und sichere Lösungen verfügbar. Unabdingbar für den Einsatz einer solchen Lösung ist, dass beim externen Zugriff Daten aus dem klinischen Datennetz nur auf dem Bildschirm dargestellt, nicht aber auf den externen Rechner heruntergeladen werden. Für Fernwartungsarbeiten, z. B. an Medizingeräten, sollte ein ähnlicher Zugang vorgesehen werden, der kontrolliert freigeschaltet und überwacht werden kann.

Für den Mail-Zugriff wird die Einrichtung eines E-Mail-Kontos empfohlen, auf das auch von außen, evtl. mit Einschränkungen oder nur für gewisse Nutzer, Zugriff möglich ist und das im allgemeinen KH-Netz angesiedelt ist. Als Voraussetzung hierfür sollte der Versand von Patientendaten per E-Mail, auch klinikintern, unterbunden oder untersagt werden. Das wiederum setzt voraus, dass dafür andere geeignete Kommunikationsmöglichkeiten zur Verfügung stehen.

[9] Hierzu gehören z. B. Netze von Intensivstationen. Die Notwendigkeit einer Fernwartung impliziert, dass auch diese Geräte einen Netzzugang benötigen, der aber dann dediziert sein muss.

Die Sicherheit des Intranets des Krankenhauses, sowohl des klinischen Datennetzes als auch des allgemeinen KH-Netzes, ist als Service-Leistung der zentralen IT-Abteilung zu verstehen. Die IT-Nutzer des Krankenhauses sollten soweit wie möglich von eigener Sorge um die Sicherheit ihrer Geräte entlastet werden. Umgekehrt dürfen sie nicht durch unterschiedliches oder mangelndes Sicherheitsverständnis einzelner Kollegen gefährdet werden.

Die Sicherheit des Intranets eines Krankenhauses ist nicht durch technische Maßnahmen allein zu gewährleisten; ergänzend müssen organisatorische Maßnahmen vorgesehen werden. Diese umfassen eine vom Vorstand zu erlassende Policy, Betriebsvereinbarungen und Betriebsanweisungen, SOPs für sicherheitskritische Prozesse sowie ein etabliertes Risikomanagement[10]. Dazu gehört auch die Vereinbarung von Kontrollmaßmaßnahmen sowie dienst- und arbeitsrechtlicher Maßnahmen bei Verstößen.

4. Status dieser Empfehlung

Diese Empfehlung gilt zunächst bis Ende 2014 und soll spätestens dann auf Aktualität überprüft werden.

Obsolet werden mit dieser Empfehlung die Empfehlungen der AG DGI

- zum Internet-Anschluss von Krankenhäusern und Gesundheitsnetzen (überarbeitet Mai 2001),
- zu Modem-Verbindungen im Krankenhaus (Oktober 1998).

Danksagung

Wesentlicher Input zu dieser Empfehlung kam von der AG IT-Sicherheit der Universitätsmedizin Mainz sowie von den IT-Abteilungen und Datenschutzbeauftragten der Universitätskliniken Marburg, Gießen, Würzburg und Frankfurt.

[10] wie in den BSI-Empfehlungen und in der Medizinprodukte-Norm DIN EN 80001 beschrieben. Die Verfahrensschritte des Risikomanagements sind in ISO/IEC 27005 und DIN EN 14971 festgelegt. Allgemein ist für das IT-Sicherheitsmanagement die Norm ISO/IEC 27001 (und folgende) grundlegend.

Bemerkungen zur Nutzung von E-Mail im Gesundheitswesen

Erarbeitet von der GMDS-Arbeitsgruppe „Datenschutz in Gesundheitsinformationssystemen“

Für die Nutzung von E-Mail im Gesundheitswesen gibt es bereits Empfehlungen, die auch die Gesichtspunkte des Datenschutzes berücksichtigen. Zu nennen sind hier vor allem:

- Netzdienste im Gesundheitswesen (GMDS-Präsidiumskommission),
- Klinische Nutzung von E-Mail (GMDS-AG Internet).
- Leitlinien für den E-Mail-Versand im Gesundheitswesen (KV Bayern).

Daher werden hier nur einige Bemerkungen zusammengestellt, die zusätzlich zur Klärung von Fragen beitragen können.

Anwendungsfälle

Grundsätzlich ist beim Einsatz von E-Mail zu unterscheiden zwischen

1. Kommunikation zwischen Trägern des Gesundheitswesens (Ärzte, Krankenhäuser, Kassenärztliche Vereinigungen, Krankenkassen),
2. Kommunikation zwischen Forschergruppen (Ärzte, epidemiologische Register, medizinische Forschungsnetze, …),
3. Kommunikation mit Patienten.

Für den ersten Anwendungsfall kann auf der Basis vorhandener oder leicht zu installierender Infrastruktur ein angemessenes Sicherheitsniveau erreicht werden. Das gilt auch für den zweiten Fall, wobei hier die Möglichkeiten zur Anonymisierung und Pseudonymisierung zu nutzen sind. Für den dritten Anwendungsfall - Kommunikation mit Patienten - bestehen erhebliche Bedenken: Grundlegende Anforderungen des Datenschutzes können nicht erfüllt werden; daher ist E-Mail-Kommunikation hier nur einzelnen Ausnahmefällen annehmbar.
In jedem Fall sind natürlich die gesetzlichen Regelungen zur Weitergabe von personenbezogenen Daten zu beachten.
Zu beachten ist auch, dass das E-Mail-Protokoll die Zustellung nicht garantiert.

Sicherheitsgesichtspunkte

Bei der Beurteilung der nötigen Sicherheitsmaßnahmen für den E-Mail-Einsatz wird oft unterschieden zwischen geschlossenen Netzen, die vollständig unter Kontrolle einer Institution (z. B. Krankenhaus) oder eines Gesundheits-/Ärztenetzes stehen, und dem offenen Internet. Aber auch im ersten Fall bildet die Institution in der Regel keine informationelle Einheit. Außerdem sind schwache Sicherheitsmaßnahmen, was E-Mail betrifft, nicht einfacher in der Installation und der Handhabung. Daher ist diese Differenzierung wenig hilfreich. Auch im geschlossenen Netz eines Krankenhauses oder einer Institution sind Patientendaten z. B. vor der Netzverwaltung zu schützen. Bei einem Gesundheitsnetz kann auch schon der Zugang zu diesem, d. h. bis zum Einwahlknoten, eine Schwachstelle sein.
Zu beachten ist weiter, dass auch bei Kommunikation innerhalb eines Netzes (z. B. einer Universitätsklinik) nicht zwingend ausgeschlossen werden kann, dass die Datenströme nicht einen Umweg über die „Außenwelt“ nehmen oder gar außerhalb liegende Mail-Accounts verwendet werden.
Zu unterscheiden ist weiter zwischen

1. der Sicherheit der Übertragung
2. und der Sicherheit der beteiligten Endgeräte und Anwendungen.

In dieser Empfehlung wird nur der Punkt 1 behandelt. Das heikle und bei der gegenwärtigen Marktlage keineswegs gelöste Problem 2 ist Gegenstand anderer Empfehlungen; als Einstieg sei dafür verwiesen auf:

- Datenschutz und informationstechnische Sicherheit bei PCs (LfD Berlin)
- Sicherheitsmaßnahmen beim PC-Einsatz (BSI-Faltblatt)

Ferner muss unterschieden werden zwischen

1. der eigentlichen mit der E-Mail übertragenen Information (Nutzdaten)
2. und den Verbindungsdaten.

Schutz der Nutzdaten

Dass die Nutzdaten kryptographisch gesichert werden müssen (Vertraulichkeit und Echtheit), ist unstrittig und wird inzwischen weitgehend eingesehen. Zu verwenden ist hierbei die im jeweiligen Gesundheitsnetz oder der Institution vorhandene kryptographische Infrastruktur; in der Regel wird die Mail dann mit dem S/MIME-Protokoll verschlüsselt.
Bei der Stärke der Verschlüsselung sind zu unterscheiden:

- symmetrische Verfahren, die Schlüssellängen von mindestens 128 Bit erfordern,
- asymmetrische Verfahren mit zu fordernden Schlüssellängen von mindestens 2048 Bit (bei den gängigen Verfahren).

In der Praxis werden in der Regel sogenannte hybride Verfahren (z.B. in S/MIME oder PGP) eingesetzt, die beide Sorten von Verschlüsselung verwenden, und zwar das asymmetrische Verfahren zur Übermittlung von Einmalschlüsseln für das symmetrische Verfahren; hier müssen nätürlich beide Schlüssellängen unabhängig voneinander ausreichend gewählt werden.

Sind Verbindungsdaten schutzbedürftig?

Die Verbindungsdaten, die bei den Netz-Betreibern anfallen, sind bei der Kommunikation innerhalb und zwischen Institutionen des Gesundheitswesens, also etwa von Arzt zu KV, nicht besonders schützenswert. Anders wäre es bei einer Kommunikation mit Patienten. Hier ließe sich allein aufgrund der Verbindungsdaten auf die Tatsache der Behandlung eines bestimmten Patienten bei einem bestimmten Arzt schließen. Darüber hinaus würden sich in Log-Dateien Patientenlisten für die beteiligten Ärzte ansammeln, die mit einfachen Extraktionsmethoden ausgewertet werden könnten. Die Verbindungsdaten können beim Provider beschlagnahmt werden. Außerdem können Patientenlisten durchaus auch einen kommerziellen Wert haben.
Diese Information preiszugeben ist seitens des Arztes also ein Verstoss gegen die Schweigepflicht, die auch gegenüber dem Provider gilt.

Weitere Sicherheitshinweise

- Die interne Kommunikation im Gesundheitswesen oder innerhalb der Institution ist möglichst von der externen, vor allem von der privaten, zu trennen, am besten durch die Verwendung unterschiedlicher Rechner und Mail-Accounts. Insbesondere ist die Weiterleitung an einen eigenen privaten Account, etwa um dienstliche E-Mail auch zu Hause bearbeiten zu können, nicht ohne weiteres zulässig.

- Mail, sowohl versendete als auch empfangene, sollte stets verschlüsselt gepeichert werden; in Frage kommt hier auch die Klartextspeicherung in einem verschlüsselten Dateisystem.
- Es ist auch auf sicheres Löschen zu achten; insbesondere sind Mail-Dateien im Papierkorb nicht gelöscht.
- Eine in Praxis- oder Krankenhaussoftware integrierte E-Mail-Funktion sollte nur dann verwendet werden, wenn sie die vorhandene kryptographische Infrastruktur einbindet, und zwar mit starker Verschlüsselung.
- Verschlüsselung schützt nicht vor der Übertragung von Viren und Schadprogrammen, im Gegenteil: Virenfilter beim Provider oder in einem Firewall können das mitverschlüsselte Schadprogramm ja gar nicht erkennen. Daher ist es wichtig, dass der Endnutzer sich selbst um einen wirksamen Virenschutz kümmert.
- Die Verwendung von Multimedia-Mail, auch von HTML-formatierter Mail, ist zu vermeiden, auch innerhalb geschlossener Netze. Zwar lassen sich deren Gefahren durch sorgfältige Handhabung vermindern; das ist aber nur unter der unrealistischen Annahme umsetzbar, dass alle Kommunikationspartner das gleiche Sicherheitsniveau einhalten. Insbesondere sollten Office-Dateien (Textverarbeitung, Tabellenkalkulation usw.) so lange nicht verschickt werden, wie die Anbieter dieser Software nicht Vorkehrungen für einen sicheren Dokumentenaustausch vorsehen. Die Gefahr besteht
    - einerseits im unbeabsichtigten Versand versteckter (z.B. scheinbar gelöschter) Daten, die in Office-Dokumenten reichlich vorhanden sind,
    - andererseits im unbeabsichtigten Empfang mitverschickter Makroviren.

E-Mail-Kommunikation mit Patienten?

Das bereits erwähnte Problem der Verbindungsdaten, das beim gegenwärtigen Stand der Informationstechnik nicht mit angemessenem Aufwand lösbar ist, spricht gegen die E-Mail-Kommunikation mit Patienten.
Ferner ist aber auch in der Regel nicht anzunehmen, dass Patienten die nötigen Kenntnisse haben, E-Mail sicher zu empfangen und zu speichern. Auch routinierte Internet- und Mail-Benutzer haben meist noch erhebliche Wissenslücken im Bereich der IT-Sicherheit. Hier muss der Arzt an seine Fürsorgepflicht erinnert werden. Da ihm eine umfassende Schulung seiner Patienten in Sicherheitsfragen nicht zuzumuten ist, sollte der E-Mail-Versand besser ganz unterbleiben. Allenfalls auf ausdrücklichen Wunsch des Patienten könnte man evtl. eine Terminvergabe per Mail mitteilen, auf keinen Fall aber sensible Informationen.
Zwar wäre sogar die unverschlüsselte Kommunikation aufgrund einer schriftlichen Einwilligungserklärung des Patienten rechtlich nicht anfechtbar; insgesamt muss aber davon abgeraten werden, dass der Arzt mit seinen Patienten per E-Mail kommuniziert.

---

23. Oktober 2001. Letzte redaktionelle Änderung: 6. Januar 2002.

Sicherheitsempfehlungen zum Betrieb von Servern und lokalen Netzen in Krankenhäusern

Erarbeitet von der GMDS-Arbeitsgruppe „Datenschutz in Gesundheitsinformationssystemen“

Lokale Netze und Client-Server-Systeme mit den Serverbetriebssystemen Windows (NT, 2000, XP) oder Unix (Linux oder andere Varianten) werden immer häufiger in Krankenhäusern eingesetzt, meist zusätzlich zu einem zentralen Patientendaten-Verwaltungssystem. Dabei treten durch mangelnde Fachkenntnis und zeitliche Überlastung des IT-Personals, aber auch aufgrund von Sicherheitslücken in den Server-Betriebssystemen, Sicherheitsprobleme auf, die wirksamen Datenschutz verhindern. Die Konfiguration eines einigermaßen sicheren lokalen Netzes ist komplex und aufwendig. Dieser Aufwand ist aber aufgrund der Datenschutzvorschriften unumgänglich, sobald Patientendaten auf dem Server oder dem Netz gespeichert oder verarbeitet werden; er sollte auch in allen anderen Fällen im eigenen Interesse nicht gescheut werden und erfordert in jedem Fall eine Vollzeitstelle für einen Systemverwalter. In dieser Empfehlung kann das Thema bei weitem nicht erschöpfend behandelt werden. Nicht behandelt wird auch die Sicherheit von Arbeitsplatzrechnern; hierzu wird auf

- Datenschutz und informationstechnische Sicherheit bei PCs (LfD Berlin) [http://www.datenschutz-berlin.de/infomat/pc/index.htm]
- Sicherheitsmaßnahmen beim PC-Einsatz (BSI-Faltblatt) [http://www.bsi.bund.de/literat/faltbl/002_sipc.htm]

verwiesen. Ebenfalls nicht behandelt wird die Sicherheit der angebotenen Dienste und Anwendungen; für HTTP-Server wird auf

- Die Einrichtung sicherer HTTP-Server (Kompetenznetz Pädiatrische Onkologie und Hämatologie) [http://www.kompetenznetz-paed-onkologie.de/prjb/ServerSSL.html]

verwiesen.

Grundsätzliches zur Sicherheit von Server-Betriebssystemen

Auf einem unsicheren Betriebssystem kann man keinen sicheren Server aufsetzen. Daher ist der Sicherung des Betriebssystems große Sorgfalt zu widmen. Prinzipiell lassen sich die gängigen System-Plattformen hinlänglich sicher konfigurieren, wobei der Aufwand nicht unterschätzt werden sollte. Die Wahl zwischen Windows NT/2000/XP oder einem gängigen Unix-System (z.B. Linux) sollte in erster Linie vom vorhandenen Know-How bestimmt werden.
Windows NT (und seine Nachfolger 2000 und XP) wird oft als sicheres Betriebssystem angepriesen. In der Tat bietet NT einige Sicherheitsmechanismen, die für IT-Betreiber, die MS-DOS, Windows 3 oder Windows 95/98/ME gewöhnt sind, sehr eindrucksvoll wirken. Dieser Eindruck ist aber irreführend, zumal die Systemvoreinstellungen nur wenige der möglichen Sicherheitsschranken in Kraft setzen. Ebenso wird die Sicherheit eines Servers, besonders bei Windows-Systemen, durch Installation und Betrieb von Anwendungssoftware in der Regel unterlaufen; manche Anwendungssoftware funktioniert sogar nur mit unsicheren System-Einstellungen. Auch die durch die Benutzungsoberfläche, besonders ab NT-Version 4.0, suggerierte Leichtigkeit der Konfiguration ist irreführend und gefährlich, da sie Nachlässigkeit provoziert. Hinzu kommt bei Windows-Systemen, dass beim Einspielen von Bugfixes und »Service-Packs« oft sorgfältig konfigurierte Sicherheitseinstellungen zurückgesetzt werden.
Unix-Systeme sind im Gegensatz dazu für den erfahrenen Systemverwalter übersichtlicher. Die

Einarbeitungszeit ist zwar möglicherweise etwas länger, dafür sind aber die Systemprozesse und Fehlerbehebungsvorgänge wesentlich leichter unter Kontrolle zu halten, und die Konfiguration ist deutlich leichter nachvollziehbar; der Server ist damit insgesamt leichter sicher zu halten. Im Zweifelsfall ist daher ein Unix-System vorzuziehen. Wichtig ist in jedem Fall eine Härtung des Servers. Das bedeutet unter anderem:

- Einspielen aller aktuellen Patches, Schließen aller bekannten Sicherheitslücken. Hier sind vor allem die Hinweise des CERT/CC laufend zu beachten. Bei Windows-Systemen ist anschließend eine genaue Kontrolle und gegebenenfalls Restaurierung aller vorher getätigten Sicherheitseinstellungen nötig.
- Deaktivieren aller nicht benötigten Dienste (File-Sharing/NFS, FTP, Mail, Telnet, RAS, RPC, …) - jeder nicht benötigte, vergessene Dienst ist ein potentielles Sicherheitsrisiko.
- Aufstellen des Servers in einem gesicherten, nicht allgemein zugänglichen Bereich.
- Verwenden eines kryptographischen Dateisystems für Dateien und Datenbanken mit personenbezogenen Daten. Unter Linux kann ein entsprechender Treiber eingebunden werden, siehe
    - The Linux Encryption-HOWTO Homepage [http://encryptionhowto.sourceforge.net/]
      Unter Windows ist PGPdisk oder ScramDisk zu empfehlen:
    - PGPdisk [http://www.pgpi.org/products/pgpdisk]
    - ScramDisk [http://www.scramdisk.clara.net/]
      Von der mit neueren Windows-Systemen mitgelieferten Dateisystem-Verschlüsselung ist wegen gravierender Mängel abzuraten.
- Soll ein HTTP-basierter Service angeboten werden, sollte man den Internet Information Server (IIS) vermeiden. Auch unter Windows ist der Apache-Server die sicherere Lösung.
- Administration des Servers nur über die Konsole. Falls die Administration über einen Netzzugang nicht zu vermeiden ist, sollte ein kryptographisch gesichertes Protokoll verwendet werden, also z. B. im Unix-Bereich nicht Telnet, sondern SSH, das in den üblichen Distributionen enthalten ist oder leicht nachgerüstet werden kann; Quelle im WWW hier. SSH -Clienten sind auch für Windows-Systeme kostenlos erhältlich. Auch eine VPN-Verbindung ist bei passender Konfiguration geeignet.

Weitere Hinweise zur Serverhärtung findet man im WWW:

- Linux Security HOWTO [http://www.linuxdoc.org/HOWTO/Security-HOWTO.html]
- The Bastille Linux Hardening System [http://www.bastille-linux.org/]
- Hardening OpenBSD Internet Servers (GeodSoft Website Consulting) [http://geodsoft.com/howto/harden]
- Deaktivieren von Diensten unter W2K [http://www.kssysteme.de/htdocs/documents/w2kservices1.html]
- Windows 2000 Security Recommendation Guides (NSA) [http://nsa2.www.conxion.com/win2k]
- Hardening Windows 2000 (Phil Cox, System Experts) [http://www.systemexperts.com/win2k/HardenWin2K.html]
- Building a Windows NT bastion host in practice [http://people.hp.se/stnor]

Das angestrebte Sicherheitsniveau sollte mindestens dem „mittleren Schutzbedarf“ im

- Grundschutzhandbuch [http://www.bsi.de/gshb] des BSI

entsprechen, soweit möglich auch darüber hinausgehen.
Um über aktuelle Sicherheitsfragen stets auf dem laufenden zu sein, sollte der Systemverwalter mindestens eine einschlägige Usenet-Newsgruppe oder Mail-Liste verfolgen.

Sicherheitsratschläge für Aufstellung und Konfiguration von Servern

Um die Sicherheitsmechanismen des Betriebssystems wirkungsvoll einzusetzen, ist eine ausführliche Planung, insbesondere der Zugriffsrechte, und eine sehr sorgfältige Umsetzung nötig. Das Prinzip der minimalen Rechte sollte bei der Zugriffsregelung strikt beachtet werden. Im Netz sollte genau festgelegt werden, welcher Rechner in welche anderen welches Ausmaß an Vertrauen setzt und welche Ressourcen an ihn freigegeben werden. Ebenso sollten die Benutzer-Zugriffsrechte auf Ressourcen und Shares in einer Rechte-Matrix spezifiziert werden.
Es sollte stets eine ausgedruckte Version der System-Konfiguration einschließlich Vernetzungsplan und eine exakte Beschreibung der Sicherheitspolitik („Policy“, „Systemrichtlinien“) zur Hand sein. Die Konfiguration sollte sorgfältig dokumentiert sein, insbesondere die Sicherheitsmaßnahmen. Eine Auswahl wichtiger Sicherheitsmaßnahmen ist:

- Server sind physisch geschützt aufzustellen, z.B. in einem verschlossenen Raum.
- Es ist sicherzustellen, dass unbefugte Benutzer nicht ein alternatives Betriebssystem booten können. Geeignete Maßnahmen hierfür sind: ◦Aufstellung in einem verschlossenen Raum,
    - verschließbares Sicherheitsgehäuse,
    - keine Installation anderer Betriebssysteme oder Betriebssystem-Versionen auf anderen Partitionen,
    - Entfernung oder Verschluss der Diskettenlaufwerke,
    - Einschränkung der Boot-Möglichkeiten in der Hardware-Konfiguration,
    - Setzen eines Hardware-Passworts (nicht geeignet, wenn autoboot für den Server notwendig ist),
    - ◦Setzen des Boot-Timeouts auf 0 Sekunden;
      sie können einzeln oder in sinnvoller Kombination angewendet werden.
- Die Benutzerkennung „Gast“ ist stillzulegen, ebenso die Gruppe Gäste ; letzteres geht nur, wenn auf dem System nicht der Internet Information Server laufen soll.
- Die CD-Autoplay-Funktion ist abzuschalten.
- Die Protokollierung ist, soweit sinnvoll, einzurichten. Um die Balance zwischen der Aufzeichnung wichtiger sicherheitsrelevanter Vorgänge und der Erzeugung einer nicht mehr überblickbaren Datenflut zu wahren, sind dazu sorgfältige Detail-Überlegungen nötig. Zugriff auf Log-Dateien sollte nur der Administrator haben. Da NT die Protokollierung stillschweigend einstellt, wenn eine Log-Datei voll ist, ist die Größe dieser Dateien stets sorgfältig zu kontrollieren.
- Der Zugriff auf die Konfigurations-Datenbank (Registry) ist soweit wie möglich einzuschränken.
- Auf Systemverzeichnisse (z.B. \winnt) und deren Unterverzeichnisse dürfen gewöhnliche Benutzer und Prozesse nur Lesezugriff haben.
- Da Backup-Operatoren Lese- und Schreibzugang zum gesamten Dateisystem haben, ist der berechtigte Personenkreis eng einzugrenzen; es sollte eine besondere Benutzer-Kennung dafür verwendet werden, deren Rechte genau an die Aufgabe angepasst sind.
- Für alle Benutzer, auch die voreingestellten, sind Passwörter zu setzen. Die Auswahl von Trivial-Passwörtern sollte verhindert werden (Passfilt.dll ab NT 4.0 mit SP2 verfügbar).
- Als Maßnahme gegen das systematische Ausprobieren von Passwörtern sollten folgende Vorkehrungen getroffen werden: ◦Konto sperren nach 3 ungültigen Fehlversuchen.
    - Konto zurücksetzen nach 30 Minuten (das betrifft den Fehlversuchs-Zähler).
    - Dauer der Sperrung: Für immer (bis der Administrator sie aufhebt).
      Unter Windows macht man das im Benutzer-Manager unter „Richtlinien“, „Konten“.

Sicherheitsratschläge für den Systemadministrator

- Systemverwalter sollten eine Benutzer-Kennung mit Administrator-Rechten nur für wirkliche Verwaltungsaufgaben nutzen. Für Arbeiten, die nicht die vollen Privilegien benötigen, sind

gewöhnliche Benutzer-Kennungen zu verwenden. Insbesondere sollte unter Administrator-Rechten nicht mit Anwendungen gearbeitet werden, die für das Einschleusen von Schadprogrammen anfällig sind, wie die MS-Office-Anwendungen, E-Mail oder WWW-Browser.
- An Servern sollte, außer für Administrator-Aufgaben, nicht lokal gearbeitet werden.
- Bei der Unterbrechung von Systemadministrator-Arbeiten sollte ein Logout ausgeführt oder die Arbeitsstation gesperrt werden (unter Windows im Task-Manager ([Strg]+[Alt]+[Entf])).
- Um das Aussperren des Systemverwalters und als Folge möglicherweise eine längerdauernde Nichtverfügbarkeit des Rechners oder einzelner Dienste (`denial of service'-Attacke) zu verhindern, darf es für Administrator bzw. root keine Passwortsperre nach mehreren Fehlversuchen geben. Daher sollte man dessen Logon nur lokal zulassen.
- Um auch in Notfällen Administrator-Aufgaben wahrnehmen zu können, sollte das Administrator-Passwort in einem versiegelten Umschlag an sicherer Stelle, z.B. in einem Safe, hinterlegt werden. Gleiches gilt für ein eventuelles Hardware-Passwort und für Schlüssel zu Zugangstüren oder Rechnergehäuse.
- Eine Anmeldung über das Netz oder gar über eine unverschlüsselte Fernverbindung (mit RAS-Berechtigung) ist unter Sicherheitsgesichtspunkten besonders kritisch zu werten. Als mögliche Sicherheitsmaßnahme unter Windows können im Benutzer-Manager unter „Benutzerrechte“ in der Rubrik „Zugriff auf diesen Computer vom Netz“ die Gruppen „Administratoren“ und „Jeder“ entfernt werden. Eine weitere, damit allerdings nicht zu vereinbarende, Maßnahme ist die Einrichtung einer anderen Kennung mit Administrator-Rechten, für die der Zugang über das Netz möglich ist, allerdings die Passwortsperre bei Fehlversuchen funktioniert.
- Als Logon-Möglichkeit über das Netz sollte nur ein verschlüsseltes Protokoll (SSH unter Unix) zugelassen werden.
- Mitarbeiter sollten auf ihren Arbeitsplatzrechnern keine, auch nicht die lokale, Administrator-Berechtigung erhalten; Ausnahmen sind nur bei besonderen Systemkenntnissen möglich.

Die gelegentlich gehörte Empfehlung, die Administrator-Kennung mit einem anderen Benutzernamen zu versehen, ist weitgehend nutzlos, da NT-Rechner auf mehreren Wegen bereitwillig die Kennung des Administrators verraten.

Weitere Verweise ins Internet

- Vergleich der Betriebssysteme:
  - The Philosophy of Security - Windows and Unix [http://www.techtv.com/cybercrime/features/story/0,23008,2382021,00.html] (by Simson L. Garfinkel)
  - Microsoft Windows NT Server 4.0 versus UNIX deutsche Übersetzung [http://www.lot-germany.com/magazin/unix-nt.htm]
  - Choosing an Operating System (CERT) [http://www.cert.org/tech_tips/choose_operating_sys.html]
  - ISS X-Force Database (Computer Threats & Vulnerabilities) [http://www.iss.net/xforce/]
- Unix:
  - Unix-Sicherheits-Tool USEIT (BSI) [http://www.bsi.bund.de/aufgaben/projekte/useitool/useit.htm]
  - UNIX Security Checklist (CERT) [http://www.cert.org/tech_tips/AUSCERT_checklist2.0.html]
  - UNIX Configuration Guidelines (CERT) [http://www.cert.org/tech_tips/unix_configuration_guidelines.html]
- Windows NT (und 2000): Bücher zum Thema „Sicherheit unter Windows NT bzw. 2000“ sind zwar zahlreich auf dem Markt, aber z.T. von zweifelhafter Qualität und oft nicht auf dem neuesten Stand. Aktueller und gründlicher kann man sich unter den folgenden WWW-Adressen informieren:

    - Orientierungshilfe und Checkliste für den datenschutzgerechten Einsatz von Windows NT (LfD Niedersachsen) [http://www.lfd.niedersachsen.de/dokumente/checkliste_windows_nt/windows_nt.html]
    - Datensicherheit bei der Installation und beim Betrieb von Windows NT (Bayern) [http://www.datenschutz-bayern.de/technik/orient/windownt.htm]
    - MS-Windows NT 4.0: Sicherheitsmaßnahmen und Restrisiken (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein) [http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/themen/edv/backup/backup02.htm]
    - Sicherheitstechnische Mindestanforderungen bei der Implementierung von Windows-NT-Betriebssystemen (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein) [http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/somak/somak98/sa98nt.htm]
    - MS-Windows NT 4.0: Resource Kit und Security Tools (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein) [http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/themen/edv/backup/backup03.htm]
    - MS BackOffice unter NT-Server 4.0 - eine datenschutzorientierte Analyse (LfD Hamburg) [http://www.hamburg.de/Behoerden/HmbDSB/material/backoff.html]
    - Security Advisor Program (Microsoft) [http://www.microsoft.com/security]
    - NTBugTraq Mailing List [http://www.ntbugtraq.com/]
    - NT Security - Frequently Asked Questions [http://www.it.kth.se/~rom/ntsec.html]
    - Windows NT/2000 Frequently Asked Questions [http://www.ntfaq.com/]
- Windows 2000:
    - Windows 2000 Security Recommendation Guides (NSA) [http://nsa2.www.conxion.com/win2k]
    - Windows 2000 Network and System Security [http://www.labmice.net/Security/default.htm]

---

21. Oktober 2001. Letzte redaktionelle Änderung: 26. Oktober 2001.

Sicherheitsempfehlungen zum Internet-Anschluß von Krankenhäusern und Gesundheitsnetzen

Erarbeitet von der GMDS-Arbeitsgruppe „Datenschutz in Gesundheitsinformationssystemen“

Einleitung

Die Kommunikation im Gesundheitswesen wird in zunehmendem Maße über das Internet abgewickelt; die Menge der im Internet angebotenen nützlichen medizinischen Informationen wächst immer weiter. Daher ist der Internet-Anschluss von Krankenhäusern und Arztpraxen weit verbreitet und kaum noch zu vermeiden.
Diese Entwicklung kollidiert aber mit den Datenschutz- und -sicherheitsanforderungen eines Krankenhauses oder einer Arzpraxis. Bei unvorsichtigem Direktanschluß sind alle Daten auf lokalen Rechnern und Netzen gefährdet; sie können ausgespäht oder von unbefugten Internet-Teilnehmern unbemerkt verfälscht werden. Diese berechtigten Sicherheitsbedenken haben viele Verantwortliche bisher von einem Anschluss an das Internet absehen lassen.
Die vom Internet ausgehenden Gefahren können wesentlich reduziert werden, wenn der Anschluss über ein sogenanntes Firewall-System vorgenommen wird. Dieses besteht aus einer Kombination von Routern mit einem Gateway-Rechner. Bei sorgfältiger Konfiguration kann dieses Vorgehen als ausreichende Sicherheitsvorkehrung gegen Angriffe aus dem Internet angesehen werden. Datenschutz und Sicherheit im lokalen Netz werden dadurch aber in keiner Weise verbessert; hierfür sind gesonderte Maßnahmen erforderlich, die Gegenstand weiterer Empfehlungen dieser GMDS-Arbeitsgruppe sind oder sein werden.
Für Arztpraxen sollte der Internet-Zugang nur über ein geschlossenes Ärztenetz oder regionales Gesundheitsnetz hergestellt werden, das nach außen durch ein Firewall-System geschützt ist. Das Ärztenetz selbst ist als »Intranet« zu behandeln; die interne Kommunikation ist von der externen möglichst strikt zu trennen, im Innern sind die informationellen Einheiten auch gegeneinander abzusichern. Ein solches Intranet kann durchaus mit Hilfe der VPN-Technik (Virtual Private Networks) über das offene Internet betrieben werden, wobei die Schutzmaßnahmen allerdings eine erhebliche Sachkenntnis erfordern.

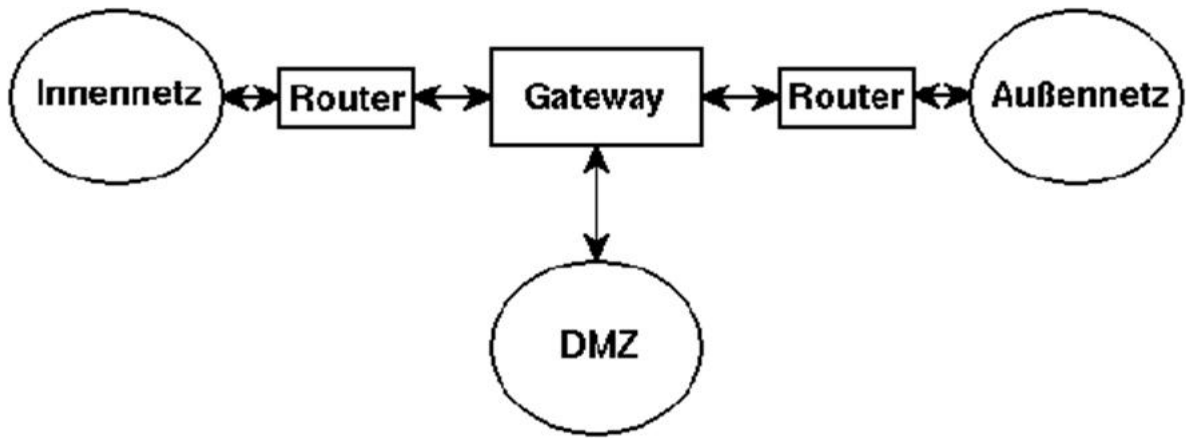
Grundsätze zur sicheren Internet-Anbindung

Die Anbindung an das Internet hat das Ziel: Möglichst komfortable Nutzung der Internet-Dienste bei möglichst großer Sicherheit vor unbefugten Zugriffen von außen. Es ist sorgfältig zu prüfen, welche Internet-Dienste wirklich benötigt werden. Die Arbeitsgruppe schlägt hierzu vor:

1. Außerhalb des durch den Firewall geschützten Bereiches dürfen keine personenbezogenen Daten gespeichert oder verarbeitet werden. Solche Daten dürfen bei der Übermittlung auch nicht den Außenbereich durchqueren.
2. Interaktive Dienste (Zugriff auf externe WWW-, Informations- oder Befundserver, telnet, ftp) sollen nur vermittelt werden, wenn die Kontaktaufnahme von der Klinik oder dem Ärztenetz in die Außenwelt erfolgt, nicht umgekehrt. Ausnahmen können für Krankenhäuser zugelassen werden, müssen dann aber einer strengen Überwachung unterliegen; eine sicherheitstechnisch akzeptable Lösung hierfür kann durch einen Modem-Server geschaffen werden. Sicherheitsempfehlungen der Arbeitsgruppe zu Modem-Verbindungen liegen vor.
3. E-Mail soll in beiden Richtungen möglich sein. Für eingehende Mail sind Filter gegen Schadprogramme (»Viren-Filter«) einzurichten. Bei ausgehender Mail sind die Datenschutzvorschriften zur Übermittlung sowie die ärztliche Schweigepflicht zu beachten.

Eine ausführlichere Empfehlung der Arbeitsgruppe zum Umgang mit E-Mail ist in Vorbereitung.

4. Erlaubt sollte nur das TCP/IP-Protokoll sein; andere Protokolle (z. B. Novell-IPX, NetBEUI) sollten gesperrt werden.
5. Dienste, die gefährliche Sicherheitslücken haben oder hohes Vertrauen zwischen den beteiligten Rechnern voraussetzen, werden gesperrt. (Beispiele: Filesharing, Terminalserver, Telekonferenzen).
6. Ebenso werden aktive Inhalte (Java, JavaScript und ActiveX) gesperrt, d. h. im Firewall ausgefiltert. Bei Java und JavaScript können für einzelne vertrauenswürdige Verbindungen Ausnahmen geschaltet werden.
7. Individuelle Verbindungen, die den Firewall umgehen, sind zu verhindern. Mögliche Ausnahmen sind in der entsprechenden Empfehlung zu Modem-Verbindungen formuliert.
8. Eigene Informationsangebote der Klinik oder des Ärztenetzes für externe Stellen (z. B. WWW - oder FTP-Server, Befundserver) sind in der »entmilitarisierten Zone« (DMZ) des Firewall-Systems anzusiedeln (siehe die Abbildung unten). Hier sind selbstverständlich die Datenschutzvorschriften zu beachten; insbesondere ist ein wirksamer Zugriffsschutz einzurichten, wenn personenbezogene Daten bereitgestellt werden sollen. Ein solcher Server ist unbedingt mit SSL zu betreiben, damit Informationen und Passwörter kryptographisch verschlüsselt übertragen werden.
9. Eigene Mail-Server sollen hinter dem Firewall-System - d. h. im Innenbereich - angesiedelt sein, damit der interne Mail-Austausch nicht über externe Netzsegmente geleitet wird.
10. Für die entsprechend den Anforderungen des Gesundheitswesens an externe Stellen zu übermittelnden Daten sind kryptographische Verschlüsselungsprogamme zu verwenden.
11. Die Systemverwaltung der Firewall-Komponenten darf nur über einen gesicherten Zugang (vertrauenswürdigen Pfad) möglich sein, am besten nur an der Konsole des jeweiligen Systems.
12. Für den Betrieb von Firewall-Systemen sind betriebsintern klare Richtlinien und Zuständigkeitsregelungen zu definieren. Diese sollen auch Vorschriften über die Protokollierung, die Behandlung von sicherheitsrelevanten Ereignissen und Sanktionen bei Sicherheitsverstößen enthalten.
    Die dem Stand der Technik entsprechende Konfiguration ist:



Dabei wird der Gateway auf Anwendungsebene betrieben („Application Gateway“ mit Proxies für alle zugelassenen Dienste); die Router arbeiten als Paketfilter. Die dabei auftretende Redundanz in den Sicherheitsmaßnahmen ist erwünscht. Der Gateway kann im übrigen je nach dem benötigten Durchsatz auf mehrere parallel geschaltete Rechner verteilt sein.

Diskussion der Vorschläge

1. Das folgt aus den Datenschutzvorschriften und der Schweigepflicht. Ausnahmen sind kryptographisch gesicherte und kontrollierte Kommunikationsverbindungen im

Behandlungszusammenhang mit zulässigen Partnern, die ein gleichwertiges Sicherheitsniveau einhalten.

2. Wichtig ist vor allem die Verhinderung von Hacker -Angriffen, die im Internet häufig automatisiert, auch mit frei verfügbarer Software, durchgeführt werden; auf einem ans Netz angeschlossenen Unix- oder Windows/NT-System genügt dann ein schwaches Passwort eines einzigen Benutzers als Einfallspforte, selbst wenn dieser nur beschränkte Zugriffsrechte hat; MS-DOS/Windows-95/-98/-ME-Rechner sind meist schon dann völlig ungeschützt, wenn auf ihnen überhaupt ein Netzprogramm gestartet wird. Und ein ungeschützter Rechner im Intranet reicht bereits aus, um die Sicherheit des ganzen Netzes erheblich zu gefährden.
3. Die Nutzung von E-Mail ist fundamental für einen erfolgreichen Einsatz des Internets. Dennoch ist die unbeschränkte Freigabe des E-Mail-Dienstes nicht ohne Probleme. Zunächst verhindert die vorgeschlagene Regelung nicht, dass Mitarbeiter des Krankenhauses oder Teilnehmer des Ärztenetzes auf diesem Weg unbefugt Daten nach außen schmuggeln . Ein entsprechendes Verbot sollte in die Verpflichtungserklärung aufgenommen werden; darüber hinaus kann die Nutzung von E-Mail auf bestimmte Mitarbeitergruppen eingeschränkt werden. Ein weiteres Problem ist die codierte (z. B. chiffrierte) Zusendung von Viren und anderen Schadprogrammen von außen an Mitarbeiter des Krankenhauses oder Teilnehmer des Ärztenetzes, insbesondere bei Verwendung von Multimedia-Mail (MIME); diese können im Firewall wegen der Codierung nicht erkannt und folglich nicht ausgefiltert werden. Es ist darauf hinzuwirken, dass alle E-Mail-Berechtigten mit dieser Gefahr vertraut sind und nicht unbedacht Programme, Macros o. ä. starten, die auf diesem Weg zu ihnen gelangt sind.
4. Zur Nutzung der Internet-Dienste reicht das TCP/IP-Protokoll aus. Die anderen Protokolle sind nur für lokale Netze geeignet, da sie voraussetzen, dass alle Rechner im erreichbaren Netz vertrauenswürdig sind. Ist das Internet über diese Protokolle erreichbar, entstehen gefährliche Sicherheitslücken.
5. Solche Sicherheitslücken entstehen auch durch einige TCP/IP-Dienste. Die Windows-Dateifreigabe, analog NFS unter Unix, erlaubt den durchsichtigen Zugriff auf Dateien anderer Rechner und beruht ebenfalls auf dem Vertrauen in den Fremdrechner. Terminal-Server-Dienste wie ICA/WinFrame oder das X-Protokoll unter Unix ermöglichen interaktive Sitzungen auf fremden Rechnern mit grafischer Benutzungsoberfläche; wegen ihrer Sicherheitsprobleme können sie nur zugelassen werden, wenn sie mit einem sicheren Protokoll wie z.B. SSH gekoppelt werden.
6. Aktiven Inhalten, dynamischem HTTP u. dgl. wird zur Zeit mit sehr viel Euphorie begegnet. Sinnvolle Anwendungen im Internet sind denkbar, aber bisher kaum zu finden. Dagegen können die vorhandenen Sicherheitsmängel leicht ausgenutzt werden. Bei diesem Konzept werden unbekannte Programmanweisungen unkontrolliert vom externen Server auf den Rechner des Benutzers geladen und sofort ausgeführt. Dies verstößt gegen ein elementares Sicherheitsprinzip und ist untragbar. Daher ist der Gateway mit einer Sperre für Java, JavaScript und ActiveX sowie mit einem Virenfilter auszustatten.
7. Immer wieder wird versucht, Direktverbindungen unter Umgehung des Firewalls zu schalten; Argument ist dabei die Bequemlichkeit einiger Vorgänge wie Fernwartung, Programm-Update oder Direktzugriff auf Informationen. Solche Verbindungen schaffen eine zusätzliche Route ins interne Netz und machen das gesamte Sicherheitskonzept hinfällig. Zur Problematik der Fernwartung gibt es Stellungnahmen der Datenschutzbeauftragten sowie Formulierungshilfen der Arbeitsgruppe.
8. Da der Gateway-Rechner aus Sicherheitsgründen möglichst einfach gehalten werden soll, empfiehlt es sich nicht, ihn mit Server-Prozessen zu belasten. In der DMZ sind Server durch den Firewall geschützt; andererseits wirkt sich ein Einbruch in einen solchen Rechner nicht auf das gesamte Innennetz aus.
9. Sind einer oder mehrere Mail-Server im Innennetz eingerichtet, ist ein Gateway für das SMTP -Protokoll nötig; alternativ kann auch ein Mail-Server in der DMZ betrieben werden, der dann allerdings eine vollständige Benutzerverwaltung für das gesamte Innennetz besitzen muss.
10. In erster Linie geeignet sind die Verfahren SSL (für Client-Server-Kommunikation) und PGP für E-Mail. Entsprechende kryptographische Infrastrukturen (PKI) sind an vielen Stellen im Aufbau, die Verfahren können und sollten aber auch unabhängig davon genutzt werden.

11. Ein Zugang über das Netz, der nur mit einem Passwort geschützt ist, ist zu unsicher.
12. Vorschläge für solche Richtlinien werden von der Arbeitsgruppe noch erarbeitet.

Durch dieses Konzept wird der völlig freie Internet-Zugang zugunsten der Sicherheit etwas behindert; die Unannehmlichkeiten halten sich aber in Grenzen und müssen im Hinblick auf Datenschutz- und Sicherheitsanforderungen einer Klinik oder eines Ärztenetzes in Kauf genommen werden.
An größeren Kliniken oder in Gesundheitsnetzen mit geschultem informationstechnischen Personal sind Abweichungen von diesen Vorschlägen denkbar, wenn sie auf einer definierten Sicherheitspolitik beruhen und in ihren Auswirkungen beherrscht werden. So ist es bei geeigneten baulichen Voraussetzungen durchaus möglich, für einen Teil des Netzes, auf dem dann aber keine personenbezogenen Daten gespeichert oder verarbeitet werden dürfen, einen weniger restriktiven Internet-Anschluß zu schalten; die Kommunikation zwischen diesem Bereich und dem stärker geschützten muss mit besonderer Sorgfalt geregelt werden.
Abschließend sei noch einmal ausdrücklich auf die Gefahren hingewiesen, vor denen ein Firewall-System nicht schützen kann: Sicherheitsverstöße im Innennetz, Umgehung durch direkte Netzverbindungen, Schadprogramme, sofern sie verschlüsselt eingeschleust werden, Angriffe und Fehler auf der Ebene der Anwendungssoftware, menschliches Versagen und neue oder unbekannte Gefahren.

Literatur und Internet-Quellen

- William R. Cheswick, Steven M. Bellovin, Firewalls and Internet Security, Addison-Wesley, Reading, Mass., 1994, ISBN 0-201-63357-4.
- D. Brent Chapman, Elizabeth D. Zwicky, Building Internet Firewalls O'Reilly, 1995, ISBN 1-56592-124-0.
- Karanjit Siyan, Chris Hare, Internet Firewalls and Network Security, NRP, ISBN 1-56205437-6.
- Uwe Ellermann, Firewalls, DFN-Bericht Nr. 76, Berlin 1994. (Bezugsquelle (kostenlos): DFN -Verein, Pariser Str. 44, 10707 Berlin)
- Marit Köhntopp, Martin Seeger, Lukas Gundermann, Firewalls - Konzept, Design und Aufbau, Computerwoche, München 1998.

Internet-Quellen des Original-Artikels Stand heute (2013-08-20) nicht mehr verfügbar.

Autoren: Prof. Dr. K. Pommerening, Dr. E. Scheidt, 21. August 1996. Überarbeitet am 5. Mai 2001. Letzte redaktionelle Änderung: 5. Mai 2001.

Formulierungshilfen für einen Fernwartungsvertrag aus der Sicht des Datenschutzes

Erarbeitet von der GMDS-Arbeitsgruppe „Datenschutz in Gesundheitsinformationssystemen“

Vorbemerkung

Die folgenden Klauseln sind als Formulierungshilfen gedacht und nur beispielhaft zu sehen. Sie ersetzen keine juristische Beratung.
Die Vertragspartner werden im folgenden

- Klinik und
- Firma

genannt, unabhängig davon, wer juristisch als Vertragspartner auftritt - z. B. „das Land XXX, vertreten durch den Verwaltungsdirektor des Klinikums YYY“.

Präambel

[Hier ist unter anderem klarzustellen, daß unvermeidbare Abweichungen von den im folgenden formulierten Vereinbarungen schriftlich zu fixieren und zu protokollieren sind und nur im Einverständnis beider Vertragspartner erfolgen können.]

1. Art und Umfang der Wartung

[Hier sind festzulegen:

- Das zu wartende System (Hard- und Software) mit Abteilungszugehörigkeit und Standort in der Klinik sowie die betroffenen Datenbestände;
- Art der Wartung (nur Fernwartung, nur vor Ort, beides) sowie Festlegung der Fälle, in denen Fernwartung betrieben werden darf;
- Beschreibung der Wartungsarbeiten, der Funktionalität und der technischen Gestaltung, z. B. welche Software-Updates vorgenommen werden sollen.
- Wartungsbereitschaft (z.B. permanent, Wochenende ausgeschlossen, Montag 6h bis Samstag 14h)]

2. Laufzeit

[Hier muß festgelegt werden, von wann bis wann der Vertrag gilt, bzw. ob er sich automatisch verlängert und wie er gekündigt werden kann.]

3. Vergütung

[…]

4. Rechtliche Konsequenzen

[Bei vorsätzlichen oder fahrlässigen Verstößen gegen diesen Vertrag haftet die Firma in Höhe des von der Klinik nachgewiesenen Schadens.]
[Hinweis auf datenschutzrechtliche und strafrechtliche Konsequenzen]
[Kündigungsrecht]

5. Datenschutzregelung

5.1 Die Firma befolgt die einschlägigen Bestimmungen des [zuständigen Datenschutzgesetzes] und unterwirft sich der Kontrolle durch die Klinik und durch die [für die Klinik zuständige Aufsichtsbehörde].
5.2 Die Firma sichert für sich bzw. ihre Mitarbeiter folgende Punkte im Zusammenhang mit der Fernwartungstätigkeit bei der Klinik zu:

- Die Firma kennt die Datenschutz-Richtlinie der Klinik zur Fernwartung (Anhang IV). Die Firma verpflichtet sich zur Einhaltung der darin enthaltenen Regeln.
- Die Mitarbeiter der Firma werden über die Regeln informiert und schriftlich zu deren Einhaltung verpflichtet. Insbesondere werden die Mitarbeiter zur Einhaltung des Datengeheimnisses nach [x des einschlägigen Gesetzes] und darauf verpflichtet, keine Informationen, die sie bei der Fernwartung erhalten, an Unbeteiligte weiterzugeben.

5.3 Die Firma dokumentiert die von ihr getroffenen aktuellen technischen und organisatorischen Datenschutzmaßnahmen in Anhang III. Anhang III ist Bestandteil dieses Vertrages. [Evtl. Anmietung eines Raums bei der Firma durch die Klinik]
5.4 Die Firma schult die für das in 1 genannte System zuständigen Mitarbeiter in den zur Erfüllung dieses Vertrages notwendigen Wartungsmaßnahmen und den zugehörigen Sicherheitsmaßnahmen und stellt dazu eine ausreichende schriftliche Dokumentation in deutscher Sprache zur Verfügung.
5.5 Die Mitarbeiter der Firma dürfen ohne Aufforderung durch einen verantwortlichen Klinikmitarbeiter weder daten-, konfigurations-, parameterverändernde noch Hardware-beeinflussende Aktionen unternehmen. Die Rechte der Mitarbeiter der Firma in Betriebs- sowie Anwendungssystem sind schriftlich festzulegen. Es dürfen nur erforderliche Rechte vergeben werden.

6. Technisch-organisatorischer Ablauf von Fernwartungsvorgängen

6.1 Fernwartungsarbeiten an dem in 1 genannten System werden nur von den im Anhang I aufgeführten festangestellten Mitarbeitern der Firma ausgeführt. Anhang I ist Bestandteil dieses Vertrages. Änderungen in der Liste der berechtigten Mitarbeiter der Firma treten in Kraft, sobald eine schriftliche Vereinbarung mit der Klinik getroffen ist. Ausnahmen in dringlichen Notfällen sind nur in Absprache mit dem Systemverantwortlichen der Klinik erlaubt; sie sind zu protokollieren. [Hier evtl. noch Regelung der Eskalation]
6.2 Die auf Seite der Klinik zuständigen Systemverantwortlichen sind in Anhang II dieses Vertrags benannt. Änderungen des Anhangs II treten in Kraft, sobald eine schriftliche Änderungsanzeige bei der Firma eingegangen ist.
6.3 Die Firma stellt die technischen Möglichkeiten zur Protokollierung aller Aktivitäten des Wartungsvorgangs zur Verfügung. Der Wartungsvorgang wird von der Firma so gestaltet, daß er auf der Konsole des in 1 genannten Systems mitverfolgt werden kann. Die Firma protokolliert den Anlaß und die im einzelnen durchgeführten Maßnahmen der Wartung und stellt der Kontaktperson der Klinik das Protokoll schnellstmöglich zur Verfügung. Das Protokoll wird mindestens 1 Jahr aufbewahrt.

6.4 Der Verbindungsaufbau oder die Fernwartungsfreigabe im Betriebs- oder Anwendungssystem muß durch Mitarbeiter der Klinik erfolgen [z. B. Einschaltung des Modems, Aktivierung der Benutzerkennung für die Wartung]. Wird die Verbindung eine gewisse Zeit nicht genutzt [zu vereinbarendes Zeitintervall: maximal 30 Minuten], wird der Verbindungsaufbau bzw. die Fernwartungsfreigabe durch die Klinik abgebrochen, sonst unverzüglich nach Ende der Wartungsarbeiten. Eine Fernwartung darf nur stattfinden, während Mitarbeiter der Klinik anwesend sind, die den Netzzugang/die Fernwartung sperren können und Mitarbeiter, die die ablaufenden Vorgänge und Änderungen kontrollieren können.
6.5 Vor Beginn einer Fernwartung absolviert der Mitarbeiter der Firma eine Anmeldeprozedur mit Authentisierung [mindestens Benutzerkennung und Paßwort; starke Authentisierung ist anzustreben].
6.6 Es ist sicherzustellen, daß für normale Wartungs- und Diagnosearbeiten kein Zugriff auf Patientendaten möglich ist außer in unumgänglichen Fällen. Die Lösung von Problemfällen hat vorrangig in Testumgebungen stattzufinden. Sollte ein Zugriff auf das Produktivsystem unabdingbar sein, hat dies unter bester Kontrolle durch die systemverantwortlichen Kliniksmitarbeiter und mit einer speziellen Nutzerkennung zu erfolgen. Vor der Einsicht in personenbezogene Daten holt der Mitarbeiter der Firma die Erlaubnis der in Anhang II dieses Vertrages benannten Systemverantwortlichen ein. [Ansonsten möglichst nur anonyme oder pseudonyme Daten] Die Übertragung personenbezogener Daten zur Firma per Dateitransfer oder Download ist verboten.
6.7 Bei der Fernwartung übertragene Daten werden keinem Dritten weitergegeben. Sie werden nur zu Wartungszwecken verwendet und nach Abschluß der Wartung oder Fehlersuche unverzüglich so gelöscht, daß sie nicht wiederherstellbar sind. Hardcopies oder Speicherung von patientenbezogenen Bildschirminhalten sind auszuschließen.
6.8 Die Fernwartung soll nicht von Arbeitsplätzen in Privatwohnungen aus durchgeführt werden. Ausnahmen in dringlichen Notfällen sind nur in Absprache mit dem Systemverantwortlichen der Klinik erlaubt und nur falls folgende Sicherheitsvorkehrungen getroffen sind: [noch zu ergänzen].

Anhang I

Liste der namentlich benannten berechtigten Mitarbeiter der Firma mit Telefonnummern
[als Anhang, da sie sich während der Vertragslaufzeit ändern kann]

Anhang II

Benennung der systemverantwortlichen Kontaktperson der Klinik und ihrer Stellvertreter
[ebenfalls mit Änderungsmöglichkeit]

Anhang III

Dokumentation der von der Firma getroffenen technischen und organisatorischen Datenschutzmaßnahmen.
[z. B. nach BDSG §9 + Anhang. Die Maßnahmen müssen adäquat sein, z. B. Sicherstellung, daß in den Geschäftsräumen der Firma keine Unbefugten Zugang zu Computern erlangen können, von denen aus Fernwartung betrieben wird; verschlüsselte Verbindung.]
[stets in Abstimmung mit der verantwortlichen Kontaktperson der Klinik aktuell zu halten]

Anhang IV

Datenschutz-Richtlinie der Klinik für Fernwartung.

Autoren: K. Pommerening, B. Hornung, M. Schurer, 21. April 1999. Letzte redaktionelle Änderung: 18. Oktober 1999.

Zugriff auf Patientendaten im Krankenhaus

Erarbeitet von der GMDS-Arbeitsgruppe „Datenschutz in Gesundheitsinformationssystemen“
Stand 21.4.1999

Ziel dieser Empfehlung ist eine Hilfestellung bei der Organisation der datenschutzkonformen Handhabung von elektronisch gespeicherten Patientendaten im Krankenhaus und bei der Erstellung eines Datenschutzkonzeptes. Insbesondere sollen Hinweise für die Umsetzung des Grundprinzips der sparsamen Datenerhebung und -verarbeitung gegeben und die Definition eines Regelwerks für Zugriffsrechte und Datenfreigabe erleichtert werden. Abweichungen von diesen Empfehlungen können aufgrund unterschiedlicher gesetzlicher Regelungen in den einzelnen Bundesländern notwendig sein. Abweichungen können auch je nach den lokalen Organisationsstrukturen sinnvoll sein. Sie erfordern dann aber eine Begründung, in der dem Patienten sonst drohender Schaden sowie durch die Abweichung entstehender Nutzen für den Patienten dargelegt sind, und müssen die konstituierenden Elemente des Datenschutzes im Krankenhaus, die ärztliche Schweigepflicht und das informationelle Selbstbestimmungsrecht des Patienten, wahren. Soweit einige der folgenden Empfehlungen in einem bestehenden System nicht unmittelbar umgesetzt werden können, sollte die entsprechende Anforderung an den Hersteller weitergegeben werden.
Papierakten und Registraturen müssen ebenfalls datenschutzkonform gehandhabt werden; die folgenden Empfehlungen beziehen sich jedoch nur auf elektronisch gespeicherte Patientendaten, weil hier, vor allem durch die rasante technische Entwicklung, ein erheblicher Regelungsbedarf besteht.

1. Grundsätze

Durch die Einführung von Informationstechnik im Krankenhaus mit dem dadurch ermöglichten einfachen, schnellen und multiplen Zugriff auf Patientendaten ergeben sich Datenschutzprobleme, die durch organisatorische Regelungen und Sicherheitstechnik gelöst werden müssen. Bisher beim Umgang mit der papierenen Patientenakte übliche Einsichtnahme- und Weitergabeverfahren können nicht ohne weiteres auf das rechnergestützte Krankenhausinformationssystem und die elektronische Patientenakte übertragen werden.
Aus dem Datenschutzrecht (siehe die Grundsatzerklärung der AG sowie die Stellungnahme für das Krankenhaus-Management) ergeben sich für die Zugriffsrechte auf Patientendaten im Krankenhaus die folgenden Grundsätze: Patientendaten dürfen nur im Rahmen der Zweckbestimmung des Behandlungsvertrages und den damit verbundenen gesetzlichen Regelungen erhoben und verarbeitet, nicht aber uneingeschränkt - d. h. über die unmittelbare Zweckbindung hinaus - ausgetauscht und verwendet werden, auch nicht innerhalb des Krankenhauses; das Krankenhaus ist in diesem Sinne keine informationelle Einheit. Das Prinzip der Erforderlichkeit ist hier streng zu beachten, das auch als Prinzip der minimalen Rechte oder need-to-know -Prinzip bezeichnet wird. Insbesondere ist hier zwischen dem Arzt und seinen berufsmäßig tätigen Gehilfen einerseits sowie den sonstigen Gehilfen andererseits zu unterscheiden. Das medizinische Fachpersonal als Produzent der Information trägt die Verantwortung für die korrekte Verwendung der Daten unter Berücksichtigung der Persönlichkeitsrechte der Beteiligten, insbesondere des Patienten, der Quelle (oder Urheber) der Information ist. Folglich kann nur der die Daten produzierende, das heißt, sie erhebende, Arzt bzw. der ärztliche Leiter der Fachabteilung die Rechte für den Zugriff auf die medizinischen Daten des Patienten und deren definierte Verwendung erteilen. Der Patient hat, sofern das zuständige Krankenhausgesetz wie etwa in Rheinland-Pfalz nichts anderes bestimmt, das Recht, Daten für bestimmte Zugriffe sperren zu lassen, wobei er auf eventuell für ihn entstehende Nachteile hinzuweisen ist; er hat andererseits auch ein Anrecht darauf, daß seine Daten zur rechten Zeit am

rechten Ort verfügbar sind, insbesondere nicht gegen seinen Willen oder seine Interessen zurückgehalten oder außerhalb der gesetzlichen Pflichten vernichtet werden.

2. Daten und Patientenakten

Unter einer Patientenakte wird im folgenden die Gesamtheit der über diesen Patienten gespeicherten Informationen verstanden, die in Form einer abgeschlossenen Dokumentation, z. B. von einem Arzt, verantwortet sind. Diese können in einer einheitlichen zentralen Datenbank oder in einem verteilten Krankenhausinformationssystem gespeichert sein. Die Patientenakte erstreckt sich über alle Behandlungszusammenhänge in diesem Krankenhaus. Wird der Patient (im Sinne des shared care) in mehreren Organisationseinheiten des Gesundheitswesens behandelt, führt jede solche Einheit eine eigene Patientenakte. Im Interesse des Patienten und unter Berücksichtigung seiner Einwilligung sind in diesem Fall analoge Datenweitergabe- und -zugriffsregelungen zu treffen, wie im folgenden für das Krankenhaus beschrieben.
Ein Behandlungszusammenhang beginnt mit der Aufnahme des Patienten und umfaßt Verlegungen, Mitbehandlung durch andere Fachabteilungen, Konsile und Leistungsanforderungen; er erstreckt sich auch über eventuellen Heimurlaub sowie über zusammengehörige ambulante Besuche. Er kann sich auch über Entlassung und Wiederaufnahme erstrecken, wenn diese der Fortsetzung einer bei einem früheren Aufenthalt begonnenen Behandlung dient.
Nicht zur Patientenakte gehören abteilungsinterne Daten, also in der behandelnden Fachabteilung über den Patienten angefallene nicht autorisierte Daten wie nicht befundete Röntgenbilder oder ähnliches; solche Daten sind aber selbstverständlich auch Patientendaten im Sinne der Datenschutzgesetzgebung und daher entsprechend zu schützen. Nicht zur Krankenakte gehören auch persönliche Arztnotizen. Es ist aber das Prinzip der ordnungsgemäßen Aktenführung zu beachten, d. h., es ist eine bearbeitungsgerechte, nachvollziehbare, auf sachlichen Prinzipien beruhende Struktur der abgespeicherten Daten anzustreben, um Behandlungsprozesse im Detail und im Kontext nachvollziehen zu können. Alles, was im Verlaufe der Behandlung an Daten erzeugt wird und derzeit relevant ist oder als künftig relevant erachtet wird, gehört in die Patientenakte.
Um die unterschiedlichen Zugriffsanforderungen und -befugnisse sowie Sensibilitätsstufen angemessen berücksichtigen zu können, sind folgende Arten von Daten zu unterscheiden, die alle dem Datenschutz und dem Arztgeheimnis unterliegen:

- Identifikationsdaten (Name, Geburtsdatum, Adresse, evtl. Krankenkassennummer, sowie krankenhausinterne Identifikatoren),
- administrative Daten:
    - Versicherungsdaten,
    - Bewegungsdaten,
    - weitere fallbezogene Daten, z. B. Wahlleistungen,
- medizinische Daten: ◦Notfalldaten,
    - allgemeine anamnestischen Daten,
    - abrechnungsrelevante Diagnosen und Therapien,
    - Befunde, Laborwerte und andere diagnostische und therapeutische Daten,
    - besonders sensible Daten (z. B. psychiatrische Daten, bestimmte Befunde),
    - genetische Daten.

Die Identifikationsdaten und administrativen Personendaten einschließlich Versicherungsdaten werden oft auch als Stammdaten bezeichnet. Die medizinische Daten sind gemäß der EU-Richtlinie zum Datenschutz weiter zu untergliedern. Zu den Patientendaten gehören auch Daten, die sich auf Angehörige, Bezugspersonen oder Dritte beziehen; dies können sowohl administrative als auch medizinische Daten sein.
Notfalldaten werden in der Patientenakte so gespeichert, daß der Zugriff auf sie unabhängig vom restlichen Teil der Patientenakte möglich ist. Zu den Notfalldaten gehören Daten, die zur Abwehr

einer Gefahr für Leben, körperliche Unversehrtheit oder persönliche Freiheit des Patienten für die mit der Untersuchung und Behandlung des Patienten befaßten Personen erforderlich sind (z. B. schwere Allergien). Sie sollen vollständig und unverzüglich in die Patientenakte eingetragen werden. Welche Daten als Notfalldaten gekennzeichnet werden, entscheidet der Arzt, bei dem sie produziert werden; Vorgaben dazu erläßt der Leiter der Fachabteilung (unter Berücksichtigung internationaler Festlegungen), ebenso wie Richtlinien, welche Daten als besonders sensibel einzustufen sind. Das Widerspruchsrecht des Patienten, sofern gegeben, bleibt unberührt.
Die Patientenakten prominenter Personen können auf deren Wunsch mit einer VIP-Kennzeichnung versehen werden und werden nur unter besonderen Einschränkungen freigegeben. Alternativ ist eine Speicherung unter einem Pseudonym möglich. Eine analoge Regelung ist für Kliniksmitarbeiter und deren Angehörige vorzusehen, wobei die Schutzmaßnahmen nach dem Prinzip der Verhältnismäßigkeit weniger streng sein können.

3. Zugriffsrechte

Daten werden in der Verantwortung der erhebenden Fachabteilung des Krankenhauses gespeichert und verarbeitet und sind vor dem Zugriff durch nicht autorisierte Mitarbeiter zu schützen. Die erhebende Stelle verantwortet die Zugriffsrechte auf diese Daten; somit können Rechte an Dritte stets nur gegeben (logische Überweisung) und, außer in Notfallsituationen, nie selbständig durch sie genommen werden. Die Datenhoheit einer Fachabteilung über die bei ihr erhobenen Daten gilt unabhängig vom Ort der Speicherung, auch, wenn diese in einer zentralen Datenbank erfolgt. Das Recht zur Einsicht und Verarbeitung der Patientendaten ist grundsätzlich an den Behandlungszusammenhang gebunden. Das Erscheinen des Patienten in einer anderen Fachabteilung ist, sofern ein Behandlungszusammenhang besteht, in der Regel als Zustimmung zum Zugriff auf die nötigen Daten der überweisenden Abteilung zu werten; aufgrund der informationellen Selbstbestimmung des Patienten kann höchstens dieser, nicht die überweisende Stelle die Freigabe verweigern. Pauschalisierte Sonderregelungen aufgrund struktureller Einheiten, funktioneller Gemeinsamkeiten und besonderer Kooperationsbedingungen zwischen Fachabteilungen bedürfen einer sorgfältigen Begründung; Beispiele dafür folgen.
Der zugriffsberechtigte Personenkreis sowie dessen Rechte sind stets nach dem Grundsatz der Erforderlichkeit zu minimieren. Auch die Krankenhausverwaltung darf nur zu den Daten Zugang haben, die für ihre Zwecke erforderlich sind. Eine zentrale Referenzdatenbank, sofern ihr Umfang über eine reine Verweisdatei hinausgeht, ist, ebenso wie ein Archiv, kein Selbstbedienungsladen; auch hier gilt die Datenhoheit der Fachabteilungen.
Zugriffsrechte werden in Form eines kliniksweiten sowie eines abteilungsspezifischen Regelwerkes festgelegt, das mit dem Datenschutzbeauftragten abzustimmen ist. Bei Bedarf wird für den einzelnen Patienten eine Rechteliste in der Patientenakte mitgeführt, z. B. wenn er von seinem Widerspruchsrecht Gebrauch gemacht hat. Die Rechte werden je nach Anwendungsfall vergeben an

- Fachabteilungen,
- Rolleninhaber,
- Einzelpersonen,

wobei hierarchisch geordnete rollenbasierte Zugriffsrechte im Krankenhausbetrieb meistens angemessen sind. Den unterschiedlichen Aufgaben und Zielen entsprechend ist der Zugriff selektiv nach der Art der Daten und der Art des Zugriffs zu gewährleisten. Die Definition der Rollen und der ihnen zugeordneten Zugriffsrechte soll durch durch den Kliniksvorstand vorgenommen und durch eine zentrale verfahrensbetreuende Stelle umgesetzt werden; die Zuweisung von Rollen zu bestimmten Personen erfolgt durch die Fachabteilung. Soweit lediglich abteilungsinterne Zugriffsmöglichkeiten betroffen sind, können eigene Rollen auch durch die Fachabteilung definiert werden.

Innerhalb des Behandlungszeitraums haben behandelnde Ärzte Zugriff auf den ganzen zum Behandlungszusammenhang gehörigen Teil der Patientenakte, soweit nicht besonders sensible Daten von anderen Fachabteilungen gesperrt sind, sowie auf die zu früheren Behandlungszusammenhängen in der gleichen Fachabteilung angefallenen Daten des Patienten. Dies gilt auch für Ärzte im Praktikum und Studenten im praktischen Jahr sowie für Ärzte, die der Fachabteilung zeitweise, z. B. im Rahmen von Nachtdienst, zugeordnet sind; deren Berechtigung ist auf die Zeit dieses Dienstes zu beschränken. Nach der Entlassung ist der Zugriff noch für einen angemessenen Zeitraum zulässig (z. B. für Arztbriefschreibung) - diese zeitliche Befristung ist allerdings nicht in allen einschlägigen Landesgesetzen vorgesehen.
Außerhalb des Behandlungszusammenhangs dürfen die Daten eines Patienten auch dem medizinischen Personal innerhalb der Abteilung nicht zur Verfügung stehen (nicht in allen Bundesländern zwingend), außer für definierte Forschungsprojekte oder Auswertungen im Rahmen der Qualitätssicherung; hierfür sind die Datenschutzregelungen für Forschungsvorhaben zu beachten, die insbesondere im Regelfall Anonymisierung oder Pseudonymisierung verlangen. Einem behandelnden Arzt sollen auch Rückgriffe auf Musterfälle seiner eigenen Behandlungstätigkeit möglich sein.
In der Fachabteilung tätige Pflegekräfte haben während des Aufenthalts des Patienten auf ihrer Station Zugriff auf die Krankenakte in einem Umfang, den der Leiter der Abteilung nach den Anforderungen der Arbeitsorganisation festlegt; auch hierbei ist der Grundsatz der Erforderlichkeit zu befolgen. Das gleiche gilt auch für sonstige Mitarbeiter der Fachabteilung. Für Famulanten, Studenten und Auszubildende legt der verantwortliche Lehrende im Rahmen seiner eigenen Befugnisse die Zugriffsberechtigung fest.
Der Nachweis eines Behandlungszusammenhangs wird in der Regel durch den Bewegungseintrag im Krankenhausinformationssystem erbracht. Oft erscheint der Patient aber schon in der neuen Abteilung, bevor wegen der Heterogenität des Krankenhausinformationssystems der Bewegungseintrag zur Verfügung steht. Für diesen Fall soll ein vorgezogener Zugriff möglich sein; unverzichtbare Grundlagen dafür sind

- die Zustimmung durch den Patienten (konkludent durch sein Erscheinen angenommen),
- die Freischaltung des Datenzugriffs durch die überweisende Abteilung (die in deren Abteilungssystem eventuell schon in Kraft ist oder in bestimmten Situationen, z. B. Röntgen, generell gewährt wird),
- die Nachvollziehbarkeit durch die Protokollierung.

Der Zugriff sollte sich auf administrative Daten und Überweisungsdiagnose beschränken. Wenn die Berechtigung nicht innerhalb einer angemessenen Frist nachgereicht wird, ist eine automatische Warnung an den für die Daten Verantwortlichen zu versenden. (Anmerkung: Dieser Fall ist in der gegenwärtigen Situation, wo die Krankenhauskommunikation an vielen Stellen noch unzulänglich funktioniert, häufig. Mit verbessertem Ausbau der Krankenhausinformationssysteme sollte er selten oder gar nicht mehr vorkommen.)
Zugriffe auf die Patientenakte sollten protokolliert werden mit Angabe von Person, Rolle, Fachabteilung, sowie Art, Zeitpunkt und Umfang des Zugriffs. Die Granularität dieser Protokollierung ist nach dem Grundsatz der Verhältnismäßigkeit unter dem Gesichtspunkt der Praktikabilität auszubalancieren; ordnungsgemäße, den Richtlinien entsprechende Zugriffe durch das behandelnde Personal der Fachabteilung brauchen nicht im Protokoll zu erscheinen; eine stichprobenartige Protokollierung hiervon erscheint aber sinnvoll. Das Zugriffsprotokoll wird als Teil der Patientenakte behandelt, egal wo es physisch gespeichert ist, und ist nur für den verantwortlichen Arzt, den Patienten selbst und für den Datenschutzbeauftragten jederzeit einsehbar; diese haben auch das Recht, eine nachträgliche Rechtfertigung für den Zugriff zu verlangen. Die Folgen bei entdecktem Mißbrauch sind durch eine Dienstvereinbarung unter Berücksichtigung des Datenschutzrechts und des Strafgesetzbuchs zu regeln. Protokolleinträge sollen für eine

angemessene Zeit aufbewahrt werden; mit Rücksicht auf das Auskunftsrecht des Patienten erscheinen 2 Jahre angemessen.
In Notfällen (z. B. Nacht- oder Wochenendaufnahme) ist im Interesse des Patienten - auch gemäß der EU-Richtlinie - ein schneller, unkomplizierter Zugriff auf die Daten zu gewährleisten. Hier ist in der Regel der Zugriff auf die Notfalldaten sowie der Hinweis auf frühere Aufenthalte ausreichend. Dabei ist über die gewöhnliche Protokollierung hinaus eine sofortige gesonderte Benachrichtigung des für die Daten Verantwortlichen und ein regelmäßiges Sonderaudit vorzusehen - in diesem Fall gehen die Datenschutzrechte des Patienten denen des Personals vor.
Die Notfalldaten eines Patienten sind ohne weitere explizite Freigabe von allen bei der Behandlung dieses Patienten beteiligten Fachabteilungen einsehbar. Die Existenz von Notfalldaten ist unübersehbar zu kennzeichnen, sie müssen besonders schnell abrufbar sein und übersichtlich zusammengefaßt präsentiert werden („Cave-Fenster“). Auch hier ist die Protokollierung zur Entdeckung eines Mißbrauchs unverzichtbar.
Über Zugriffe auf die als besonders sensibel gekennzeichneten Daten entscheidet der Leiter der Fachabteilung, in der sie produziert wurden. Bei Zielkonflikten zwischen Notfalldaten und besonders sensiblen Daten - z. B. Diagnose AIDS - hat die Sensibilität der Daten Vorrang. Eine Einwilligung des Patienten reicht hier aber auch zur Freigabe.

4. Technische Absicherung der Zugriffsrechte und -Einschränkungen

Patientendaten sind nach dem Stand der Technik zu schützen, wobei das Prinzip der Verhältnismäßigkeit zu beachten ist. Für medizinische Daten ist wegen ihrer Sensibilität ein entsprechend hoher Aufwand zur Realisierung der Sicherheit geboten. Durch technische und organisatorische Maßnahmen muß gewährleistet sein, daß genau die in der entsprechenden Rechteliste definierten Zugriffe auf eine Patientenakte stattfinden können. Die vom Sicherheitskonzept geforderten Beschränkungen müssen durch geeignete Implementation und durch Sicherheitstechnik garantiert werden. Natürlich dürfen auch die Möglichkeiten zum Datenzugriff unter Umgehung der Anwendungsprogramme nicht vergessen werden, z. B. mit Hilfe von direktem Plattenzugriff oder Netzmonitorprogrammen. Die Sicherheitsanforderungen sind daher nur durch kryptographische Techniken - verschlüsselte Speicherung und Übertragung, starke Authentisierung - zu erfüllen.
Verschlüsselte Übertragung soll die Daten zwischen Ursprungs- und Zielsystem vor der Einsicht durch Unberechtigte, auch durch IT-Personal, schützen. Verschlüsselt werden sollten die Nutzdaten der Übertragung, nicht die Verbindungsdaten, wie etwa Protokoll-Header. Der geeignetste Ansatz scheint die Verschlüsselung auf der Protokoll-Ebene zu sein, etwa die Verwendung von SSL (siehe Glossar) beim Einsatz von Intranet-Techniken. Eine Minimalforderung, solange im Einzelfall geeignete kryptographische Techniken noch nicht zur Verfügung stehen, ist das Unterdrücken von Identifizierungsdaten bei der Übermittlung; werden bei der Übertragung nur Patientennummern mitgeschickt, ist bereits eine wenigstens schwache Pseudonymisierung erreicht.
Um IT-Personal bei Systempflege und -wartung an sachlich nicht notwendigen Einblicken in Patientendaten zu hindern, wird eine Speicherung der identifizierenden Daten in einer getrennten Tabelle und die Verwendung von Pseudonymen für den Fall, daß die Zusammenführung unvermeidbar ist, empfohlen.
Server und Kommunikationsknoten sind als besondere Sicherheitsbereiche zu definieren und physisch zu schützen, in der Regel in verschlossenen Räumen.
Zum Nachweis der Benutzerberechtigung sollte entsprechend deutscher, europäischer und internationaler Rechtsgrundlagen eine Sicherheitsinfrastruktur nach dem Stand der Technik aufgebaut werden, die insbesondere starke Authentisierung und Rechteprüfung aufgrund von Zertifikaten (siehe Glossar) beinhaltet. Hier sind zukünftig die Möglichkeiten der Health Professional Card (HPC) zu nutzen. Es soll ein fliegender Rollen- oder Benutzerwechsel möglich

sein; dazu ist eine Speicherung der aktuellen Benutzungsoberfläche in einem sicheren Systembereich geeignet, so daß sie nur durch erneute Authentisierung wieder aktiviert werden kann. Auf analoge Weise ist ein Time-Out zu realisieren.
Die Benutzungsoberfläche ist so zu gestalten, daß die Sicht, die dem Benutzer gewährt wird, genau seinen Rechten entspricht; d. h., es sind nur die Daten sichtbar, für die Leserecht besteht, und nur die Datenfelder editierbar, für die Schreibrecht besteht. Die Existenz von Notfalldaten ist deutlich anzuzeigen. Die Bedienungselemente für Notfallzugriffe außerhalb bereits gewährter Rechte sind mit deutlichen Warnhinweisen auf die Konsequenzen zu versehen. Die Berechtigung dazu ist lokal unter dem Gesichtspunkt der Praktikabilität eindeutig zu regeln.
Noch nicht Stand der Technik, aber spätestens nach Einführung der Health Professional Card anzustreben, ist die konsequente Anwendung der digitalen Signatur, um die Verbindlichkeit (Zurechenbakeit, Unleugbarkeit) von Dokumentation und Maßnahmen zu sichern. Dazu gehört auch ein, vom Trustcenter anzubietender, sicherer Zeitstempeldienst.

5. Typische Beispielsituationen

Hier werden Empfehlungen für die Ausgestaltung der Zugriffsrechte in typischen Situationen des Krankenhausalltags gegeben.

Aufnahme

Die reguläre Aufnahme eines Patienten erfolgt durch einen dazu berechtigten Verwaltungsmitarbeiter. Bei der Aufnahme wird der Patient, in der Regel durch einen separaten Vordruck, auf seine Rechte bezüglich des Datenschutzes hingewiesen und darüber informiert, welche Daten von wem verarbeitet werden, und stimmt mit seiner Unterschrift der Speicherung und Verarbeitung seiner Daten zu. Er wird durch den aufnehmenden Verwaltungsmitarbeiter einer Fachabteilung zugewiesen. Dadurch werden die Zugriffsrechte für diese Fachabteilung freigegeben. Handelt es sich um eine Wiederaufnahme, d. h. wurde der Patient schon einmal in diesem Krankenhaus behandelt, darf bei der Aufnahme auf bereits vorhandene Stammdaten zugegriffen werden. Bei Identifizierungsproblemen ist eine minimierte Auswahl an Fällen und identifizierenden Daten anzubieten, auf keinen Fall aber eine vollständige Patientenliste zur Auswahl. Die Anzeige eines anderen Patienten in einer solchen minimalen Auswahlliste braucht nicht als Zugriff auf dessen Daten protokolliert zu werden. Bei einer Wiederaufnahme ist, sofern das Landesrecht nichts anderes vorsieht, der Patient zu fragen, ob medizinische Daten aus früheren Aufenthalten in anderen Fachabteilungen herangezogen werden dürfen. Widerspricht der Patient, so ist für den behandelnden Arzt ein entsprechender Vermerk zu machen, ohne jedoch die betroffenen anderen Abteilungen zu nennen. Der Arzt hat so die Möglichkeit, später doch noch die Zustimmung des Patienten zu erhalten. Der aufnehmende Verwaltungsmitarbeiter darf in diese Daten keinen Einblick erhalten.
Die Häufigkeit des Zugriffs auf Auswahllisten durch bestimmte Benutzer ist zu protokollieren, ebenso wie unnötige Zugriffe, um Mißbrauch zu entdecken. Ein Mißbrauch liegt z. B. vor, wenn eine Aufnahme vorgetäuscht wird, um in frühere Patientendaten einer Person Einblick zu erhalten.

Kurzaufnahme

Eine Kurzaufnahme erfolgt außerhalb der normalen Dienststunden direkt in der Fachabteilung. Welche Personen, z. B. auch Pflegepersonal, zu einer Kurzaufnahme berechtigt sind, legt der Abteilungsleiter in Absprache mit der ansonsten für die Aufnahme zuständigen Verwaltungsstelle fest. Die Prüfung, ob der Patient bereits im Krankenhausinformationssystem vorhanden ist, erfolgt entsprechend zur regulären Aufnahme. Die Kurzaufnahme ist baldmöglichst vom dazu berechtigten Verwaltungspersonal in eine reguläre Aufnahme zu überführen. Nach Abschluß der Kurzaufnahme

erhält die aufnehmende Abteilung den Zugriff auf die Notfalldaten des Patienten sowie, wenn dies nicht ohnehin unbeschränkt möglich ist, auf eventuell schon vorhandene Daten in der eigenen Abteilung mit Fallbezug.

Notaufnahme

Eine Notaufnahme erfolgt, wenn aufgrund des Gesundheitszustandes des Patienten eine reguläre Aufnahme oder eine Kurzaufnahme nicht möglich ist. Ist der Patient nicht bei Bewußtsein, ist in seinem Interesse von der Einwilligung zum Datenzugriff im benötigten Umfang auszugehen; ist seine Identität nicht ermittelbar, wird er zunächst unter einem Pseudonym eingetragen.

Wiederaufnahme im gleichen Behandlungszusammenhang

Hier wird die unmittelbar vor der Entlassung gültige Datensicht wiederhergestellt.

Ambulante Aufnahme

Die ambulante Patientenaufnahme erfolgt in der Regel dezentral in den Polikliniken und in Leistungsbereichen wie der technischen Orthopädie oder der physikalischen Therapie. Es gelten analoge Empfehlungen wie für die Kurzaufnahme.

Erstkontakt mit dem Arzt

Im Interesse des Patienten ist es, schon aus haftungsrechtlichen Gründen, unerläßlich, daß eine neu aufnehmende Fachabteilung Lesezugriff auf die in der Patientenakte enthaltenen Informationen über frühere Kliniksaufenthalte auch in anderen Fachabteilungen hat; letztlich kann nur die neu behandelnde Fachabteilung beurteilen, welche medizinischen Daten sie für die Behandlung dieses Patienten braucht. Der verantwortliche Arzt muß daher vom Krankenhausinformationssystem über die Existenz früherer oder paralleler Behandlungszusammenhänge informiert werden, aber nicht über Art und Abteilung - dieses nur nach Zustimmung des Patienten. Notfalldaten müssen in jedem Fall sichtbar sein, auch wenn dadurch Rückschlüsse auf frühere Aufenthalte möglich sind.

Verlegung

Mit einer angeordneten Verlegung eines Patienten in eine andere Fachabteilung werden die im Behandlungszusammenhang benötigten Daten für die neue Abteilung freigegeben und sind dann dort unter Berücksichtigung der Rolle des Zugreifenden verfügbar, in der Regel nur mit Leseberechtigung. Der Patient ist bei der Besprechung seiner Weiterbehandlung auch über die vorgesehene Datenfreigabe und sein eventuelles Widerspruchsrecht zu informieren.
Hier sollte die im Routinefall übliche Freigabe im benötigten Datenumfang in den Verlegungsvorgang des Krankenhausinformationssystems eingebaut werden; in der Regel handelt es sich um die administrativen Daten sowie den in der Verantwortung der überweisenden Abteilung gespeicherten Teil der Patientenakte ohne die besonders sensiblen Daten. Das Speichern der Daten der alten Abteilung im System der neuen Abteilung würde sie der Datenhoheit der alten Abteilung entziehen und ist daher nicht zulässig, wenn auch technisch kaum zu verhindern.

Mitbehandlung und Konsil

Für die Mitbehandlung in einer anderen Fachabteilung ist die Datenfreigabe analog zur Verlegung zu regeln, zusätzlich ist umgekehrt die Freigabe der hier anfallenden Informationen für die

hauptsächlich behandelnde Fachabteilung ohne weitere Umstände als Rückmeldung vorzusehen. Gleiches gilt für Konsiliardienste. Wie weit rückgemeldete Daten in die Hoheit der anfordernden Abteilung übergehen, ist im Einzelfall verbindlich zu regeln.
Ausnahmeregelungen, wo die Notwendigkeit zur expliziten Freigabe im Einzelfall als zu einschränkend erachtet wird, sind bei routinemäßiger abteilungsübergreifender Zusammenarbeit möglich, wenn sie im Einvernehmen mit dem Datenschutzbeauftragten vom Kliniksvorstand schriftlich genehmigt wurden. Beispiele hierfür können sein die Zusammenarbeit zwischen operativen Abteilungen und der Anästhesie oder zwischen der Geburtshilfe und der Kinderklinik. Auch hier ist aber das Widerspruchsrecht des Patienten, soweit vorhanden, in der Form zu berücksichtigen, daß gegebenenfalls die Daten gesperrt werden können.

Leistungsanforderung

Mit der Leistungsanforderung, z. B. von Laborleistungen oder bildgebenden Verfahren oder bei anderen Funktionsbereichen, werden die benötigten Daten freigegeben, sofern der Patient nicht widerspricht. Auch hier sollte der typische Datenumfang im Krankenhausinformationssystem implementiert sein; in der Regel ist das nur ein Teil der Patientenakte. Werden darüber hinaus weitere Daten benötigt, ist das Recht dazu von der datenspeichernden Abteilung explizit einzuholen. Werden als Rückmeldung Daten nicht nur freigegeben, sondern übermittelt, liegt die Datenhoheit für die übermittelten Daten dann beim Empfänger.

Abteilungssysteme mit Stammdaten

Fachabteilungen oder Funktionsbereiche, die mitbehandeln oder Leistungen erbringen, können die Stammdaten des betroffenen Patienten in ihrem eigenen Abteilungssystem speichern; dies erhöht die Ausfallsicherheit des Krankenhausinformationssystems und hilft, wenn die Krankenhauskommunikation zu langsam oder unzuverlässig funktioniert, wie es in der gegenwärtigen Praxis oft noch der Fall ist. Eine völlige Freigabe der Stammdaten aller Patienten, möglichst sogar Mitteilung der Neuaufnahmen per Broadcast, wird insbesondere vom Zentrallabor und der Radiologie oft gewünscht; da in diesen beiden Fällen fast alle Patienten im Laufe ihrer Behandlung dort sowieso erfaßt werden, ist eine Ausnahmeregelung wie unter „Mitbehandlung“ sinnvoll. Diese sollte aber vorübergehenden Charakter haben, bis die Krankenhauskommunikation zuverlässig funktioniert, und verbietet sich bei Leistungsstellen, die nicht zum Krankenhaus gehören, z. B. bei Outsourcing.

Zentralküche

Es ist sinnvoll und unbedenklich, wenn jeder neu aufgenommene stationäre Patient mit Namen, Geburtsdatum, Station und gegebenenfalls Diätverordnung automatisch an die Zentralküche gemeldet wird. Auf Wunsch des Patienten sind hier auch Ernährungsbesonderheiten mitzuteilen - auf keinen Fall aber die Religionszugehörigkeit. Wird die Essensversorgung außer Haus gegeben, sind die Vorschriften für Datenverarbeitung im Auftrag zu beachten.

Pförtner- und Telefonliste

Mit Einverständnis des Patienten können Name und Station in die Pförtnerliste aufgenommen werden. Ebenfalls mit Einverständnis des Patienten kann die Telefonzentrale die Nummer seines Anschlusses bei Anfragen nennen.

Umherirrender Patient

Für den Fall, daß ein verwirrter Patient auf dem Flur angetroffen wird, wird gelegentlich gewünscht, daß von jeder Station aus auf Identifizierungs- und Bewegungsdaten aller momentan stationär aufgenommenen Patienten lesend zugegriffen werden kann. Dies erscheint aber nicht notwendig. Eine Klärung am Telefon ist hier sinnvoller.

Entlassung und Abrechnung

Die Ärzte der jeweiligen Abteilung sind für die Mitteilung der ausgeführten Leistungen (Diagnosen, Therapien, und, soweit schon ermittelt, Fallpauschalen und Sonderentgelte) an die Kliniksverwaltung verantwortlich. Diese abrechnungsrelevanten Daten werden von der Fachabteilung bzw. dem Funktionsbereich an die Kliniksverwaltung übermittelt und für den verantwortlichen Sachbearbeiter der Verwaltung mit Leserecht versehen. Da Prüfung des Abrechnungsvorschlags und eventuell Nacherfassung durch die Verwaltung nötig ist, ist dieser mit Schreibrecht zu versehen. Der Sachbearbeiter der Verwaltung erhält auf diese Weise unvermeidlich auch Einblick in besonders sensible Daten, z. B. Diagnosen und Therapien einer psychiatrischen Behandlung. Ferner hat der Sachbearbeiter Zugriffsrechte auf die administrativen Daten und verwaltungsinterne Sonderdaten wie Buchhaltungsdaten bei Selbst- und Zuzahlern.

Archivierung

Zugriffe auf archivierte Daten, egal wo diese physisch lagern, sind wie für aktuell gehaltene Daten zu regeln. Insbesondere unterliegen sie weiterhin der Datenhoheit der Fachabteilung. Die Vorschriften über Aufbewahrungsfristen und Löschpflichten sind zu beachten. Eine Archivierung der Daten und damit Herausnahme aus dem Direktzugriff ist nach etwa 5 Jahren sinnvoll; für die Aufbewahrungsfrist im Archiv erscheinen in der Regel 30 Jahre angemessen, sofern nicht andere Gesichtspunkte oder gesetzliche Vorschriften dem entgegenstehen (z. B. medizinische Gesichtspunkte, Archivgesetzgebeung). In jedem Fall sind die Vorschriften des Sperrens bzw. Löschens von Daten angepaßt an das jeweilige Speichermedium wirksam umzusetzen.

Glossar

- starke Authentisierung
  Anmeldeverfahren mit Identitätsprüfung, das im Gegensatz zum herkömmlichen Paßwortverfahren gute Abhör- und Fälschungssicherheit bietet. Es beruht darauf, daß nur der Inhaber eines (geheimen) Signaturschlüssels eine beliebige Zeichenkette gültig signieren kann.
- SSL
  'Secure Socket Layer', ein Standardverschlüsselungsprotokoll, das auf dem TCP/IP-Protokoll aufsetzt und insbesondere von WWW-Servern und allen gängigen WWW-Browsern unterstützt wird. Programmbibliotheken sind frei verfügbar.
- Time-Out
  Unterbrechung einer Kommunikationsbeziehung oder Beendigung einer gültigen Anmeldung an einem IT-System, wenn über einen definierten Zeitraum keine Aktivitäten stattfanden.
- Trustcenter
  Im Zusammenhang dieser Empfehlung eine Instanz, die Zertifikate für Nutzer eines Informationssystems ausgibt und evtl. einen Zeitstempeldienst anbietet.
- Zeitstempel
  Durch digitale Signatur eines Trustcenters wird eine Information unfälschbar mit einer Zeitangabe versehen.

- Zertifikat
  bescheinigt die Zusammengehörigkeit eines öffentlichen Schlüssels zu einem Namen und wird von einem Trustcenter ausgegeben.

Weitere Texte zum Thema

- Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz: Datenschutz im Krankenhaus. (Informationen zum Datenschutz, Heft 4)
- Arbeitspapier des Hessischen Datenschutzbeauftragten: Rechtsfragen der Kommunikation innerhalb des Krankenhauses.

Autoren: Klaus Pommerening, Marita Sergl (unter Verwendung von Texten von Bernd Blobel, Jörn Erdmann, Judith Hartig, Bernd Hornung, Manfred Schnabel, Norbert Schuber, Rita Wellbrock, Rüdiger Wehrmann) - 12. Februar 1998; letzte redaktionelle Änderung: 1. Juni 1999

Sicherheitsempfehlungen zu Modem-Verbindungen im Krankenhaus

Erarbeitet von der GMDS-Arbeitsgruppe „Datenschutz in Gesundheitsinformationssystemen“
Aus verschiedenen Gründen kann für Rechner in einem Krankenhaus ein Modem-Anschluß wünschenswert sein:

- Zugriff auf externe Informationen im Internet.
- Systemverwaltungsarbeiten in Heimarbeit.
- Anwendungsbearbeitung in Heimarbeit.
- Fernwartung durch Firmen.
- Telemedizinische Anwendungen.

Dabei entstehen erhebliche Sicherheitsrisiken, sowohl für den Schutz der Patientendaten und anderer personenbezogener Daten als auch für die Integrität der angeschlossenen Rechner und des gesamten Krankenhaus-Informationssystems, die besonders sorgfältige Planung, Konfiguration und Dokumentation erfordern.

1. Grundsätze zum Modem-Anschluß

„Remote Access Server“ (RAS) und Modems besitzen umfangreiche und sehr komplexe Konfigurationsmöglichkeiten, wobei die Voreinstellungen oft unsicher sind. Die zuverlässige Konfiguration erfordert erhebliche Systemkenntnisse und Sorgfalt. Da Sicherheitsprobleme nur in einer möglichst einfachen Konstellation beherrschbar bleiben, ist ein zentraler Modem- und Access-Server einzurichten, der unter der Verantwortung einer geeigneten Stelle im Krankenhaus (Rechenzentrum, zentrale Service-Abteilung) betrieben wird. Diese Stelle ist so auszustatten, daß sie die nötige Kompetenz erwerben kann. Weitere Modem-Verbindungen sind in der Regel zu verhindern, weil sie die Sicherheit des gesamten Klinikinformationssystems unkontrolliert untergraben können. (Eine technische Kontrolle auf ungenehmigte Anschlüsse ist allerdings schwierig.) Ausnahmen von dieser Regel können gestattet werden

- für Rechner, die in der Klinik nicht weiter vernetzt sind und auf denen keine personenbezogenen Daten gespeichert sind - etwa zur Informationssuche im Internet, wenn keine andere Möglichkeit besteht,
- in begründeten Ausnahmefällen, sofern die unten aufgeführten Maßnahmen getroffen sind und die Möglichkeiten eines sicheren Firewall-Tunnels nicht genützt werden können - etwa um einen 24-Stunden-Notdienst an wichtigen Systemen zu gewährleisten oder wenn eine Fernwartungsverbindung über den zentralen Modemserver nicht möglich ist.

2. Anforderungen an einen Modem-Anschluß

Folgende Anforderungen gelten sowohl für einen zentralen Modem-Server als auch für Einzelanschlüsse, soweit sie für die Einwahl von außen ins Krankenhausnetz verwendet werden sollen:

- Es ist ein Rückruf-Modem (oder die im allgemeinen besser konfigurierbare Rückrufmöglichkeit des RAS) zu verwenden; die Umgehung der Rückruffunktion sollte ausgeschlossen werden können. Eine Rückrufweiterleitung, wie bei ISDN möglich, ist zu verhindern.
- Es ist ein verschlüsselndes Modem zu verwenden, damit die übertragenen Daten kryptographisch gesichert sind.

- An jedem externen Arbeitsplatz ist eine gesicherte Umgebung herzustellen; insbesondere ist der Zugriff durch Familienangehörige oder weitere Personen zu verhindern.
- Der Datenschutzbeauftragte des Krankenhauses ist von der geplanten Installation in Kenntnis zu setzen; von ihm für diesen Zweck vorgesehene Verpflichtungserklärungen sind zu unterschreiben.
- Vor Inbetriebnahme ist eine sorgfältige Konfigurationsbeschreibung vorzulegen, aus der insbesondere hervorgeht, ◦welche Anwendung ausgeführt werden soll und welche Daten dabei übertragen werden,
    - welche Übertragungsprotokolle verwendet und wie Nebenwirkungen, wie z. B. IP-Routing, kontrolliert werden,
    - welche sicherheitsrelevanten Konfigurationsoptionen eingestellt werden, insbesondere wie die Rückruffunktion konfiguriert ist,
    - welches kryptographische Verschlüsselungsverfahren verwendet wird,
    - welche Sicherheitsmaßnahmen sonst getroffen werden,
    - wie die Konfigurationsdaten des Modems und gegebenenfalls des RAS vor Zugriff geschützt sind,
    - welche Ereignisse aufgezeichnet werden und wie diese Aufzeichnungen behandelt werden.

Mit dieser Beschreibung belegt der Betreiber des Anschlusses zugleich seine Befähigung, mit dem Anschluß verantwortungsvoll umzugehen.
Bemerkung: Die kryptographische Verschlüsselung der Übertragung ist auch dann wünschenswert, wenn keine personenbezogenen Daten übertragen werden, um die Integrität des Krankenhausinformationssystems nicht unnötigen Risiken auszusetzen, insbesondere, um Paßwörter zu schützen.
Hingewiesen werden soll hier auch auf den Abschnitt über Modems im IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

3. Anwendungsfälle

Die oben formulierten allgemeinen Anforderungen gelten in jedem der folgenden Fälle, sofern nicht ausdrücklich etwas anderes gesagt wird.

3.1 Systemverwaltung

Ein Fernzugriff ist nur bei gründlicher Sachkenntnis zuzulassen. In diesem Fall ist der Zugriff über einen sicheren Firewall-Tunnel oder, soweit das nicht möglich ist, über ein Einzelmodem mit direkter Verbindungsschaltung vorzuziehen. Für die Verwendung eines privaten Rechners gilt das im Abschnitt Anwendungsbearbeitung Gesagte.

3.2 Anwendungsbearbeitung

Die Notwendigkeit zum Fernzugriff ist besonders gründlich zu prüfen. Der Zugang über einen sicheren Firewall-Tunnel oder den Modemserver mit RAS sollte dann obligatorisch sein. Ein privater PC soll für diesen Anwendungsfall nicht verwendet werden; wegen der Beschlagnahmeproblematik soll der Rechner dem Krankenhaus gehören und inventarisiert sein. Er unterliegt dann auch der Kontrolle durch den Datenschutzbeauftragten des Krankenhauses.

3.3 Fernwartung

Fernwartung ist rechtlich unter dem Gesichtspunkt der Auftragsdatenverarbeitung zu sehen. Auftragsdatenverarbeitung und Fernwartung sollten in ihren Modalitäten in einem

rechtsverbindlichen Vertrag festgelegt werden, insbesondere, wenn personenbezogene Daten verarbeitet werden. Dieser Vertrag sollte enthalten:

- Festlegung der Beteiligten, die persönlich zu benennen und zu verpflichten sind
- Festlegung des Umfanges der Datenverarbeitung
- Festlegung der Verantwortlichen und ihrer Stellvertreter
- Organisation der Datenübermittlung

Auch die mögliche Weiterleitung von Wartungsproblemen an übergeordnete Service-Zentren oder Software-Entwickler („Eskalation“) sollte im Vertrag geregelt sein; bei internationalen Firmen ist hier für die eventuelle Übermittlung von Daten ins Ausland die Datenschutzgesetzgebung zu beachten. Die Weitergabe von Daten im Rahmen der Fernwartung ist allerdings nur dann datenschutzrelevant, wenn es sich um sensible Daten handelt, nicht aber, wenn die Daten anonymisiert sind.
Die Sicherheitsanforderungen für Fernwartungsverbindungen sind in der Regel durch ein Einzelmodem mit direkter Verbindungsschaltung am besten erfüllbar. Das Modem sollte außer im unmittelbaren Anwendungsfall abgeschaltet sein. Fernwartungsverbindungen sollen nur vom Krankenhaus her aufgebaut werden dürfen; gleichwertig hierzu ist das Vorgehen: Anruf vom Krankenhaus beim Fernwartungsservice, Einschalten des Modems, Einwahl durch die Firma. Ein beliebiges Einwählen durch die beauftragte Firma ist abzulehnen.
Bei der Konfiguration kann, nach entsprechender vertraglicher Gestaltung, auf die Sachkenntnis der externen Firma zugegriffen werden. Die Anmietung eines Raumes bei der Firma durch das Krankenhaus zum Zweck der Fernwartung ist zu empfehlen. Die Fernwartung ist abzustufen nach

- Hardware
- Betriebssystem
- •Anwendungssoftware

nur die jeweils unbedingt nötigen Zugriffe sind zu gewähren. Vor allem ist sicherzustellen, daß kein Zugriff auf Patientendaten erfolgen kann, etwa durch Anonymisierung; in unvermeidbaren Ausnahmefällen ist auf die persönliche Verpflichtung zum Datengeheimnis zu verweisen. Die Fernwartungsaktivitäten sind lokal durch einen Systemverantwortlichen mitzuverfolgen, der gegebenenfalls die Verbindung sofort unterbrechen kann; sie sind außerdem automatisch zu protokollieren. Nach Möglichkeit ist ein Testsystem bereitzustellen; nach Abschluß der Wartung werden dann die Änderungen vom lokalen IT-Personal in das Produktionssystem übernommen. Auf diese Weise wird auch die Stabilität des Produktionssystems besser gewährleistet.
Zum Thema „ernwartung“gibt es eine Reihe von Stellungnahmen der Landesdatenschutzbeauftragten, insbesondere Leitlinien des Landesbeauftragten für den Datenschutz Bremen, die von der Konferenz der Datenschutzbeauftragten zustimmend zur Kenntnis genommen wurden und von der Arbeitsgruppe unterstützt werden.

3.4 Telemedizinische Anwendungen

Hier ist die Verbindung grundsätzlich über den Modemserver und RAS aufzubauen. Eine besonders gründliche IP-Nummern-Kontrolle ist vorzusehen.

3.5 Internet-Anschluß

Der Anschluß, außer von einzeln stehenden Rechnern ohne personenbezogene Daten, ist über ein Firewall-System zu realisieren. Hierzu liegt bereits eine Empfehlung der Arbeitsgruppe vor.

Autor: Klaus Pommerening, 19. Januar 1998; letzte Änderung: 15. Oktober 1998

Datenschutz und Datensicherheit in Informationssystemen des Gesundheitswesens

Erschienen (in leicht redigierter Form) in f&w 2/97, 133-138.
B. Blobel (1) und K. Pommerening (2)

Zusammenfassung

Mit den gegenwärtigen und längst noch nicht abgeschlossenen dramatischen strukturellen Veränderungen entwickelt sich das Gesundheitswesen zu einer offenen und verteilten Struktur im Sinne des „Shared Care“. Zur Steigerung der Effizienz trägt entscheidend die elektronische Informationsverarbeitung bei. Die hohen Ansprüche an Datenschutz und Datensicherheit in der Medizin erfordern dabei effektive und sorgfältig geplante Maßnahmen.
Dieser Artikel richtet sich an die Verantwortlichen im Management und in den Anwendungsbereichen der Informationstechnologie in Einrichtungen des Gesundheitswesens. Er soll ihnen einen Überblick über die in diesem Rahmen bestehenden Anforderungen, Probleme und Lösungskonzepte geben und Entscheidungsgrundlagen liefern. Insbesondere werden Empfehlungen für die organisatorischen und technischen Maßnahmen formuliert, die zur Umsetzung solcher Konzepte geeignet sind. (3)
Fazit: Vollständige Sicherheit kann es auch in einem Gesundheitsinformationssystem nicht geben. Mit dem Stand der Technik läßt sich aber prinzipiell ein angemessenes Sicherheitsniveau erreichen, ohne die Arbeitsabläufe im Gesundheitswesen unzumutbar zu beeinträchtigen.

1. Veränderungen in Struktur und Funktion des Gesundheits- und Sozialwesens unter dem Aspekt der Datensicherheit

Die Bemühungen um Sicherung des sich qualitativ und quantitativ ausweitenden Versorgungsauftrages bei gleichzeitiger Dämpfung der Kostenexplosion werden nur durch eine straffe, auf Effizienz und Qualität ausgerichtete Gestaltung der Betreuungsprozesse erfolgreich sein können. Die Arbeitsteiligkeit im Gesundheitswesen und die Verzahnung seiner Strukturen nehmen zu. Das erfordert eine entwickelte Kommunikation und Kooperation innerhalb der sowie zwischen den Einrichtungen des Gesundheits- und Sozialwesens im Sinne des Shared Care [7, 8, 13, 14]. Unter Shared Care verstehen wir nach [19] die „fortlaufende und koordinierte Tätigkeit von verschiedenen Personen in verschiedenen Institutionen unter Einsatz verschiedener Methoden zu verschiedenen Zeiten, um Patienten in medizinischer, psychologischer und sozialer Hinsicht optimal helfen zu können“.
Mit der Schaffung der kommunikativen Infrastruktur in den Gesundheitseinrichtungen, mit der informationslogistischen Begleitung der arbeitsteiligen Prozesse in der medizinischen Versorgung und der daraus resultierenden Realisierung komplexer, z. T. strukturübergreifend kooperierender Krankenhausinformationssysteme ergeben sich hohe Anforderungen zur Gewährleistung von Datensicherheit und Datenschutz [4, 5, 10, 25]. Durch die Entwicklung der politischen und wirtschaftlichen Integration sind diese Fragen der sicheren Kommunikation in verteilten Gesundheitsinformationssystemen nicht nur im nationalen, sondern auch im internationalen (bzw. zumindest im europäischen) Rahmen zu sehen.
Die zu gewährleistenden Dimensionen der Datensicherheit für Gesundheitsinformationen sind

- die Integrität der Informationen
- die Vertraulichkeit der Informationen
- die Verfügbarkeit der Informationen sowie

- die Verantwortlichkeit für Informationen und Prozesse im Sinne der Verläßlichkeit und Verbindlichkeit

Die Vertraulichkeit der Information spricht Aspekte des Datenschutzes an. Die Integrität und Verfügbarkeit der Information stellt inzwischen eine wesentliche Bedingung im Gesundheitswesen dar - insbesondere unter den Bedingungen zunehmender Integration der Informationsverarbeitung in die realen Abläufe und der daraus resultierenden Abhängigkeit von der richtig aufbereiteten Information zur rechten Zeit am rechten Ort. Somit darf die Betrachtung nicht auf die Dimensionen des Datenschutzes beschränkt bleiben, sondern muß die Aspekte der Datensicherheit als Grundlage für Kooperativität integrieren.

2. Rechtliche Basisprinzipien für die Verarbeitung medizinischer Informationen

Im Volkszählungsurteil hat das Bundesverfassungsgericht erstmals das Recht des Bürgers auf informationelle Selbstbestimmung definiert. Diese Gedanken wurden von der Europäischen Union adaptiert und in Verbindung mit fortschrittlicher Datenschutzgesetzgebung, bei der das deutsche Datenschutzrecht an vielen Stellen Pate stand, als rechtsverbindliche EU-Direktive [4, 5, 40] zum Schutz des Individuums bei automatisierter Verarbeitung seiner persönlichen Daten und deren Austausch formuliert. Diese Direktive ist bis zum 24. Oktober 1998 von allen EU-Mitgliedsländern in nationale Gesetze umzusetzen. Danach dürfen personenbezogene Daten nur für einen klar definierten und rechtlich abgesicherten Zweck erfaßt und nicht von diesem Zweck abweichend weiterverarbeitet werden. Das generelle Verbot der Erfassung und Verarbeitung sensitiver Daten wird nur aufgehoben, wenn

- eine nachprüfbare (schriftliche) Einwilligung durch den Patienten bzw. seinen Vertreter vorliegt
- die Erfassung und Verarbeitung für medizinische oder gesundheitsbezogene Zwecke durch Personen erfolgt, die durch ein Berufsgeheimnis (z. B. die ärztliche Schweigepflicht) oder eine gleichwertige Verpflichtung gebunden sind
- der Schutz der vitalen Interessen des Patienten die Erfassung und Verarbeitung notwendig macht
- ein unabdingbares, rechtlich gesichertes Gemeininteresse über das Individualinteresse zu stellen ist oder sonstige, rechtlich fixierte Ausnahmen die Erfassung und Verarbeitung erfordern

Dabei hat die Erfassung und Verarbeitung der Daten fair und rechtmäßig zu erfolgen und ist auf ein zweckbezogen adäquates, relevantes und minimales Maß zu beschränken. Die Daten müssen korrekt sein und dürfen nur für eine zweckgebunden unbedingt notwendige Zeit gespeichert werden.
Der Patient hat das Recht auf Informiertheit über die beabsichtigte Erfassung und Verarbeitung seiner personenbezogenen Daten sowie auf Berücksichtigung seiner Rechte hinsichtlich des Zwecks der Erfassung und Verarbeitung. Der Patient darf auf diese Daten direkt oder über eine Person des Vertrauens (z. B. seinen Hausarzt) zugreifen. Infolge der Durchdringung der medizinischen Prozesse mit Informationstechnik kann es zunehmend zur Verselbständigung der Patientendaten kommen, so daß die Daten einen status personae annehmen und mit Persönlichkeitsrechten auszustatten sind. Deshalb ist laut EU-Direktive eine automatisierte Entscheidungsfindung allein auf der Grundlage gespeicherter Daten unzulässig.
Der Patient darf erwarten, daß seine persönlichen Daten im Gesundheitswesen mit äußerster Sorgfalt und Vertraulichkeit behandelt werden. Auch darf der Patient voraussetzen, daß vorhandene, erforderliche Informationen zur rechten Zeit am rechten Ort in der erforderlichen Aufbereitung der berechtigten Person zur Verfügung stehen, um eine optimale Betreuung zu gewährleisten. Ebenso sind die persönlichen Daten der Beteiligten im Gesundheitsprozeß entsprechend der Datenschutzgesetzgebung zu schützen.

Das arbeitsteilig organisierte Gesundheitswesen benötigt zur Erfüllung seiner Aufgaben entsprechende Informationen über den Patienten, spezifische Teile seiner Krankengeschichte sowie diagnostische und therapeutische Informationen aus dem Behandlungsgeschehen. Sowohl die ärztliche Schweigepflicht (§203 Abs.1 Nr. 1 StGB (4)) als auch das „Datengeheimnis“ (§5 BDSG (5)), das den Beschäftigten im Gesundheitswesen die Verarbeitung von Patientendaten nur im Rahmen der Zweckbestimmung des Behandlungsvertrages gestattet, verbieten es aber, Patientendaten uneingeschränkt - d.h. über die unmittelbare Zweckbindung hinaus - auszutauschen und zu verwenden.
Erschwerend in der Diskussion um den Datenschutz wirkt die diffizile Rollenverteilung bei den informationellen Prozessen in der Medizin. Diese Rollenverteilung ist mit einer unterschiedlichen Distanz zum Ursprung der Information verbunden, definiert Rechte und Pflichten und begründet Rechtsverhältnisse (in der Bundesrepublik noch als Eigentumsverhältnisse diskutiert) an Informationen [3]. Ein besonderer Bereich ist die Notfallmedizin mit ihrem zunächst anonymen Arzt -Patienten-Verhältnis, was in Sicherheitskonzepten entsprechend berücksichtigt werden muß.
Der Patient als Urheber und das medizinische Fachpersonal als Produzent der Information tragen die Verantwortung für die korrekte Verwendung der Daten unter Berücksichtigung der Persönlichkeitsrechte der Beteiligten. Folglich kann nur der die Daten produzierende, das heißt, sie erhebende Arzt bzw. die Institution unter Einbeziehung des Patienten die Rechte für den Zugriff auf die medizinischen Daten des Patienten und deren definierte Verwendung erteilen. Das gilt auch für archivierte Daten [3, 4].

3. Folgerungen für Datenschutz und Datensicherheit in medizinischen Informationssystemen

Vorschriften und Maßnahmen zur Datensicherheit im Gesundheitswesen tragen dazu bei, daß das Vertrauensverhältnis zwischen Patient und Arzt und das Persönlichkeitsrecht des Patienten bei der Datenverarbeitung gewahrt bleiben. Datensicherheit muß bereichsspezifisch, insbesondere medizinspezifisch gestaltet werden. Das Problem der Datensicherheit im Gesundheits- und Sozialwesen ist insbesondere auch unter ethischen Gesichtspunkten zu lösen.
Patientendaten sind nach dem Stand der Technik zu schützen, wobei aber das Prinzip der Verhältnismäßigkeit zu beachten ist (siehe auch EU-Direktive [40]). Insbesondere für medizinische Daten ist wegen ihrer Sensitivität ein entsprechend hoher Aufwand zur Realisierung der Sicherheit geboten. Durch technische und organisatorische Maßnahmen muß gewährleistet sein, daß nur der zuständige Arzt und, soweit für die Behandlung nötig, mitbehandelnde Ärze und Pflegepersonal sowie sonstige berechtigte Personen (6) die Patientendaten lesen oder im zulässigen Rahmen weitergeben können. Auch eine Krankenhausverwaltung darf nur zu den Daten Zugang haben, die für ihre Zwecke erforderlich sind. Als technische Absicherung müssen Patientendaten (wie auch andere möglicherweise vertrauliche Daten) per Systemvoreinstellung gegen Einsichtnahme und Übermittlung geschützt sein; die jeweilige Freigabe muß ein bewußter Akt sein. Den unterschiedlichen Aufgaben und Zielen entsprechend ist der Zugriff selektiv nach

- Identifikationsdaten
- administrativen Daten
- sozialen Daten
- medizinischen Daten
- genetischen Daten

zu gewährleisten [40].
Die Sicherheitsmaßnahmen sollen die Aufmerksamkeit des Arztes nicht vom Patienten ablenken. Zwar sind Datenschutzmaßnahmen ohne Mitwirkung der Beteiligten nicht zu verwirklichen, aber die Belastung des medizinischen Personals durch organisatorische und technische Verfahren ist zu

minimieren. Der sachgerechte Umgang mit den Patientendaten darf durch Schutzmaßnahmen nicht beeinträchtigt werden. Die Verfügbarkeit der Daten, besonders in kritischen Situationen, ist im Interesse des Patienten zu gewährleisten. Auch ist die Verfügbarkeit der Daten im begründeten allgemeinen Interesse zu gewährleisten, wobei hier strenge Maßstäbe anzusetzen sind. Technische Datenschutzmaßnahmen sollen den Austausch nicht sensitiver Informationen, z.B. den Zugriff auf externe Informationsdienste im Internet und elektronische Post, möglichst wenig behindern. Auch die Verwendung der Daten für Forschungszwecke soll, soweit die Datenschutzanforderungen für wissenschaftliche Forschungsvorhaben (7) erfüllt sind, gewährleistet sein. Dabei sollten die Daten zum frühest möglichen Zeitpunkt anonymisiert werden. Erfordert der Forschungszweck die Zusammenführung der Daten aus verschiedenen Quellen oder die Möglichkeit zur Reidentifizierung von Fällen, sollten Pseudonyme verwendet werden [32].
Die technischen und organisatorischen Datenschutzmaßnahmen in einer Institution des Gesundheitswesens sind nicht nebenbei zu erledigen. Sie erfordern die Schaffung einer entsprechenden Infrastruktur und eine klare Festlegung der Verantwortlichkeiten sowie die Einplanung eines angemessenen finanziellen und persönlichen Aufwands (siehe Abschnitt 6.).

4. Kommunikation im Gesundheitswesen: Gefahren, Bedrohungen und Schutzobjekte

Die Kommunikation im Gesundheitswesen kann bezüglich des Inhalts, der Partner, der Infrastruktur und der Dienste unterschieden werden. Kommunikationsinhalte betreffen die Medizin- oder Personenbezogenheit, insbesondere in der Differenzierung nach Identifikationsdaten usw. wie in Abschnitt 3. Die Kommunikationspartner können im Gesundheitswesen (z. B. Ärzte, Krankenhäuser, Krankenkassen) bzw. außerhalb des Gesundheitswesens (z. B. Lieferanten, Bibliotheken) angesiedelt sein. Die Kommunikationsinfrastruktur bezieht sich auf die Systemarchitektur und die genutzten Kommunikationsverbindungen, während die Dienste von der elektronischen Post über Messagesysteme wie HL7 (8) bis hin zu verteilten kooperierenden Systemen auf der Basis von CORBA (9) und/oder DHE (10) [6] reichen können [13, 14]. Die verschiedenen Kommunikationsinhalte, -partner, -infrastrukturelemente und -dienste können beliebig kombiniert werden und führen zu unterschiedlichen Bedrohungen mit unterschiedlichen Risiken und erfordern somit unterschiedliche Gegenmaßnahmen (für Messagesysteme siehe z. B. [9]).
Die Risiken, die durch die Informationstechnik im Gesundheitswesen drohen, sind vor allem:

- die Gefährdung der Patienten durch fehlerhafte Prozeduren oder unrichtige sowie unvollständige Daten
- die Nichtnachvollziehbarkeit der Verantwortung von Maßnahmen
- die Bedrohung der Vertraulichkeit, insbesondere die Verletzung der Schweigepflicht und des Datenschutzes, sowie
- die Nichtverfügbarkeit von Daten oder des Informationssystems

Bei diesen Bedrohungen kann man unterscheiden zwischen sich zufällig, mittelbar, mit geringer krimineller Energie ergebenden Aktionen (Fahrlässigkeit) sowie aggressiveren, gezielten, mit hoher krimineller Energie ausgeführten Angriffe (Vorsätzlichkeit). Die ersten entstehen durch

- unbefugte Betriebsfremde (z.B. zufällige Besucher an unbeaufsichtigten Geräten)
- unbefugte Betriebsangehörige (z.B. nicht-medizinisches Personal und Personal ohne Sonderbefugnis)
- befugte Betriebsangehörige mit abweichender Befugnis (z.B. Systemverantwortliche, Administratoren)
- befugte Betriebsfremde mit abweichender Befugnis (z.B. Wartungsdienst, Reparaturdienst)

Die Bedrohungen der zweiten Art sind zwar auch real und müssen bedacht werden, sie stellen jedoch auch nach den Ergebnissen internationaler Untersuchungen (veröffentlicht als sogenannte Incident-Reports) hinsichtlich Häufigkeit (< 20%) und z. t. auch auswirkungen das geringere potential dar. die differenzierung der bedrohungen ist allerdings von untergeordneter bedeutung, da die datenschutzvorschriften prinzipiell die bestmögliche sicherung nach dem stand der technik verlangen [31].
Zu den fahrlässigen Bedrohungen des Datenschutzes und der IT-Sicherheit durch Befugte zählen vor allem Benutzerfehler, die die Integrität der Daten und der Systeme beeinträchtigen, aber auch die für den Anwender unzureichende Transparenz von Verhalten von Betriebssystemen und Anwendungen (wie z. B. für den Benutzer nicht erkennbare Reste gelöschter Textpassagen bei Textverarbeitungssoftware) und unbeabsichtigte Nebenwirkungen von Benutzeraktionen (z. B. überschreiben einer gleichnamigen existierenden Datei beim Datentransfer). Zu vorsätzlichen Bedrohungen gehören absichtliche Manipulationen durch Insider, die z. B. die Verantwortung für begangene Fehler vertuschen wollen, aber auch „Frustreaktionen“ von Mitarbeitern. Von außen werden Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen vor allem bei einem Anschluß an öffentliche Netze bedroht. Die CERT-Advisories [15] warnen in jüngster Zeit immer wieder vor ständig beobachteten Netzaktivitäten, die automatisch die ans Internet angeschlossenen Rechner auf Sicherheitslücken testen.
Unter dem Aspekt des Datenschutzes zu beachtende Objekte sind in erster Linie die Patientendaten, aber auch die Personaldaten der Institution, deren Schutzwürdigkeit vor unbefugter Einsichtnahme sich aus den Datenschutzgesetzen ergibt. Zu schützen sind aber auch Betriebsdaten der Institution und Systemdaten aller verwendeten Rechenanlagen. Um sich nicht in komplexen Details zu verlieren, ist es am besten, auf alle Daten das 'Need-to-Know'-Prinzip bzw. das Prinzip der minimalen Rechte anzuwenden: Ein Datum darf grundsätzlich nur von demjenigen eingesehen oder verändert werden, zu dessen Aufgabe das ausdrücklich gehört [5, 31, 36].
Auch Daten, die bei der Aufzeichnung von Benutzeraktivitäten entstehen, unterliegen den Datenschutzvorschriften. Sie dürfen nur im begründeten Fall zum Nachweis von Sicherheitsverstößen verwendet werden, nicht aber zur Erstellung von Tätigkeits- und Bewegungsprofilen der Mitarbeiter (vgl. Betriebsverfassungsgesetz). Zur Regelung dieser Problematik sind begleitend zur Einführung von Informationssystemen gegebenenfalls betriebliche Vereinbarungen zwischen Personalvertretung und Management abzuschließen.

5. Modellierung und Implementierung sicherer Informationssysteme

Der Realisierung eines Informationssystems, insbesondere unter dem Gesichtspunkt der im Gesundheitswesen erforderlichen Sicherheit, muß ein klare Konzeption vorausgehen, in der Anwendungsziele und erwarteter Nutzen definiert, Probleme identifiziert und Lösungsmöglichkeiten benannt werden. Die Entwicklung von Lösungen und deren integrative Implementierung in existierende Anwendungsumgebungen erfordern klare Aufgabendefinitionen, Aufgabenteilungen, Kommunikation und Kooperation zwischen Entwicklern/Systemanbietern, Management und Nutzern [12]. Da die Einführung von IT-Anwendungen an den Zielen und Prozessen der betroffenen Institutiotiert sein muß, ist die wichtigste Aktivität eine klare und vollständige Beschreibung der Unternehmenspolitik (Ziele; Maßnahmen; Management-, Prozeß- und Qualitäts-Bewertungskriterien). Die zweite Aktivität sollte auf die komplexe Prozeßanalyse einschließlich der Integrationsmechanismen gerichtet sein [11, 12]n orien. Dann ist eine generelle Risikoanalyse des Systems und seiner Umgebung sowie die Definition von Bedrohungen und Gegenmaßnahmen durchzuführen. Qualitätsmanagement und Systembewertung werden als Entwicklungsergebnis oft unterschätzt, sind jedoch von besonderer Bedeutung für den Erfolg eines Informationssystems [39, 41].
Eine entscheidende Voraussetzung für die Entwicklung und Implementierung sicherer

Informationssysteme ist die klare Zuweisung und Beschreibung von Verantwortlichkeiten innerhalb der Institution sowie beim Partner. Die umfassende Integration der Anwender und Einbeziehung der Personalvertretung ist selbstverständlich.
Alle Aktivitäten sind zu dokumentieren bzw. in der Durchführungsphase detailliert zu protokollieren.
Für jeden Schritt der Entwicklung und Implementierung sind die kontinuierliche Fortschreibung der Sicherheitsgrundsätze und die Verbesserung des Datensicherheitsbewußtseins wichtig. Dabei kommt dem Training sowie der Ausbildung und Schulung sowohl des Managements als auch der Mitarbeiter höchste Bedeutung zu [41].
Folgende Grundsätze für die Speicherung, Kommunikation und Verarbeitung von Daten in Gesundheitsinformationssystemen sind zu beachten [5, 7, 8]:

- Die Organisation der Systeme einschließlich der Kommunikationsinfrastruktur (Netzwerktopologie) sollte unter Beachtung struktureller Einheiten und funktioneller Gemeinsamkeiten/Bedingungen erfolgen
- Der berechtigte Personenkreis sowie dessen Rechte sind stets zu minimieren
- Daten werden in der Verantwortung der erhebenden Institution oder Abteilung der Leistungsstelle gespeichert und verarbeitet und sind vor anderen Institutionen/Abteilungen zu schützen. Die erhebende Stellen tragen die Verantwortung für die erhobenen Daten sowie für die funktionellen und Zugriffsrechte auf diese Daten. Somit können Rechte an Dritte stets nur gegeben (logische Überweisung) und nie selbständig durch sie genommen werden
- Produktion sowie Test und Schulung sind strikt zu trennen
- Für Netzwerke sind die ISO-Sicherheitsstandards zu realisieren [33, 37]

Noch nicht befriedigend gelöst ist die Definition geeigneter, technischer Standards für medizinische Anwendungssysteme aller Arten in Anlehnung an die IT-Sicherheitskriterien [44], die man den Herstellern gegenüber durchsetzen kann und die die Planung und Beurteilung von Systemen erleichtern. Datenschutzinhalte und -ziele sowie Sicherheitsanforderungen sind dafür so zu spezifizieren, daß Hersteller genügend genaue Richtlinien in die Hand bekommen. Insbesondere ist eine geeignete kryptographische Infrastruktur zu definieren und soweit wie möglich zu schaffen; ein wesentlicher Schritt in diese Richtung wird zur Zeit durch das EU-Project TRUSTHEALTH [24, 38, 42, 43] sowie durch das Multimedia-Gesetz [18] geleistet.
Die vom Sicherheitskonzept geforderten Beschränkungen müssen von der Implementation garantiert, d. h., durch Sicherheitstechnik verwirklicht werden, z. B. die Festlegung, wer Zugang zu welchen Informationen hat. Hier dürfen natürlich auch die Möglichkeiten zum Datenzugriff unter Umgehung der Anwendungsprogramme nicht vergessen werden, z. B. mit Hilfe von direktem Plattenzugriff oder Netzmonitorprogrammen.

6. Verantwortlichkeiten und organisatorischen Maßnahmen

Jede Institution des Gesundheitswesens braucht einen Datenschutzbeauftragten und einen IT-Sicherheitsverantwortlichen ('Security Officer'). Diese Aufgaben sind zu trennen, da der Datenschutzbeauftragte Kontrollinstanz ist und nicht gleichzeitig Ausführender sein kann. Beide Funktionsträger benötigen, abhängig von Größe und Struktur der Institution, für die Erfüllung ihrer Aufgaben ausreichend Zeit, Mittel (auch Räumlichkeiten) und Unterstützung, insbesondere durch Schreibkräfte für Korrespondenz, Dokumentations- und Organisationsaufgaben, sowie Durchsetzungsbefugnisse. Der Datenschutzbeauftragte hat die im zuständigen Datenschutzgesetz festgelegten Aufgaben; er sollte nach Möglichkeit Mediziner sein, evtl. kommt auch ein Jurist in Betracht. Im einzelnen sind seine Aufgaben:

- Dokumentation personenbezogener Datensammlungen
- Überprüfung der Informationssysteme durch Revision

- Überwachung, Verfolgung und Auswertung von Datenschutzverletzungen
- zielgruppenorientierte Information und Schulung in Datenschutzfragen, Beratung der Abteilungen
- Mitwirkung bei Auskunftsersuchen und Beschwerden
- Zusammenarbeit mit dem IT-Sicherheitsverantwortlichen
- Vertretung der Institution bei Aufsichtsbehörden und anderen relevanten Gremien

Der IT-Sicherheitsverantwortliche sollte Informatiker oder Medizin-Informatiker sein. Er erstellt das Datenschutz- und IT-Sicherheitskonzept der Institution, stimmt es mit dem Datenschutzbeauftragten ab, setzt es mit Hilfe des vorhandenen IT-Personals um und schreibt es fort [39, 41]. Im einzelnen ist er verantwortlich für:

- die physische Sicherheit der Rechner, Netze und Datenträger einschließlich Brandschutz und Schutz vor Naturgewalten
- Kontrolle der Sicherheit von Datenarchiven
- die Konfiguration der Systeme, so daß sie dem Sicherheitskonzept genügen (insbesondere hinsichtlich des Einrichtens der Zugriffsrechte) [5, 7-10, 13, 14, 36]
- die Überwachung des lokalen Netzes auf unerwünschte Datenflüsse, insbesondere auf ungenehmigte Anschlüsse an des Internet (über Modems) [37]
- die Verwaltung von Sicherheitsausweisen, Paßwörtern und Schlüsseln (mit Systemunterstützung) [31, 39, 41]
- die Auswertung von sicherheitsrelevanten Systemaufzeichnungen (gegebenenfalls Alarm und Einleiten von Abwehrmaßnahmen)
- die Kontrolle der Implementation von Software
- die Prüfung der Systemvoreinstellungen auf Sicherheitslücken
- Schulung des IT-Personals und der Benutzer in Sicherheitsfragen
- Erstellung von Verpflichtungserklärungen für IT-Personal und Benutzer (in Abstimmung mit dem Datenschutzbeauftragten und der Personalvertretung) [36]
- technische Beratung des Datenschutzbeauftragten

In großen Institutionen wie z. B. Universitätskliniken erfordern die Tätigkeiten des Datenschutzbeauftragten und des IT-Sicherheitsverantwortlichen je eine volle Stelle, wobei die Aufgaben des letzteren anteilig auf mehrere Personen verteilt sein können und zusätzliche Unterstützung durch das vorhandene IT-Personal notwendig ist. Ferner sollte jede Abteilung mit eigenem IT-Personal auch einen Verantwortlichen für die IT-Sicherheit (Mitglied des IT-Personals in Teilzeit) sowie einen Verantwortlichen für den Datenschutz (Mediziner, ebenfalls in Teilzeit) haben.
In kleinen Institutionen stellt sich das Problem des 'Outsourcing' in der Form des Heranziehens externer Sicherheitsberater. Hier sollte die Verantwortung aber auf jeden Fall im Hause bleiben, zusammen mit ausreichenden Grundkenntnissen von Problemen und Lösungen. Beim Datenschutzbeauftragten wäre an die Bestellung eines gemeinsamen Datenschutzbeauftragten für mehrere Häuser zu denken. Da die differenzierte Kenntnis der lokalen Verhältnisse wichtig ist, wird Outsourcing oft als wenig effektiv und zu teuer erachtet.

7. Empfohlene technische Maßnahmen und Sicherheitsinfrastruktur

Die zunehmende Tendenz auch in größeren Häusern, IT-Systeme auf dem Markt einzukaufen und weitgehend Standard-Software zu verwenden, führt zu einer wachsenden Abhängigkeit von den Herstellern dieser Systeme: Sicherheit muß nämlich schon bei der Konzeption und Entwicklung der Systeme berücksichtigt werden und kann nachträglich auf ein fertiges System in der Regel nicht mehr wirksam aufgepfropft werden [39, 41]. Die zur Zeit angebotenen Systeme erfüllen aber bestenfalls einzelne der folgenden, in offenen Systemen unverzichtbaren Anforderungen:

- verschlüsselte Datenspeicherung
- verschlüsselte Kommunikation (Datenübermittlung)
- überprüfbare Zugriffskontrolle (mandatory) aufgrund einer systemweit definierten Zugriffsmatrix bei dezentraler Verantwortlichkeit für die Zugriffsrechte [11, 36]
- Verbindlichkeit und Integrität von Verordnungen, Leistungsanforderungen, Kommunikation, Dokumentation durch elektronische Unterschrift
- Schaffung der technischen Voraussetzunge zur Integration der künftigen Health Professional Card und zur Einrichtung der dazu nötigen vertrauenswürdigen Schlüsselverwaltungs-Infrastruktur (Thrusted Authorities, Thrusted Third Parties und deren gesicherte Kommunikation) [2, 7, 8, 42]
- Integration von PC- und Netz-Sicherheitssystemen
- sicherer Internet-Anschluß über ein Firewall-System [16, 35, 37]

Die technische Entwicklung hinsichtlich der Umsetzung dieser Anforderungen ist zur Zeit allerdings in starke Bewegung gekommen. Man kann im Moment nur an die Hersteller appellieren, diese Entwicklungen nicht zu verschlafen und insbesondere das kryptographische Know-How schnellstmöglich zu erwerben. Die Verantwortlichen für die Beschaffung von IT-Systemen im Gesundheitswesen sollten von Herstellern und Anbietern mit Nachdruck die Erfüllung der obigen Anforderungsliste verlangen.
Die technischen Systemleistungen sollten für den Benutzer verständlich und durchschaubar konzipiert werden, ihn nicht mit komplizierten Prozeduren belasten und für die seiner Datenhoheit unterstehenden Bestände kontrollierbar sein. Sie dürfen aber von ihm nicht ohne weiteres abgeschaltet oder umgangen werden können.
Für detaillierte technische Empfehlungen ist hier nicht der Ort. Die GMDS-Arbeitsgruppe „Datenschutz in Krankenhausinformationssystemen“ arbeitet auch hieran und wird zu gegebener Zeit ihre Ergebnisse veröffentlichen. Der aktuellste Stand ist stets über den WWW-Server der Arbeitsgruppe [20] abzurufen.

8. Schlußfolgerungen und Ausblick

Die gegenwärtigen offenen Informationssysteme gewährleisten nicht das für den Einsatz im Gesundheitswesen erforderliche Niveau an Datenschutz und Datensicherheit. Die technischen Voraussetzungen sind aber gegeben, diese ohne große Zusatzkosten in die Systeme zu integrieren: Chipkartenleser sind weit verbreitet und ihre Spezifikation für die Belange von Datenschutz und Datensicherheit definiert [1], die Health Professional Card geht in den Feldtest [2, 7, 8], kryptographische Software ist frei verfügbar [34].
Auf der Anwenderseite werden durch konsequente technische Sicherheitsmaßnahmen kaum Beeinträchtigungen der Arbeitsabläufe entstehen. Es ist aber ein nicht zu vernachlässigender organisatorischer Aufwand für die in Abschnitt 6 empfohlenen Maßnahmen nötig. Dieser führt zu einer wesentlichen Verbesserung der Qualität der Informationen und der Erfüllung gesetzlicher Auflagen. Die dadurch entstehenden Kosten werden aber vom Rationalisierungseffekt der Informationstechnik im Gesundheitswesen bei weitem aufgefangen.
Datenschutz und Datensicherheit erfordern Bewußtsein, Bildung und Training bei allen Involvierten vom Manager über das IT-Fachpersonal bis zum Anwender einschließlich des Patienten, Organisation und technische Mittel. Die Zeit ist reif, ernsthafte Anstrengungen für die Verbesserung von Datenschutz und Datensicherheit in Informationssystemen zu unternehmen.

9. Literaturverzeichnis

[1] Arbeitsgemeinschaft „Karten im Gesundheitswesen“, GMD-Forschungszentrum Informationstechnik GmbH: Multifunktionale KartenTerminals (MKT) für das Gesundheitswesen

und andere Anwendungsgebiete. Spezifikation Version 0.9, August 1995.
[2] Arbeitskreis „Health Professional Card“ der Arbeitsgemeinschaft „Karten im Gesundheitswesen“: Deutscher Modellversuch „Health Professional Card (HPC)“, Göttingen, Oktober 1996.
[3] Bakker, A. R., et al. (Edrs.): Caring for Health Information. Safety, Security and Secrecy. North-Holland, Amsterdam 1995.
[4] Barber, B., Treacher, A., and Louwerse, K.: Towards Security in Medical Telematics. Legal and Technical Aspects. IOS Press, Amsterdam, Washington DC, Tokio, 1995.
[5] Blobel, B. (Hrg.): Datenschutz in medizinischen Informationssystemen. Vieweg, Braunschweig, Wiesbaden, 1995
[6] Blobel, B., and Holena, M.: Advanced Healthcare System Architecture Using Middleware Concepts - A Comparative Study. HANSA Deliverable, September 1996.
[7] Blobel, B.: A regional clinical cancer documentation system for an optimal shared health care in cancer. In: Brender, J., Christensen, J. P., Scherrer, J.-R., McNair, P. (Edrs.): Medical Informatics Europe '96, pp 1019-1026. IOS Press, Amsterdam 1996.
[8] Blobel, B.: Clinical record systems in oncology. Experiences and developments on cancer registers in eastern Germany. In: Anderson, R. A., et al. (Edrs.): Personal Information - Security, Engineering and Ethics. Conference Preprint, pp 37-54. International Workshop, Cambridge 21-22 June, 1996, to appear in Springer LNCS.
[9] Blobel, B.: Datensicherheitsaspekte beim standardisierten Datenaustausch im Gesundheitswesen. In: Mayr, H. T.: Informatik '96. Beherrschung von Informationssystemen, Band 8, S. 155-165. R. Oldenbourg Verlag, München und Wien 1996.
[10] Blobel, B.: GSG `93 und GNG `95 - Umstrukturierung der Krankenhaussysteme. klinikarzt Nr. 10/24 (1995) 491-499.
[11] Blobel, B.: Modelling for design and implementation of secure health information systems. In: Bakker, A. R., et al. (Edrs.): Communicating Health Information in an Insecure World. Conference Preprint, pp 149-156. Data Protection and Security Working Conference, Helsinki 30 September - 3 October 1995, to appear at North-Holland, Amsterdam.
[12] Blobel, B.: Moderne Architektur für ein integriertes Krankenhausinformationssystem - Grundzüge und Magdeburger Realisierungsbeispiel. In: Pöppl, S. J., et al. (Hrg.): Medizinische Informatik - Ein integrierender Teil arztunterstützender Technologien. S. 46-49. MMV Medizin Verlag München, München 1994
[13] B.Blobel: Datensicherheit in offenen Gesundheitsinformationssystemen, Teil 1. krankenhausumschau 11 (1996) S. 852-857.
[14] B.Blobel: Datensicherheit in offenen Gesundheitsinformationssystemen, Teil 2. krankenhausumschau 12 (1996).
[15] CERT Coordination Center. Im World Wide Web unter http://www.cert.org [http://www.cert.org]
[16] Chapman, D. B., and Zwicky, Elizabeth D.: Building Internet Firewalls. O'Reilly Associates, Inc., Sebastopol 1995.
[17] Datenschutzkommission Rheinland-Pfalz, Mainz. Datenschutzrechtliche Anforderungen an wissenschaftlichen Forschungsvorhaben, 1987
[18] Der Deutsche Bundestag: Multimedia-Gesetz (Referenten-Entwurf) Bonn, 1996. Im World Wide Web unter http://www.fitug.de/ulf/politik/iukdg.html [http://www.fitug.de/ulf/politik/iukdg.html]
[19] Ellsässer, K.-H., Köhler, C. O.: Shared Care: Konzept einer verteilten Pflege - Kurz- und langfristige Perspektiven in Europa. Informatik, Biometrie und Epidemiologie in Medizin und Biologie 24 (1993) H. 4, S. 188-198.
[20] GMDS-Arbeitsgruppe Datenschutz in Krankenhausinformationssystemen . Im World Wide Web unter http://www.uni-mainz.de/FB/Medizin/IMSD/AGDatenschutz [http://www.uni-mainz.de/FB/Medizin/IMSD/AGDatenschutz]
[21] HANSA Consortium: Middleware Approaches in Healthcare. A Presentation for the Healthcare

Management (Draft). August 1996.
[22] Health Level Seven Inc.: HL7 Version 2.2, 1995.
[23] HL7 Technical Steering Committee Retreat: HL7 Version 3, 1996
[24] Klein, G. (Edr.): Trusted Health Information Systems, Part 1 - 2, SPRI, Stockholm 1994.
[25] McCurley, K. S.: Protecting privacy and information integrity of computerized medical information. 1995. World Wide Web at http://www.cs.sandia.gov/~mccurley/health.html [http://www.cs.sandia.gov/~mccurley/health.html]
[26] OMG: Common Facilities Architecture. Revision 4.0, 1995.
[27] OMG: Common Secure Interoperability. OMG Doc.No. orbos/96-06-20.
[28] OMG: CORBA Services: Common Object Services Specification. Revised Edition, 1996.
[29] OMG: The Common Object Request Broker: Architecture and Specification. Revision 2.0, 1995.
[30] OMG: The CORBA Security Specification. OMG Doc.No. 95-12-01.
[31] Pommerening, K.: Datenschutz und Datensicherheit. BI-Wissenschaftsverlag, Mannheim, Wien, Zürich, 1991
[32] Pommerening, K.: Pseudonyme - ein Kompromiß zwischen Anonymisierung und Personenbezug. In: Trampisch, H. J., Lange, S. (Hrg.). Medizinische Forschung - ärztliches Handeln. S. 329-333. MMV Medizin Verlag, München 1995
[33] Ruhland, Ch.: Informationssicherheit in Datennetzen. DATACOM-Verlag 1993
[34] Schneier, B.: Applied Cryptography. Second Edition. John Wiley & Sons, Inc., New York 1996.
[35] Security Issues for the Internet and the World Wide Web; CTR Report No 8, Computer Technology Research Corp., Charleston 1996.
[36] Seelos, H-J.: Informationssysteme und Datenschutz im Krankenhaus. DuD-Fachbeiträge 14. Vieweg, Braunschweig, Wiesbaden, 1991
[37] Stallings, W.: Network and Internet Security. Principles and Practice. Prentice Hall, Hemel Hempstead 1995.
[38] Swedish Institut for Health Service Development: Trusted Health Information Systems. Version 2, 1994-11-30.
[39] The Commission of the European Communities DG XIII/F AIM. Data Protection and Confidentiality in Health Informatics, AIM Working Conference, Brussels, 19-21 March 1990, IOS Press, Amsterdam, Washington DC, Tokio, 1991.
[40] The European Parliament and the Council of the European Union: Directive 95/ /EC of the European Parliament and of the Council of the European Union on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. Im World Wide Web unter http://www.rewi.hu-berlin.de/Datenschutz/EURichtlinie/directive.html [http://www.rewi.hu-berlin.de/Datenschutz/EURichtlinie/directive.html].
[41] The SEISMED Consortium (Edr.): Data Security for Health Care, Volume I - III. IOS Press, Amsterdam 1996.
[42] TRUSTHEALTH1: Functional Specification of TTP Services (Version 1.0). 1996-07-29.
[43] TRUSTHEALTH1: Selection of Security Services and Interfaces (Version 1.0). 1996-07-29.
[44] Zentralstelle für Sicherheit in der Informationstechnik, Köln. IT-Sicherheitskriterien - Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT), 1989

Fußnoten

(1) Otto-von-Guericke-Universität Magdeburg, Medizinische Fakultät, Institut für Biometrie und Medizinische Informatik
(2) Johannes-Gutenberg-Universität Mainz, Fachbereich Medizin, Institut für Medizinische Statistik und Dokumentation
(3) Dabei werden die von der Arbeitsgruppe Datenschutz in Krankenhausinformationssystemen

der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e. V. [20] erarbeiteten Ergebnisse berücksichtigt.
(4) Strafgesetzbuch
(5) Bundesdatenschutzgesetz
(6) Entsprechend der EU-Direktive [40] unterliegen alle Personen, die im Rahmen ihrer Tätigkeit Zugang zu personenbezogenen Daten haben, einer Schweigepflicht, unabhängig davon, ob eine solche in einer Berufsordnung verankert worden ist.
(7) §40 BDSG, vgl. auch [7].
(8) Health Level 7, ein Protokoll zur systemunabhängigen Datenkommunikation im Gesundheitswesen [22, 23]
(9) Common Object Broker Architecture ist die objekt-orientierte Architektur der Object Management Group (OMG) für verteilte kooperierende Informationssysteme [26-30].
(102) Distributed Healthcare Environment beschreibt die europäische Architektur für Gesundheitsinformationssysteme und ihre Standardisierung [6, 21].

Allgemeine Grundsätze für den Datenschutz in Krankenhausinformationssystemen

Die zunehmende Installation und Erweiterung von Krankenhaus-Informations- und Kommunikationssystemen erfordert besondere Anstrengungen, um den Anforderungen des Datenschutzes gerecht zu werden. Der Patient darf erwarten, dass seine persönlichen Daten im Medizinbetrieb mit äußerster Sorgfalt und Vertraulichkeit behandelt werden. Dieser Anspruch erwächst aus dem Grundrecht auf informationelle Selbstbestimmung und der ärztlichen Schweigepflicht. Vorschriften und Maßnahmen zum Datenschutz im Krankenhaus tragen dazu bei, dass das Vertrauensverhältnis zwischen Patient und Arzt und das Persönlichkeitsrecht des Patienten bei der Datenverarbeitung im Krankenhaus gewahrt bleiben. Ebenso sind die persönlichen Daten der Beteiligten im Gesundheitsprozess entsprechend der Datenschutzgesetzgebung zu schützen. Der Datenschutz muss bereichsspezifisch, insbesondere medizinspezifisch gestaltet werden.

Die Spezifikation des Datenschutzbedarfs muss von der arbeitsteiligen Organisation des Krankenhauses und der ärztlichen Schweigepflicht ausgehen. Der arbeitsteilig organisierte Krankenhausbetrieb kann unter Verweis auf die ärztliche Schweigepflicht und das Zusammenarbeitsgebot der einzelnen Aufgabenträger, unbeschadet seiner rechtlichen Organisationsform und organisatorischen Binnenstruktur, grundsätzlich als „speichernde Stelle bei gemeinsamer Aufgabe“ im Sinne des Datenschutzrechtes definiert werden. Sowohl die ärztliche Schweigepflicht (§ 203 Abs. 1 Nr. 1 StGB) als auch das „Datengeheimnis“ (§ 5 BDSG), das den Beschäftigten im Krankenhaus die Verarbeitung von Patientendaten nur im Rahmen der Zweckbestimmung des Behandlungsvertrages gestattet, verbieten es aber, den Krankenhausbetrieb als eine „informationelle Einheit“ anzusehen, in der uneingeschränkt Patientendaten ausgetauscht und verwendet werden dürfen. Die Entscheidung über die Übertragung von Zugriffsrechten auf die medizinischen Daten eines Patienten oder ihre Verwendung liegt bei der behandelnden Fachabteilung; dies gilt auch für archivierte Daten. Daten werden unter Verantwortung der erhebenden Stelle oder der Stelle ihrer überwiegenden Verwendung gespeichert und nur bei Bedarf nach einem überprüfbaren Verfahren anderen Leistungsstellen offenbart. Die Distribution von Patientendaten innerhalb des Krankenhausbetriebes als „speichernde Stelle“ stellt datenschutzrechtlich keine Übermittlung, wohl aber eine Offenbarung im Sinne Par. 203 StGB dar, die einer Befugnisnorm bedarf (§ 4 BDSG, §9 MBO-Ä). Die Verarbeitung von Patientendaten im Rahmen der Zweckbestimmung des Behandlungsvertrages und das Anerkenntnis des Patienten eines arbeitsteilig strukturierten Krankenhausbetriebes legitimieren unter dem Gebot der Zweckbindung und Erforderlichkeit eine innerbetriebliche Offenbarung von Patientendaten zur Erfüllung des Behandlungsvertrages konkludent, insoweit keine besonderen bereichsspezifischen Rechtsvorschriften als Befugnisnormen gelten. Die Offenbarung ist nur gestattet, wenn sie im Rahmen der Behandlung oder aufgrund rechtlicher Vorschriften nötig ist; nur die erforderlichen Teilinformationen aus der Krankenakte sollen dabei offenbart werden. Auch die Krankenhausverwaltung darf nur zu den Daten Zugang haben, die für ihre Zwecke erforderlich sind. [1)]

Patientendaten sind nach dem Stand der Technik zu schützen, wobei aber das Prinzip der Verhältnismäßigkeit zu beachten ist. Insbesondere für medizinische Daten ist wegen ihrer Sensitivität ein hoher Sicherungsaufwand geboten. Durch technische und organisatorische Maßnahmen muss gewährleistet sein, dass nur der zuständige Arzt und, soweit für die Behandlung nötig, mitbehandelnde Ärzte und Pflegepersonal die Patientendaten lesen oder im zulässigen Rahmen weitergeben können. Als technische Absicherung müssen Patientendaten (wie auch andere möglicherweise vertrauliche Daten) per Systemvoreinstellung gegen Einsichtnahme und Übermittlung geschützt sein; die jeweilige Freigabe muss ein bewusster Akt sein und richtet sich

nach der im Datenmodell definierten Zugriffsmatrix (Sicherheitsprinzip des geschlossenen Systems [2]).

Die Sicherheitsmaßnahmen sollen die Aufmerksamkeit des Arztes nicht vom Patienten ablenken. Zwar sind Datenschutzmaßnahmen ohne Mitwirkung der Beteiligten nicht zu verwirklichen, aber die Belastung des medizinischen Personals durch organisatorische und technische Verfahren ist zu minimieren. Der sachgerechte Umgang mit den Patientendaten darf durch Schutzmaßnahmen nicht beeinträchtigt werden. Die Verfügbarkeit der Daten, besonders in kritischen Situationen, ist im Interesse des Patienten zu gewährleisten. Technische Datenschutzmaßnahmen sollen den freien Austausch nichtgeschützter Informationen möglichst wenig behindern, z. B. den Zugriff auf externe Informationsdienste wie DIMDI und elektronische Post. Auch die Verwendung der Daten für Forschungszwecke soll, soweit die Datenschutzanforderungen für wissenschaftliche Forschungsvorhaben (§40 BDSG) erfüllt sind, gewährleistet sein.

Die technischen und organisatorischen Datenschutzmaßnahmen in einer Klinik sind nicht nebenbei zu erledigen. Sie erfordern die Schaffung einer entsprechenden Infrastruktur und eine klare Festlegung der Verantwortlichkeiten sowie die Einplanung eines angemessenen finanziellen und personellen Aufwands, insbesondere für einen Sicherheitsverantwortlichen. Auch der Datenschutzbeauftragte der Klinik benötigt für seine Aufgaben ausreichende Mittel und Unterstützung.

Für medizinische Anwendungssysteme aller Arten sind geeignete technische Standards in Anlehnung an die IT-Sicherheitskriterien [3] wünschenswert, die man den Herstellern gegenüber durchsetzen kann und die die Planung und Beurteilung von Systemen erleichtern. Insbesondere ist eine geeignete kryptographische Infrastruktur zu definieren und soweit wie möglich zu schaffen. Datenschutzinhalte und -ziele sowie Sicherheitsanforderungen sind so zu spezifizieren, dass Hersteller genügend genaue Richtlinien in die Hand bekommen. Die technischen Schutzmaßnahmen sollen als Systemleistung konzipiert werden, die vom Benutzer kontrollierbar, aber nicht ohne weiteres abschaltbar ist.

Die Notwendigkeit, aber auch die Möglichkeit, realisierbare Sicherheitskonzepte zu entwickeln, ist gegeben. Die Zeit ist reif, daraus funktionsfähige Systeme zusammenzubauen, anstatt weiterhin auf unwirksame oder schwache vermeintliche Sicherheitsmaßnahmen zu vertrauen.

---

[1] Hans-Jürgen Seelos. Informationssysteme und Datenschutz im Krankenhaus. DuD-Fachbeiträge Band 14, Vieweg, Braunschweig, Wiesbaden, 1991, ISBN 3-528-05185-X

[2] Klaus Pommerening. Datenschutz und Datensicherheit,4, II.4. BI-Wissenschaftsverlag, Mannheim, Wien, Zürich, 1991, ISBN 3-411-15171-4

[3] Zentralstelle für Sicherheit in der Informationstechnik. IT-Sicherheitskriterien. Bundesanzeiger-Verlagsges. mbH, Köln, 1989, ISBN 3-88784-192-1