ポスター | 病院情報システム
ポスター11
病院情報システム
2019年11月24日(日) 09:00 〜 10:00 ポスター会場2 (国際展示場 展示ホール8)

[4-P2-1-06] 電子計算機室に機器等を設置するための基準作成に向けた取組み

○松永 敏明[1]、難波 孝宏[1]、三浦 亜耶乃[1]、森 龍太郎[2]、青木 光広[2]（1. 岐阜大学医学部附属病院　経営企画課　医療情報係, 2. 岐阜大学医学部附属病院　医療情報部）

キーワード：Installation standard, Hospital Information System, Standardization

【背景と目的】地域医療連携や研究を目的とし、院内システムで管理されている患者情報を外部の情報ネットワークを介して院外機関と連携する必要性が近年増加している。一方で医療情報システム管理部門では、既存システムの厳格な管理に加え、院外機関と連携するために他部署等が新たに設置する情報通信機器等（以下、外部機器等と言う。）の管理が加わり、システム全体の情報セキュリティや個人情報保護の対応等で非常に苦慮している。

外部機器等を電子計算機室に設置するにあたり調整等で非常に時間を要すこと、管理のために必要な情報等が適切に提供されない等の問題があった。

さらに要配慮個人情報である患者情報の取扱いに関し、連携する院外機関からの契約書等の中には、個人情報の扱いが不十分、記載がない、さらには許可なく第三者提供できるようになっていたものもあった。

このような状況を解消するため本院では、電子計算機室に外部機器等を安全に設置するための管理基準の作成に取り組んだ。

【結果】電子計算機室に機器等を安全に設置するための基準を作成した。電子計算機室に外部機器等を設置する場合には基準に基づき申請書を提出する運用に変更した。

本基準により外部機器等の情報や責任者が誰であるかを申請書の形で残すことができた。また、各種の法律やガイドラインを遵守することを申請書の中でチェックさせ、個人情報の管理や扱いを統一することができた。

他にも本基準の中で保守・点検、利用者制限、監査、損害賠償等についても定めた。

【考察】本基準により個人情報の管理や扱い、機器等の管理について統一された基準で行わせることができるようになった。また、申請者側に事前に本基準に基づき申請する必要がある旨を伝えることで、これまでは何回かやり取りを重ねていた手続きを省略することができた。
運用の中で改良の余地が見受けられたため、改訂を重ねてより良い基準を作り上げていきたい。

電子計算機室に機器等を設置するための基準作成に向けた取組み

松永 敏明[*1]、三浦 亜耶乃[*1]、難波 孝宏[*1]、
森 龍太郎[*2]、青木 光広[*2]
*1 岐阜大学医学部附属病院 経営企画課 医療情報係、
*2 岐阜大学医学部附属病院 医療情報部

Efforts to create standard for installing equipment in the computer room

Toshiaki Matsunaga [*1], Ayano Miura[*1], Takahiro Nanba[*1],
Ryutaro Mori[*2], Mitsuhiro Aoki[*2]
*1 Management Planning Division, Gifu University Hospital,
*2 Medical Information Department, Gifu University Hospital

In order to properly manage information security, personal information protection and information management in the hospital, a standard was established for installing equipment in the computer room.
With the creation of standards, it has become possible to operate on the basis of standards that are clearly documented in and out of the hospital.

Keywords: Installation standard, Hospital Information System, Standardization.

1. 緒論・目的

地域医療連携や研究を目的とし、院内システムで管理されている患者情報を外部の情報ネットワークを介して院外機関と連携する必要性が近年増加している。一方、医療情報システム管理部門では、既存システムの厳格な管理に加え、院外機関と連携するために他部署等が新たに設置する情報通信機器等(以下、外部機器等と言う。)の管理が加わり、システム全体の情報セキュリティや個人情報保護の対応等で非常に苦慮している。

外部機器等を電子計算機室に設置するにあたり調整等で非常に時間を要すこと、管理のために必要な情報等が適切に提供されない等の問題があった。

さらに要配慮個人情報である患者情報(以下、データと言う。)の取扱いに関し、連携する院外機関からの契約書等の中には、個人情報の扱いが不十分、記載がない、さらには許可なく第三者提供できるようになっていたものもあった。

このような状況を解消するため本院では、電子計算機室に外部機器等を安全に設置するための管理基準の作成に取り組んだ。

2. 方法

基準作成の方針として、個人情報の保護は担保される必要がある。しかし、そのために厳しすぎる基準にしては地域医療連携や研究の妨げになってしまう。トレードオフの関係であるため、適切となるように考慮する。

また、クラウドの活用等、技術進歩や環境変化や法律改正等が考えられるため、基本方針と最低限守られなければいけない内容を盛り込み、運用する中でより良い形に改訂することを想定の下、個人情報の保護に関する法律と医療情報システムの安全管理に関するガイドラインを参考に基準案を作成し、添削と修正を繰り返し、基準を作成した。

3. 結果

「電子計算機室に機器等を設置するための基準」を作成した。電子計算機室に外部機器等を設置する場合には基準に基づき申請書を提出する運用に変更した。

3.1 構成

基準の構成を次に挙げる。

第1条　趣旨
第2条　定義
第3条　設置申請手続
第4条　設置承認手続
第5条　設置作業手続
第6条　設置変更手続
第7条　機器撤去手続
第8条　保守・点検
第9条　個人情報保護対策
第10条 機器利用者制限
第11条 監査
第12条 費用
第13条 使用制限・停止・撤去
第14条 免責
第15条 損害賠償等
第16条 準拠する法令・ガイドライン等
第17条 雑則
附則
機器設置・変更申請書
機器接続時チェックシート
機器撤去届
作業申請書

3.2 要点

基準作成時に注力した内容を次に挙げる。

3.2.1 第 3 条　設置申請手続

設置申請では以下に掲げる中で関係のある様式の提出を定めた。

- 設置申請書
- 関係者情報
- 物品情報
- 設定情報
- システム構成図
- ネットワーク構成図
- データフロー
- 運用フロー
- 個人情報に関する情報
- データ匿名化に関する情報

申請に必要な様式は多いが、今後異動などで当時の担当者がいなくなったとしても、誰が見てもどのような外部機器等

が設置されているかを把握できるようにするために定めた。また、システム構成図・ネットワーク構成図・データフローは外部機器等が関係する範囲を明確にするためと、申請者の最低限の技術力を確認するために定めた。

3.2.2 第 4 条　設置承認手続

本病院内の運用などに影響を及ぼす可能性がある場合は、院内の医療情報セキュリティ委員会の議を経ることを定めた。

セキュリティに関しては院内の運用のとおり委員会の議を経ることを定めた。

3.2.3 第 8 条　保守・点検

定期及び随時に外部機器等の保守・点検の実施を定めた。作業前日までに作業内容の許可を受け、作業後には作業報告書の提出を義務付けた。

事前調整もなくいきなり保守作業のため電子計算機室に入らせてほしいと訪問してきた、作業後に何の報告もなく帰ろうとしたベンダーが過去にあったため定めた。

3.2.4 第 9 条　個人情報保護対策

申請前に個人情報保護対策について医療情報部長との協議することを定めた。また、外部機器等への指定ログの保存を定めた。

医療情報部長と事前に協議を行うことで、考えなしに外部機器等を設置しようとする動きを防ぐ効果を狙って定めた。

3.2.5 第 15 条　損害賠償等

本病院や患者への損害賠償を定めた。また、承認された目的以外にデータを利用した場合や、承認されたデータフロー以外へのデータ送信等も損害賠償の対象とした。

あくまでも損害賠償は抑止力としての効果を狙って定めた。しかし、地域医療連携の大義を掲げて、本院の全患者情報を吸出し、許可されていない研究への利用や無関係な別サービスへの利用を企む某病院の影響もあり、賠償額も定めた。賠償額の算定は1バイト当たり1円又は、1人当たり想定損害賠償額（JNSA 情報セキュリティインシデントに関する調査報告書別紙の想定損害賠償額算定式より算定される金額）[1] と定めた。

3.2.6 第 16 条　準拠する法令・ガイドライン等

次に掲げる法令やガイドライン等の最新版を準拠するようにした。

- 個人情報の保護に関する法律（平成１５年５月３０日　日本法律第５７号）
- 個人情報の保護に関する法律についてのガイドライン（通則編）（外国にある第三者への提供編）（第三者提供時の確認・記録義務編）（匿名加工情報編）（平成２８年１１月　個人情報保護委員会）
- 医療情報を受託管理する情報処理事業者向けガイドライン
- 医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス（平成２９年４月１４日　個人情報保護委員会、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（平成２９年５月　厚生労働省）
- クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン（平成３０年７月　総務省）

クラウドサービスのような日々変化しているサービス等を利用する場合があるため、申請書を出した時点の法令やガイドライン等の準拠ではなく、最新版を準拠とした。

3.2.7 第 17 条　雑則

特に定めのない場合には、この基準を最優先とするようにした。

問題発生の原因となりやすい、お互いの認識違いを防ぐため、また、本病院に不利な内容を適用させないため定めた。

3.2.8 接続時チェックシート

ウイルス対策や時刻合わせの方法等に加え、ログの管理や法令やガイドライン等の準拠を行うことをチェックさせ、設置申請と共に提出することを定めた。

ログの管理や法令やガイドライン等の準拠を基準の中で定めるだけでなく、明示的にチェックさせることで遵守させることを意識させるために定めた。

4. 考察

基準を作成により個人情報の管理や扱い、機器等の管理について統一された基準で行わせることができるようになった。また、申請者側に事前に基準に基づき申請する必要がある旨を伝えることで、これまでは何回かやり取りを重ねていた手続きを省略することができた。

設置された外部機器等の管理情報を一ヶ所にまとめることができるようになったため、管理の効率化を図れる見通しがたった。

しかし、運用の中で次に掲げる課題が見受けられた。

・過去に設置された外部機器等への対応

今から設置申請の提出が難しい場合もあるため、対応検討中。次期医療情報システムの更新時には提出を義務付ける予定。

・提出者が基準の内容を理解できない

あるベンダーで基準に書かれた内容について、この条件では承諾できないとの話があったが、内容を詳しく聞いてみるとそもそも免責が何かわかっていないだけであり、その日本語の意味を伝えることで解決したことがあった。

基準の内容について打合せの中で確認を行い、書き方で伝わりにくい場合には次版での改訂を検討する。

5. 結論

基準の作成により、院内・院外に対して明文化された基準を元に運用することができるようになり、情報セキュリティの強化と安定した運用管理につながった。

先日、ベンダーが導入した Linux サーバのパッチ適用を導入ベンダーで行うことが出来ず、別ベンダーに適用作業を行うことがあった。技術進歩によりシステム導入のハードルが下がるのはいいが、技術員のレベルも下げられては困る。

参考文献

1) JNSA. 2018 年 情報セキュリティインシデントに関する調査報告書【速報版】別紙（想定損害賠償額の解説）. JNSA, 2018. [https://www.jnsa.org/result/incident/2018.html].