

Protokoll der 30. Sitzung der AG „Datenschutz in Gesundheitsinformationssystemen“ (DGI)

Zeit: 08. Mai 2014, 10:00 bis 12.00 Uhr

Ort: conhIT, Raum Passau 1

Protokoll: Jens Schwanke

Teilnehmer:

Name	Anwesend	Abgesagt	Keine Rückmeldung
Alkemade, Jan		X	
Bahls, Thomas			X
Blobel, Bernd		X	
Brenner, Hubert		X	
Brunner, Manfred			X
Bürger, Norman	X		
Drepper, Johannes		X	
Heidenreich, Georg		X	
Isele, Christoph	X		
Lautenbacher, Heinrich		X	
Pommerening, Klaus	X		
Sax, Ulrich (Pate AG)			X
Schütze, Bernd	X		
Schwanke, Jens	X		
Stahmann, Alexander		X	
Wichterich, Eric		X	
Höppner, Carsten	X		

Tagesordnung

Top 1. Begrüßung

Herr Schütze begrüßt alle Teilnehmer der AG-Sitzung. Nachfolgend stellen sich die Teilnehmer gegenseitig kurz vor, indem sie ihre Schwerpunkte im Bereich ihrer beruflichen Tätigkeiten darstellen.

Top 2. Formalia

1. Die Tagesordnung wird angenommen.
2. Das Protokoll der letzten Sitzung vom 08. Mai 2014 wird angenommen.

Top 3. Vorstellung des Jahresberichts 2013

Herr Schütze spricht kurz die Problematik des Jahresberichts an. Ein Jahresbericht wird am Anfang eines Jahres für das vergangene Jahr erstellt und enthält daher Planungen für das laufende Jahr, wobei die Planungen ggfs. schon umgesetzt wurden.

Herr Schütze bittet daher die Teilnehmer, gewünschte Themen für das Jahr 2015 der AG-Leitung im Verlauf des Jahres 2014 per E-Mail mitzuteilen.

Top 4. Empfehlungen der AG DGI

Herr Schütze erklärt, dass die AG derzeit sieben Empfehlungen auf der Webseite zur Verfügung stellt und einige der Empfehlungen überarbeitet werden müssten. Daher hat er in der Einladung zur AG-Sitzung darum gebeten, die Empfehlungen kritisch durchzusehen. Herr Schütze schlägt vor, dass die Teilnehmer gemeinsam über den Umgang mit den Empfehlungen abstimmen, ob diese gültig bleiben, überarbeitet werden müssen oder ggf. als ungültig erklärt werden. Die Teilnehmer sind mit dem Vorgehen einverstanden.

Nachfolgend die Ergebnisse der Abstimmung:

1. Empfehlungen zur Sicherheit des Intranets von Krankenhäusern (bleibt gültig)
2. Bemerkungen zur Nutzung von E-Mails im Gesundheitswesen (für ungültig erklärt; verbleibt aber auf der Webseite mit Verweis auf BSI)
3. Sicherheitsempfehlungen zum Betrieb von Servern und lokalen Netzen in Krankenhäusern (für ungültig erklärt; verbleibt aber auf der Webseite mit Verweis auf BSI)
4. Formulierungshilfen für einen Fernwartungsvertrag aus der Sicht des Datenschutzes (bedarf einer Überarbeitung)
5. Zugriff auf Patientendaten im Krankenhaus (bleibt gültig)
6. Sicherheitsempfehlungen zu Modem-Verbindungen im Krankenhaus (für ungültig erklärt; verbleibt aber auf der Webseite mit Verweis auf BSI)
7. Datenschutz und Datensicherheit in Informationssystemen des Gesundheitswesens (für ungültig erklärt; verbleibt aber auf der Webseite mit Verweis auf OH-KIS)

Die Überarbeitung erfolgt per Mail, d.h. die Empfehlung bzgl. der Formulierungshilfen für einen Fernwartungsvertrag wird als Word-Datei zwecks Überarbeitung an die AG gemailt.

Top 5. Stellungnahme zur OH KIS

Herr Schütze erläutert kurz, dass er die Kommentierung der OH-KIS an Herrn Schmücker weitergeleitet hat. Dieser wollte die Kommentierung zur OH-KIS seitens der AG bis zu conhIT 2014.

Generell muss die Stellungnahme noch durch das Präsidium freigegeben werden. Herr Schütze geht davon aus, dass es noch einige sprachliche Überarbeitungen gibt.

Herr Pommerening merkt an, dass die Kommentierung gegenüber den Datenschutzbeauftragten diplomatischer formuliert sein sollte. Herrn Schütze erklärte, dass als Ziel der Stellungnahme die Kritik an der OH KIS wie beispielsweise die praxisferne deutlich herausgearbeitet werden muss, zugleich die Bereitschaft zur Kooperation dargestellt werden muss.

Herr Isele merkt an, dass generell die IT-Leiter der Krankenhäuser nicht in die Kommentierung der OH-KIS involviert waren.

Herr Schütze erklärt, dass für die Krankenhausgesellschaft NRW fünf Personen (ein IT-Leiter, ein Berater aus dem Krankenhausumfeld, zwei Mitarbeiter der Krankenhausgesellschaft NRW und Herr Schütze selbst) eine Kommentierung der OH-KIS durchführten und diese an den Bundesverband der Krankenhausgesellschaft weiterleiteten. Diese „NRW-Kommentierung“ ist aber innerhalb der Kommentierung, welche die Krankenhausgesellschaft an die Aufsichtsbehörden weitergaben, nicht berücksichtigt worden.

Herr Pommerening macht noch einmal deutlich, dass Diplomatie wichtig ist. Er merkt ebenso an, dass es durch die EU-Datenschutzverordnung zu Änderungen kommen wird. Dies würde sich auch auf die Themenbereiche der Arbeitsgruppe auswirken.

Herr Schütze merkt an, dass in dem derzeitigen Vorschlag einer EU-Datenschutzgrundverordnung viele Themenbereiche (z. B. Gesundheitswesen und Arbeitsrecht) herausgenommen wurden und durch das jeweilige Landesrecht von jedem EU-Land selbst geregelt werden sollen. Weiterhin weist er darauf hin, dass der derzeitige Vorschlag einer geplanten EU-Datenschutzgrundverordnung in der vorliegenden Form wohl kaum verabschiedet wird, da die EU-Kommission jetzt neu besetzt wird und nicht zu erwarten ist, dass die kommende EU-Kommission den Vorschlag 1:1 übernimmt. Er schlägt vor, dass die Arbeitsgruppe ein Review der EU-Datenschutzverordnung durchführt, wenn die nächste Kommentierung eines Entwurfs ansteht.

Top 6. Verschiedenes

1. Stellungnahme zu §203 StGB

Herr Schütze diskutiert die Themenpunkte „Stellungnahme zu §203 StGB“ und „Empfehlung zur Auftragsdatenverarbeitung“ gemeinsam.

(Anmerkung des Protokollanten: Die Diskussion findet sich unter TOP 6.2)

2. Empfehlung zur Auftragsdatenverarbeitung

Herr Schütze berichtet, dass die Datenschutz-Aufsichtsbehörden bzgl. des §203 StGB eine Gesetzesänderung vorschlagen wollen. Herr Pommerening fragt, wer die zuständige Aufsichtsbehörde ist. Herr Schütze erklärt, dass dies der Düsseldorfer Kreis ist.

Herr Schütze weist daraufhin, dass der bvitg ebenfalls an dem Thema bzgl. der §203 StGB-Problematik arbeitet. Bei einem Telefonat mit Herrn Mittelstaedt vom bvitg stellte sich heraus, dass eine Zusammenarbeit bzgl. dieser Thematik sowie der Erstellung eines „Muster-ADV-Vertrages“ viel Synergieeffekte bietet. Nach Rücksprache mit der jeweiligen Arbeitsgruppen des Fachbereichs Medizin in der GDD sowie dem BvD wurde die Gründung einer AG bestehend aus Mitgliedern der vier Organisationen beschlossen.

Ziel ist es einen Mustervertrag zur Auftragsdatenverarbeitung zu erstellen sowie einen Vorschlag zur Änderung von §203 StGB zu erarbeiten. Die Arbeitsgruppe setzt sich seitens der GMDS-AG aus folgenden Mitgliedern zusammen: Bernd Schütze, Johannes Drepper, Jens Schwanke sowie Christoph Isele (wenn dieser nicht seitens des bvitg schon in der AG mitarbeitet). Grundlage der Arbeitsgruppe bilden die Vorarbeiten von Herrn Schütze, die an bvitg, GDD und BvD weitergeleitet wurden.

Herr Höppner fragt, wie mit bestehenden Verträgen zur Auftragsdatenverarbeitung (ADV) umgegangen werden soll.

Herr Isele erläutert, dass diese durch neue Verträge ersetzt werden können. Seitens Siemens würden solche komplexen Verträge bereits erstellt werden.

Herr Schütze merkt an, dass kleinere Firmen keine eigene Rechtsableitung haben und daher solche komplexen Verträge nur schwer umzusetzen sind. Gleiches gilt für kleinere Krankenhäuser sowie Arztpraxen. Die Ergebnisse sollen im Rahmen der conhIT 2015 vorgestellt werden. Herr Pommerening regt an, die ADV-Vertragsvorlagen der Landesdatenschutzbeauftragten zu berücksichtigen.

Herr Schütze würde gerne eine kommentierte Checkliste für ADV-Verträge zusätzlich zum Mustervertrag erstellen. Diese soll ähnlich zu Checkliste für Einwilligungserklärungen der TMF gestaltet sein.

Herr Pommerening fragt was an §203 geändert werden soll.

Herr Schütze erklärt, dass die Auslagerung von Aufgaben an Externe, insbesondere die Fernwartung, nicht durch den im §203 StGB vorhandenen Gehilfen-Begriff abgedeckt ist, so dass eine Fernwartung zwar datenschutzrechtlich einwandfrei angebildet werden kann, strafrechtlich jedoch eine unerlaubte Offenbarung darstellt, d.h. eine Ärztin bzw. ein Arzt gibt unerlaubt Patientengeheimnisse an die Mitarbeiter der fernwartenden Firma weiter und macht sich so strafbar.

Die Mitarbeit von Volljuristen an dem Vorschlag zur Änderung von §203 StGB erscheint unabdingbar, daher hat Herr Schütze bereits Volljuristen, die in der GDD im Arbeitskreis Medizin mitarbeiten, um Mitarbeit gebeten.

Herr Pommerening merkt an, dass es ein enger Zeitplan ist um alles bis zur conhIT 2015 fertigzustellen.

3. Name der Arbeitsgruppe

Herr Schütze regt eine Namensänderung der Arbeitsgruppe „Datenschutz in Gesundheitsinformationssystemen“ an. Hintergrund ist, dass die Kommentierung des IT-Sicherheitsgesetzes an der GMDS vorbei gegangen ist. Um derartige Fragestellungen in der GMDS zu adressieren ist eine Arbeitsgruppe nötig, die Fragestellungen zur IT-Sicherheit bearbeitet.

Herr Pommerening merkt an, dass die Arbeitsgruppe schon immer die IT-Sicherheit als Teil des Aufgabengebietes hatte.

Herr Isele bekräftigt dies, da echter Datenschutz ohne IT-Sicherheit nicht möglich ist.

Herr Schütze schlägt die Namensänderung der AG in „*Datenschutz und IT-Sicherheit im Gesundheitswesen*“ vor.

Herr Schwanke leitet eine formelle Abstimmung ein: alle anwesenden Mitglieder stimmen für eine Namenänderung, keine Enthaltungen oder Gegenstimmen. Herr Schütze wird das Ergebnis an den Fachausschuss für Med. Informatik der GMDS weiterleiten und um eine Namensänderung bitten.

4. conhIT als Treffpunkt?

Herr Schütze möchte von den anwesenden Mitgliedern der Arbeitsgruppe wissen, ob die conhIT als Treffpunkt auch für das nächste Jahr genutzt werden soll.

Herr Isele schlägt vor den Termin nach 11 Uhr anzusetzen, da dann kostenlose Ausweise möglich sind. Ebenso empfiehlt er die Sitzung nicht parallel zu ähnlichen Themenbereichen zu legen.

Alle anwesenden Mitglieder begrüßen die conhIT als Treffpunkt der AG und stimmen einem Treffen im Rahmen der conhIT für 2015 zu.

Herr Schwanke regt an, kurz über die Sitzungstermine der Arbeitsgruppe im Jahr 2014 zu sprechen. Eine weitere Sitzung ist am 19.11.2014 gemeinsam mit der TMF AG Datenschutz geplant. Herr Schwanke fragt daher ob es eine dritte Sitzung im Rahmen der GMDS in Göttingen geben soll. Die Teilnehmer halten dies nicht für notwendig, da zwei Termine ausreichend sind.

Herr Isele weist darauf hin, dass bei einem Treffen auf der GMDS-Jahrestagung die AG für neue Mitglieder der GMDS besser ansprechbar ist. Dem stimmen alle zu.

Herr Schütze regt an, dass im Rahmen GMDS-Jahrestagung für einen begrenzten Zeitraum (1-2 Stunden) Vertreter der AG als Ansprechpartner für neue GMDS-Mitglieder zur Verfügung stehen. Herr Schwanke klärt dies mit der Tagungsleitung in Göttingen ab.

5. TMF Datenschutzkonzept Forschung

Herr Schwanke hat diesen Unterpunkt aufgenommen und erklärt kurz, dass die TMF ein neues generisches Datenschutzkonzept publiziert hat. Herr Schütze bittet daraufhin Herrn Pommerening, als einen der Autoren, kurz die Publikation vorzustellen.

Herr Pommerening erklärt, dass das generische Datenschutzkonzept durch die Konferenz der Datenschutzbeauftragten des Bundes- und der Länder als Leitfaden für biomedizinische Forschungsvorhaben empfohlen wurde. Das generische Datenschutzkonzept beschreibt den datenschutzkonformen Aufbau von IT-Infrastrukturen für die biomedizinische Forschung. Forschungsvorhaben können bei der AG Datenschutz der TMF ein Votum für ihre IT-Infrastruktur erhalten. Diese Konformitätserklärung der TMF führt dazu, dass die jeweiligen Landesdatenschutzbeauftragten auf eine explizite Begutachtung des Datenschutzkonzeptes in der Regel verzichten.

6. Nächstes Treffen

Die nächste Sitzung findet am 19.11.2014 zusammen mit der TMF in Berlin statt.