

Informatik - Fachberichte

Herausgegeben von W. Brauer

im Auftrag der Gesellschaft für Informatik (GI)

13

Wilhelm Steinmüller
Leonhard Ermer
Wolfgang Schimmel

Technische Hochschule Darmstadt
FACHBEREICH INFORMATIK
B I B L I O T H E K
Inventar-Nr.: 3336
Sachgebiete: _____
Standort: _____

Datenschutz bei riskanten Systemen
Eine Konzeption entwickelt am Beispiel
eines medizinischen Informationssystems

Fachbereichsbibliothek Informatik
TU Darmstadt



Springer-Verlag
Berlin Heidelberg New York 1978

I N H A L T S V E R Z E I C H N I S

	<u>Zum Geleit (W. Brauer)</u>	<u>VII</u>
	<u>Vorwort</u>	<u>IX</u>
<u>1.</u>	<u>Rahmenbedingungen der Datenschutzkonzeption für ein INA</u>	<u>1</u>
1.1	ADV und ärztliche Schweigepflicht	2
1.2	Das Projekt "INA" - zugleich ein Geleitwort (O.P.Schaefer)	6
1.2.1	Entstehung und förderungspolitischer Zusammenhang	6
1.2.2	Einige Lehren aus der Projektarbeit	10
1.3	Das Teilprojekt "Datenschutzkonzeption für ein INA"	12
1.3.1	Schwierigkeiten bei der Durchführung	12
1.3.2	Literaturlage	13
1.3.3	Neuheit der Problemstellung	14
1.4	Ziel und Aufbau dieser Studie	15
<u>2.</u>	<u>Deskriptive Vorgaben: Der hypothetische Soll-Zustand von INA</u>	<u>17</u>
2.1	Terminologie	18
2.2	Das systemanalytische Beschreibungsverfahren	22
2.3	Hypothetisch-empirische Annahmen im einzelnen	24
2.3.1	INA-Hardware-Konfiguration	24
2.3.2	Datenarten	27
2.3.3	Datenbahnen und -operationen; Software	28
2.3.4	Informationsorganisation	30
2.3.5	Rechtliche und Kontrollorganisation	31
2.3.6	Umweltrelation: Interessenten und Umsystem	32
<u>3.</u>	<u>Normative Vorgaben: Rechtliche Randbedingungen (W. Schimmel)</u>	
3.1	Ärztliche Schweigepflicht	34
3.1.1	Gesetzliche Grundlagen	34
3.1.2	Umfang und Voraussetzungen der ärztlichen Schweigepflicht	40
3.1.3	Befugnis zur Weitergabe von Informationen, die der Schweigepflicht unterliegen	44
3.1.4	Datenverkehr innerhalb von INA	46
3.1.5	Wissenschaftliche und gesundheitspolitische Auswertung	49
3.1.6	Auskunftsrecht des Patienten	50
3.2	Datenschutzrecht	51
3.2.1	Geltung des BDSG	51
3.2.2	Inhalt des BDSG	53
3.3	Krankenhausgesetze	69
3.4	Ergebnis	70
<u>4.</u>	<u>Das System des Datenschutzes</u>	<u>71</u>
4.1	<u>Grundannahmen der bisherigen Datenschutztheorie</u>	<u>72</u>
4.1.1	Komplementarität von Datenschutz und Datenverarbeitung	72
4.1.2	Informationskontrolle und Datenverkehrsrecht	73
4.1.3	Datenschutz als Organisationsproblem	75
4.1.4	Spezifische Leistung von Informationssystemen	77
4.1.5	Das System und seine Umwelt	79
4.2	<u>Unzureichende Lösungsvorschläge</u>	<u>82</u>
4.2.1	"Privatsphäre"	82
4.2.2	"Personenbezogene Daten"	84
4.2.3	"Sensitive Daten"	85
4.2.4	"Verrechtlichung"	86
4.2.5	"Einwilligungstheorie"	86
4.2.6	"Entfremdungstheorie"	87
4.2.7	"Kein Datenschutz für Planung und Forschung notwendig"	88
4.2.8	Datenschutzgesetze	89

4.3	<u>Skizze des Lösungsprinzips</u>	90
4.3.1	Umfassender Schutzbereich	90
4.3.2	Gesamtplanung des Datenschutzes	91
4.3.3	Flankierende Maßnahmen	93
4.3.4	Selbst- und Fremdkontrolle	94
4.3.5	Kontroll- und Abwehrrechte der Betroffenen	95
4.4	<u>Spezielle Datenschutzhypothesen</u>	96
4.4.1	Postulat I der ökonomischen Realisierung	96
4.4.2	Postulat II des Vorrangs der technischen Realisierung	97
4.4.3	Postulat III der möglichst dichten Abschottung	98
4.4.4	Postulat IV der Ausschließung des undichten Dritten	99
4.4.5	Postulat V der definierten Struktur	100
4.4.6	Postulat VI der möglichsten Einfachheit	101
4.4.7	Postulat VII der verteilten Kontrolle	101
4.4.8	Postulat VIII des zusätzlichen Schutzes	103
4.4.9	Postulat IX der Beteiligung der Betroffenen	103
4.4.10	Postulat X des überschaubaren Systems	104
5.	<u>Datenschutzkonzept - Realisierungsvorschlag</u>	105
5.1	<u>Vorschläge auf der Ebene der Hardware</u> (einschließlich Betriebssystem)	107
5.2	<u>Vorschläge auf der Ebene der Daten</u>	108
5.2.1	Depersonalisierung durch Patientenummer	108
5.2.2	Arztnummer	109
5.2.3	Verschlüsselung	110
5.2.4	Bedingte Aufhebung der Depersonalisierung	110
5.2.5	Manuelle Informationsverarbeitung	111
5.2.6	Spezielle Datenprobleme	112
5.2.7	Auswirkungen dieser Vorschläge	115
5.3	<u>Vorschläge auf der Ebene der Informationsbahnen und -programme</u>	
5.3.1	Minimierung des manuellen Informationsverkehrs	116
5.3.2	Programmkontrolle	117
5.3.3	Funktionsentmischung von Daten	119
5.4	<u>Vorschläge auf der Ebene der Informationsorganisation</u>	120
5.4.1	Differenzierung von allgemeiner und Informationsorganisation	
5.4.2	Elemente der Informationsorganisation	121
5.4.3	Datei- und Datenbankorganisation	123
5.4.4	Zugriffs- und Bedienungsrechte	123
5.4.5	Drei Ebenen der Verantwortung	124
5.4.6	Folgen der ärztlichen Gesamtverantwortung	126
5.4.7	Kontrollstelle	127
5.5	<u>Vorschläge auf der Ebene der Benutzer</u>	129
5.5.1	Praxis	129
5.5.2	Labor und apparative Zentren	130
5.5.3	Rechenzentrum	130
5.5.4	Das manuelle Teilsystem	131
5.5.5	Patient	132
5.5.6	Sonderfälle	132
5.6	<u>Vorschläge auf der Ebene der Interessenten</u>	134
5.6.1	Prinzipielle Schwierigkeit	135
5.6.2	Interimslösung entsprechend "Datalag"	136
5.6.3	Kontrollgremium und betrieblicher Datenschutzbeauftragter	139
5.6.4	Anforderungen an Interessenten	140
5.6.5	Einzelprobleme	143

5.7	<u>Vorschläge auf der Ebene der rechtlichen Organisation</u>	149
5.7.1	Rechtliche Organisationsform	149
5.7.2	Satzung	152
5.7.3	Einwilligungsrevers des Patienten	154
5.7.4	Beirat	155
6.	<u>Datensicherungskonzept (L.Ermer)</u>	157
6.1	<u>Problemstellung</u>	157
6.2	<u>Begriffsbestimmung</u>	158
6.2.1	Datensicherung i.e.S. und i.w.S.	158
6.2.2	Ziele der Datensicherung	159
6.2.3	Methoden der Datensicherung	160
6.3	<u>Rechtliche Randbedingungen der Datensicherung</u>	161
6.3.1	Aspekt des Datenschutzes	161
6.3.2	Aspekt der Datensicherung i.e.S.: Haftungsproblem	162
6.4	<u>Gefährdung des EDV-Systems von INA im einzelnen</u>	166
6.4.1.	Gefährdung durch Fehler	166
6.4.2.	Gefährdung durch Katastrophen	167
6.4.3.	Gefährdung durch Mißbrauch	167
6.5	<u>Maßnahmen zur Datensicherung im einzelnen</u>	168
6.5.1	Doctor's Office Computer	168
6.5.2	Doctor's Office Terminal	181
6.5.3	Doctor's Interchange Computer	184
6.6	<u>Zusammenfassung</u>	186
7.	<u>Verallgemeinerung für riskante Systeme</u>	193
8.	<u>Anhang: Ausgewählte Rechtstexte</u>	197
9.	<u>Register und Verzeichnisse</u>	
9.1	Abkürzungsverzeichnis	
9.2	Gesetzesregister	
9.3	Verzeichnis der Abbildungen	
9.4	Literaturverzeichnis	
9.5	Sachregister	