HIPAAプライバシールール (9)

- 保健福祉省はデータ保持者がごく小規模から大規模なものまであることを認識しているため、ルールのフレキシビリティとスケーラビリティは、それぞれのニーズや環境に応じて適切に設定されるとされている。
  - プライバシーポリシーと手順
    - データ保持者はプライバシールールに沿ったプライバシーポリシーや手順を文書により設定しなくてはならない。
  - プライバシー担当者
    - データ保持者は、プライバシー担当者を指名しなくてはならない。
  - 作業員のトレーニングと管理
    - データ保持者は、全ての関与する作業員にプライバシーポリシーや手順についてトレーニングを行わなくてはならない。
  - 軽減措置
    - 作業員やビジネスアソシエートがプライバシーポリシーや手順又はプライバシールールに違反した場合、有害な事象を実行可能な範囲で軽減しなくてはならない。

HIPAAプライバシールール (10)

管理上の要求（2）

- データの保護措置
  - データ保持者はプライバシールールに違反した意図的、非意図的な使用や開示に対して、合理的かつ適切な管理的、技術的、物理的な保護措置を維持し、偶発的な使用や開示を制限しなくてはならない。
- 申し立て
  - データ保持者は、個人情報提供者からのプライバシールールの遵守等に関する申し立てに関する手順を設定しなくてはならない。
- 報復と権利の放棄
  - データ保持者は、保健福祉省やその他の適切な当局の調査を補助する又はプライバシールールに反していると思われる際に、プライバシールールに基づいて権利を実施した個人等に対して、報復をしない。データ保持者は、データ提供者に対し、プライバシールールに基づき治療、支払い等についての権利の放棄を要求しない。
- 文書と記録の保持
  - データ保持者は、直近のデータが作成された時又はプライバシーポリシーや手順等のプライバシールールで定められる事項が設定された時の遅いほうから起算して、６年間文書と記録を保管しなくてはならない。

HIPAAセキュリティールール (1)

一般則　（1）

◆ セキュリティールールは、データ保持者に合理的かつ適切な行政的、技術的及び物理的措置により電子化された個人情報を保護するよう求めており、関係者は以下を遵守する必要がある

1. 作成、受領、保持及び転送に供する全ての電子化された個人情報に関する機密性、統合性、可用性を確保しなくてはならない。
2. 予測されるセキュリティー上の脅威を同定し、それらから情報を保護しなくてはならない。
3. 予測される許容されない使用法や公表に対して、情報の保護を行わなくてはならない。
4. 従業員がコンプライアンスを遵守することを確保しなくてはならない。

HIPAAセキュリティールール (2)

一般則　（2）

◆ DHHSは小規模から大規模までデータ保持者が多様であることから、セキュリティールールはデータ保持者のニーズや環境に合わせてフレキシブル、スケーラブルであるとしているが、以下のことを考慮しなくてはならない。

- データ保持者の規模、複雑さ、能力
- データ保持者の技術的、ハードウェア、ソフトウェアのインフラ状況
- データの保護に要するコスト
- 電子的な個人情報の潜在的なリスクの尤度とインパクト

HIPAAセキュリティールール (3)

リスクの分析と管理

- データ保持者はリスクの管理の一環として、リスクの分析を行うことが求められている。リスク分析には、以下のものを含む（以下のものに限られるわけではない）
  - 電子的な個人情報の潜在的なリスクの尤度とインパクトの推定
  - リスク分析により特定されたリスクに応じた適切なセキュリティ確保のための手段の実施
  - 選択したセキュリティ確保のための手段の文書化、及び必要な場合は、その手段を講じた論理的な理由
  - 継続的、合理的、かつ、適切なセキュリティ確保のための手段の維持

- 定期的にリスク分析を行い、電子的な個人情報へのアクセスをレビューし、セキュリティに関するインシデントを検出する。また、定期的にセキュリティ確保のための手段の有効性について評価し、電子的な個人情報の潜在的なリスクを再評価する。

HIPAAセキュリティールール (4)

セキュリティ確保手段の実施

- 前述のスライドに記述しているように、データ保持者は電子的な個人情報の潜在的なリスクを特定し、分析しなくてはならない。また、リスクと脆弱性を合理的かつ適切なレベルに減少させるためのセキュリティ確保のための手段を実施しなくてはならない。
  - セキュリティ確保担当者
    - データ保持者はセキュリティ確保を企画立案・実施する担当者を指名しなくてはならない。
  - 情報アクセス管理
    - 個人情報の使用と公開は必要最小限とし、アクセスがデータ使用者や方法が適切なときにのみアクセスを許可すべき。
  - 作業者のトレーニングと管理
    - データ保持者は電子的な個人情報を扱う作業者の適切な管理を行う。データ保持者はセキュリティポリシーに沿って、全ての作業者をトレーニングすることが必要であり、セキュリティポリシーに違反した作業者に適切な処罰を行うことが必要である。
  - 評価
    - データ保持者は、セキュリティポリシーやセキュリティ確保の方法がセキュリティルールの基準を満たしているかどうか、定期的な評価を実施しなくてはならない。

HIPAAセキュリティールール (5)

セキュリティ確保手段

◆ 物理的方法

- 施設のアクセスの管理
  - データ保持者は、許可されたアクセスのみに限られるよう、施設への物理的なアクセスを制限する必要がある。
- ワークステーションと装置のセキュリティー
  - データ保持者は、ワークステーションと電子媒体の適切な使用とアクセスを確保するため、ポリシーと手続きを実施する必要がある。また、ポリシーと手続きには、電子的な個人情報を保護を確保するため、メディアの移動、削除、廃棄、再利用が規定される必要がある。

◆ 技術的方法

- アクセスコントロール
  - 有資格者のみが電子的な個人情報にアクセスが可能とする。
- 監査によるコントロール
  - 電子的な個人情報を含むハードウェア、ソフトウェア、手続き、アクセスの記録等の活動の監査。
- データの完全性によるコントロール
  - 電子的な個人情報が不適切に変更又は破壊されないことを確保するような、電子的な手段の導入。
- データ転送に関するセキュリティ管理
  - 電子的な個人情報への電子ネットワークを通じた不適切なアクセスに関する技術的なセキュリティー手段を講じる。

HIPAAセキュリティールール (6)

管理上の要求

◆ データ保持者の責任

- データ保持者がビジネスアソシエートの活動が義務に違反していることを知った場合、データ保持者は違反を是正する措置を講じなくてはならない。違反には、電子的な個人情報を合理的かつ適切に保護する手段を実施していないことも含まれる。

◆ ビジネスアソシエート契約

- 米国保健社会福祉省は、HITECH Act of 2009に基づき、ビジネスアソシエートの義務及びビジネスアソシエート契約についての規制を作成中である。