一般口演4
セキュリティとプライバシー保護

2019年11月22日(金) 09:00 ～ 11:00 H会場 (国際会議場 3階中会議室304)

[2-H-1-03] 厚労省ガイドライン第５版にもとづく情報システム運用管理規程の改訂とシステム監査実施について

○福田 秀樹[1]、藤岡 和美[1]、平井 智裕[2]、尾崎 勝彦[1]（1. 徳洲会インフォメーションシステム株式会社, 2. 岸和田徳洲会病院）

キーワード：Information System Operations Management Stipulation, System audit, Guidelines for Medical Information Systems

徳洲会グループでは、徳洲会インフォメーションシステム株式会社（以下 TIS）とグループの IT統括部門である情報システム管理部会（グループ病院約150名の SEで組織：以下 SE部会）、また外部機関（一般社団法人メディカル ITセキュリティフォーラム）の協力も得て、グループの65病院共通で利用する情報システム運用管理規程の第4.2版から第５版への改訂作業に取り組み、昨年11月にこの新版をリリースした。

改訂にあたっては共通の帳票・台帳類を新たに作成し、この帳票等を利用することで規程に沿ったシステム運用ができることを目指した。各病院の新規程への切り替えと新しい運用への移行状況を TISと SE部会で把握し、病院から様々な質問や相談を受けながらフォローを行ってきた。

また、新規程にもとづいたシステム監査を行うべく監査表・監査手順を検討・作成し、４月に大阪のグループ病院で第１回の監査を次のとおり実施した。

監査実施日時と事前提出文書通知（約１ヵ月前） → 文書提出締切（約２週間前） → 事前（文書）監査実施 → 現地監査（文書監査結果確認・関係者インタビュー・現場確認・総評） → 監査結果打合せ・監査報告書作成 → 病院へ監査報告書提出

この手順で、夏以降は月２～３病院のペースで監査を行うべく計画している。

新規程は厚労省ガイドライン第５版に準拠し、かつ会計監査の視点も取り入れた内容としているが、規模や体制、従来の運用は各病院で異なり、規程に沿った運用が難しいケースもある。様々な意見を汲みながら今後規程のブラッシュアップを継続する必要がある。また４月のシステム監査では、パスワードの変更ルールや情報機器持ち出し時の承認手順など複数の指摘事項があり、その後病院から改善報告が行われた。

新規程の適用とシステム監査は病院のセキュリティレベルの向上に寄与するものと考える。さらなるレベルアップを目指して活動を続けたい。

厚労省ガイドライン第5版にもとづく情報システム運用管理規程の改訂とシステム監査実施について

福田秀樹[*1]、藤岡和美[*1]、
平井智裕[*2]、尾﨑勝彦[*1]
*1 徳洲会インフォメーションシステム株式会社、
*2 医療法人徳洲会 岸和田徳洲会病院

Revision of Information System Operations Management Stipulation based on the Ministry of Health, Labour and Welfare Guideline for Medical Information Systems ver.5 and Information System Audit Implementation

Hideki Fukuda[*1] , Kazumi Fujioka[*1], Tomohiro Hirai [*2] , Katsuhiko Ozaki[*1]
*1 Tokushukai Information System Inc., *2 Kishiwada Tokushukai hospital

Ministry of Health, Labour and Welfare of Japan has published the Safety Administration Guidelines for Medical Information Systems ver.5 in May 2017. Since 2018, medical corporations above certain size have been obligated to conduct an accounting audit. With this change, hospitals turn to manage patient information on their inner hospital servers more cautiously and properly. Tokushukai Information System Inc., therefore, has revised the Information System Operations Management Stipulation covering 65 hospitals of Tokushukai medical group in November 2018. We made this stipulation in cooperation of few system engineers of Tokushukai hospitals, Medical IT Security Forum and PricewaterhouseCoopers Aarata LLC to reduce the risk of information security in the hospital. We also aspire to ensure that hospitals have become able to work out the accountability and responsibility for information management by this new stipulation. However, there exist some hospitals hard to comply with this new stipulation. Hence, we have started an information system auditing for those hospitals since April 2019. We interview and check the status of handling of information systems operation and patient information, define the specific concerns and issues by means of the hearings with related personnel, and provide operational support for the improvement.

Keywords: Information System Operations Management Stipulation, System audit, Guidelines for Medical Information Systems

1. 緒論

2017 年 5 月の改正個人情報保護法の全面施行により、医療機関が保有する患者情報は「要配慮個人情報」にカテゴライズされ、より慎重かつ適切な取り扱いが求められるようになった。また、2018 年度より一定規模以上の医療法人に対して会計監査が義務化され、財務面のみでなく、非財務面、つまり患者情報の電子的な管理の透明性についても対外的に説明する責任がより強く求められている。このような状況の下、徳洲会グループでは、2017 年 5 月にリリースされた厚生労働省「医療情報システムの安全管理に関するガイドライン第 5 版」（以下「厚労省ガイドライン」という）と、会計監査で求められる IT 内部統制の必要要件を満たすことも念頭に、徳洲会グループ病院で統一的に利用してきた「情報システム運用管理規程」（以下「運用管理規程」という）第 4.2 版の大幅な改訂を行った。さらに上述の説明責任の観点も踏まえ、この規程にもとづく運用状況を記録として継続的に管理すべく、帳票・台帳類の新たな定義を合わせて行うこととした。徳洲会グループ全体として統一された帳票・台帳類にもとづくシステム管理を行うことで、患者情報管理の透明性を向上させることとなった一方、これは大幅な運用の見直しを伴うものであるため、現場への浸透に加え、システム管理を担う院内 SE 間の認識統一も不可欠である。こうした背景から、改訂された規程を各病院で適用した後、運用が適切な認識の下で行われているかという観点を中心に現場の状況を調査・点検、そこで検出された認識齟齬や課題を解決し、より合理的な運用が行えるよう各病院を支援するため、2019 年4月よりシステム監査を開始した。

2. 目的

今回の一連の取り組みは、徳洲会グループ各病院におけるセキュリティレベルをより高度かつ強固なものとすることにある。医療機関のセキュリティは「システム」「ルール」「運用」によって実現されると考えるが、ここではそのうちの「ルール」と「運用」によるセキュリティの向上を目指し、また各病院が医療機関に求められるコンプライアンス、「管理責任」と「説明責任」を果たせるようにすることを目的としている。

3. 方法

3.1 体制

運用管理規程改訂およびシステム監査は、徳洲会インフォメーションシステム株式会社（以下「TIS」という）および徳洲会グループ情報システム管理部会 法令順守部門（以下「SE 部会」という）が主体となり、一般社団法人メディカル IT セキュリティフォーラム（以下「MITSF」という）と PwC あらた有限責任監査法人（以下「PwC」という）の協力も得て実施した。

TIS は一般社団法人徳洲会の 100%出資の関連会社で、

徳洲会大阪本部内に置かれていた情報システム部が2009年10月に独立した組織であり、徳洲会グループ全体のIT化を統括・推進する役割を担っている。SE部会は、徳洲会グループ各病院に在籍するシステムエンジニア約130名で構成する病院横断的な組織で、医療機関のITに関する情報提供・共有、教育・研修、災害・障害対策やセキュリティ対策の検討などを行っている。またMITSFは2013年に設立された医療分野における情報セキュリティの重要性の啓発と問題解決のためのソリューション提供を行う団体で、今回はそのセキュリティアドバイザーを務めるPwCとともに各種検討に加わり、貴重な助言と支援をいただいた。

3.2 改訂の概要と作業

今回の運用管理規程改訂のポイントと行った主な作業は次のとおり。

1 厚労省ガイドラインに準拠:

最新の厚労省ガイドライン第5版の内容に準拠するよう旧規程を見直し、不十分だった要件も盛り込んだ。

2 会計監査上の必要要件を反映:

会計監査におけるIT内部統制(医療情報システムの信頼性)の検証で必要とされる取り組みについても、規程に反映させた。

3 全体の構成の見直し:

規程の構成(章立て)を厚労省ガイドライン第5版の構成に合わせるよう組み直した。これにより規程とガイドラインとの対応がわかりやすくなり、また今後の改訂時の作業も容易になる。

4 内容の整理:

旧規程では、重複した内容・同様の記述が複数の章に存在し、表現がそれぞれ微妙に異なるものもあった。これらを一箇所にまとめて整理することで読みやすくし、不要な別紙も削除するなど全体のボリュームもコンパクトにした(旧規程:47ページ → 新規程:39ページ)。

5 運用上必要な帳票・台帳類を新たに定義:

業務の運用上、記録・管理することが必要な事項については規程にその旨を記載し、徳洲会グループ病院が共通で利用する帳票・台帳類の標準書式も作成した。

3.3 経過

2017年7月～12月:TISとSE部会が厚労省ガイドライン第5版の内容確認と改訂すべき点の洗い出し、運用管理規程第4.2版からの改善に関する検討などを行った。

2018年1月～6月:運用管理規程第4.2版と改訂すべきと思われる点をMITSFに提示し、打ち合わせと改訂案の修正を重ね、旧規程を大きく見直した運用管理規程第5版の案を作成、共通の帳票・台帳類を新たに作成した。

2018年7月:TIS代表取締役社長 尾﨑より、運用管理規程改訂の主旨と概要について徳洲会グループ各病院の幹部に説明が行われ、7月末に運用管理規程の改訂案と帳票・台帳類がTISより各病院へ配付された。各病院とも新規程への切り替えは11月中、新しい運用への移行は2019年2月中に行うことを目標に設定した。

2018年8月～10月:各病院から新規程や帳票・台帳類に対する質問や意見をTISで受け付け、これをもとに新規程の内容を一部修正後、10月末に内容を確定させた運用管理規程第5版と関連資料(3.4参照)を再度TISから各病院へ配付した。

2018年11月～2019年4月:各病院の情報システム委員会等でSEから改訂について説明、協議して運用管理規程を第5版に切り替え、また新しい帳票・台帳類を使用した運用への移行を実施した。しかしながらルールと運用の大きな変更となったことでさらに多くの質問や相談がTISへ寄せられ、SE部会・MITSFの支援も得ながら回答と対応を行った。

2019年1月～3月:運用管理規程にもとづくシステム監査について、TIS・SE部会・MITSFで検討し、スケジューリングと体制整備、監査チェックシートや報告書式作成などの準備を行った。

2019年4月:八尾徳洲会総合病院(大阪府)にて徳洲会グループとして初のシステム監査を実施した。

3.4 改訂時の配付資料

2018年10月末に新しい運用管理規程の確定版を配付した際、合わせて次の資料も各病院へ提供した。

1 帳票・台帳類:

各病院で新規程にもとづく運用の移行がスムーズに行えるよう、次の23の標準書式を作成し規程の別紙として提供した。

- 役務任命簿
- リスク評価・対策検討表
- サーバー管理台帳
- 端末管理台帳
- ネットワーク機器管理台帳
- 入退室記録表
- 入退室記録管理点検表
- ID／アクセス権限登録・変更・削除申請書
- 管理者ID・システムID管理台帳
- 管理者ID利用記録簿
- 共用ID利用者一覧
- ID・権限棚卸結果報告書
- ID・権限棚卸結果管理表
- パスワード再発行履歴管理台帳
- 情報機器持出し・持込み申請書
- 外部記憶媒体貸与台帳
- 媒体・機器等廃棄記録台帳
- ウイルス対応報告書
- ウイルス対応管理台帳
- アクセスログ点検結果表
- バッチ処理結果確認表
- 保守作業計画書兼結果報告書
- ネットワーク作業実績管理台帳

2 運用管理規程改訂に伴う新旧関連表:

改訂に伴い再編した運用管理規程の各章・各項目に対して、旧規程のどの範囲が関連するかを一覧化した。

3 運用管理規程改訂に関する質問・意見と回答集:

改訂および新しい運用への移行に際し、2018年10月末までに各病院から寄せられた約90件の質問・意見・相談内容とその回答・対応についてQ&A集としてまとめた。

3.5 システム監査の準備と実施

システム監査については、約 3 ヵ月で次のとおり準備を行い、実施した。

1 作成した書類等:

システム監査実施にあたって次の書類等をTISとSE部会、MITSFの協力も得て準備した。

A システム監査実施の通知文書:

現地監査日時・監査員・当日のタイムテーブル・事前に必要な資料の提出期限を記した対象病院(院長)宛ての通知。

B システム監査依頼資料一覧:

事前の文書監査に必要な提出資料の一覧で、A の通知文書とともに病院宛てに送付。

C システム監査チェックシート:

監査項目（81 項目）の一覧で、監査時のチェック対象・方法・留意点なども記載した。監査員は文書監査および現地監査でこのチェックシートを使用し、監査結果とコメントを記入する。

D システム監査報告書:

現地監査後に監査員が協議して作成する病院宛ての結果報告書。各監査項目は 3 段階（○:充足 △:一部充足 ×:未充足）で評価され、△と×の項目についてはそれぞれ問題・課題を指摘し、合わせて改善策を提示する。また、病院からの改善報告に必要な資料とその提出期限を示す。

2 システム監査対象:

徳洲会グループで電子カルテを利用している 65 病院が監査対象となる。

3 監査員:

1 病院のシステム監査は、原則として次の 3 名で行う。

A SE 部会 担当ブロック長 1名:

SE 部会は各ブロック（北海道・東北・北関東・南関東・関西・大阪・九州・離島・沖縄）ごとにブロック長を置いている。北海道ブロックの病院が監査対象となった場合は、北海道ブロック長が監査のリーダーを務める。

B SE 部会 法令順守部門メンバー 1名:

SE 部会は教育研修・災害対策・学術研究・コスト削減などテーマごとに部門を置き、TIS とともに課題の解決に取り組んでいる。運用管理規程やシステム監査は法令順守部門が担っており、ここに所属するメンバーから 1 名が監査員となる。

C TIS 1名:

TISからも社内でプライバシーマークやISMSを担当し、SE 部会法令順守部門を支援するメンバー2 名のうち 1 名が監査員として入る。

4 現地監査当日のタイムテーブル:

平日の午後、所要時間は 3 時間 30 分で、挨拶と監査主旨・手順等説明（10 分）の後、文書監査結果にもとづく質問と確認（30 分）、現場確認と関係者インタビュー（2 時間 10 分）を行い、監査結果を取りまとめて（20 分）、総評を行う（20 分）のが標準的なタイムテーブルである。

5 監査全体スケジュール:

原則として現地監査の 4 週間前に病院へ日時を通知し、その後 2 週間で文書監査用の資料提出を受け、続く 1 週間で対象病院担当の監査員が文書監査を行い、事前ミーティングを経て現地監査を実施する。事後ミーティングで結果をまとめ、現地監査の 1 週間～10 日後には病院へ監査報告書を提出する。未充足および一部充足と評価された項目については、監査報告書到着後 3 ヵ月以内に病院から改善報告を文書で行い、監査員は文書あるいは現地訪問により改善状況を確認し、問題がなければ完了とする。

4. 結果・考察

運用管理規程の第 5 版への切り替えと新しい帳票・台帳類による運用への移行は、その過程を通じて病院全体で情報セキュリティの重要性とそのために必要な事項を再認識する好機となった。ここからUSBメモリの運用に関する問題提起があり、各病院の実態調査と徳洲会グループとしての対策検討が進むなど、より具体的な動きが生まれている。システム監査はこうした動きをさらに後押しする契機となっている。

こうしたポジティブな効果があった一方、全病院を対象として運用の移行状況について2019 年 3 月に調査をしたところ、移行割合は 20～100%と病院によって大きな差が生じており、全体として未だ十分な定着には至っていない。規程改訂に伴って各病院から寄せられた質問の多さにもみられるとおり、現場で個別最適化された運用が行われている状況に対して、今回のような全体最適型のルールを適用しようとする場合、説明会や Q&A 集の配付等の準備以外にも、現場担当者も含め関係者間の認識統一を事前に、より丁寧に行うことが重要と考えられる。

またシステム監査のなかで、病院によっては規程で求められる管理対策が現場の運用上大きな負荷をもたらし、対応が困難となっているケースも見受けられる。こうしたケースでは、別の方法によりリスク低減を図るアプローチをシステム監査の中で拾い上げ、SE 部会等で検討を行うこととしている。今後法的な必要条件やセキュリティレベルを保持しながら規程をより合理的な内容に修正していくことが、新しい運用を定着させていく上で重要なポイントとなる。

5. 結論

今回の一連の取り組みは、規程をトップダウンで改訂することにより各病院が直面する歪みを、システム監査による現場の声のヒアリングや指導を通じてボトムアップに是正していくというアプローチにもとづいている。システム監査というと規程の準拠性に焦点を置いたものと捉えられ、現場にとってはネガティブなイメージが強い。しかし限られたリソースで運用に取り組む現場の声を聴きながら、徳洲会グループ全体のセキュリティ管理水準を皆で一体となって考えていくための手段としてシステム監査を実施することは、病院が患者情報に関する管理責任・説明責任を果たす上でも、ポジティブな効果を発揮するものと考える。

参考文献

1) 厚生労働省. 医療情報システムの安全管理に関するガイドライン 第 5 版. 2017.
2) 特定非営利活動法人デジタル・フォレンジック研究会「医療」分科会 一般社団法人メディカルITセキュリティフォーラム合同委員会. 「医療情報システムの安全管理に関するガイドライン」対応のための手引 Ver.1.00. 2016.
3) 新日本監査法人監査技術部. リスクベースで進めるIT 内部統制の実務. 中央経済社, 2007.