参考資料1

米国のHIPAA法における
個人情報等の保護に関する規定について

Health Insurance Portability and Accountability Act

- 1996年にHIPAA（Health Insurance Portability and Accountability Act of 1996;医療保険の携行性と責任に関する法律）が制定。
- HIPAAにより、米国DHHS（保健社会福祉省）は健康情報に関するプライバシールール及びセキュリティルールを策定

HIPAAプライバシールール

Standards for Privacy of Individually Identifiable Health Information

健康情報の保護の国家基準を設定

HIPAAセキュリティールール

Security Standards for the Protection of Electronic Protected Health Information

電子的に保持・移動される健康情報のセキュリティに関する国家基準を設定

HIPAAプライバシールール (1)

プライバシールールの対象者

◆ プライバシールールは、保健情報を電子的フォームで送信する保健計画、保健医療提供者、保健医療クリアリングハウスに適用される。

- 保健計画：医科、歯科、眼科、薬科の保険業者、保健維持組織、メディケアー、メディケイドの保険業者、長期ケアの保険業者
- 保健医療提供者：早期保健医療提供者。病院、医療施設に属していない医師、歯科医師、その他の保険医療従事者、ヘルスケアを提供し、支払いを受けるその他の組織や個人
- 保健医療クリアリングハウス：標準化されていない情報を受け取り、標準化し、他の組織等に受け渡す、あるいはその逆を行う組織等。

HIPAAプライバシールール (2)

ビジネスアソシエート

◆ ビジネスアソシエートは、

- 自分の組織以外の従業員以外の個人や組織であり、支払い手続き、データ分析、請求書の送付を行う。保護されている健康情報を開示しない場合は、個人や組織はビジネスアソシエートとは見なされない。

◆ ビジネスアソシエート契約

- データ保持者が、外部契約者等を使用する場合、情報の保護等の規定を含むビジネスアソシエート契約（協定）を結ぶ必要がある。ビジネスアソシエート契約には、データ保持者は、使用、開示される個人を特定可能な保健情報について文書化された保護規定を義務付けが含まれる。

HIPAAプライバシールール (3)

保護の対象となる情報

- プライバシールールは、データ保持者又はそのビジネスアソシエートに保持、送付される全ての「個人が特定可能な保健情報」に適用される。電子媒体、紙媒体、口頭などの全ての手段が含まれる。プライバシールールでは、これらの情報を「保護対象保健情報：protected health information (PHI)」と呼ぶ。

- 個人が特定可能な保健情報は、以下について言及する統計データを含む情報である。
  - 個人の過去、現在、将来の身体的又は精神的な健康状況
  - 個人へのヘルスケアの対策
  - 個人の過去、現在、将来のヘルスケアの支払いの状況

HIPAAプライバシールール (4)

匿名化された情報

- 匿名化された保健情報(de-identified health information)の使用又は開示には制限はない。

- 匿名化された保健情報は、個人を特定することが不可能であるか、個人を特定できる合理的な事項を提供しない。情報の匿名化には、以下の２つの方法がある。
  1. 有資格の統計学者により決断される
  2. 特定の個人特定可能な情報や親族に関する情報、家族構成員に関する情報を削除し、データ保持者が残りの情報で個人が特定できないようにする。

HIPAAプライバシールール (5)

データ使用の原則

◆ 基本原則

- データ保持者は、以下の場合以外にデータを使用、開示してはならない。
  1. プライバシールールにより許可される、要求される場合
  2. 対象となる個人（又は代諾者）が文書により許可した場合

◆ 開示が要求される場合

- データ保持者は、以下の２つの場合にのみデータを開示しなくてはならない。
  - (a) 個人（又は代諾者）が自分に関する保健情報へアクセスや開示を求めた場合
  - (b) 遵守状況確認調査又は措置実施の評価のために、保健社会福祉省(DHHS)に提供する場合

HIPAAプライバシールール (6)

許可される使用又は開示

- データ保持者は、以下の場合には個人の許諾を得ずに保護対象の保健情報を使用又は開示することが許可される。しかし、求められるわけではない。
  1. データ提供者の個人に対して（アクセスや情報開示の説明の要求が無い場合）
  2. 治療、支払い、ヘルスケアの実施の際
  3. 同意や反対の機会
  4. それ以外の許可された使用や開示に関する偶発的事象
  5. 公共の利益やベネフィットにつながる場合
  6. 研究目的、公衆衛生、ヘルスケアオプションのための限定されたデータセット
- データ保持者は、どの使用や開示の条項となるのかを決定する際に、専門家としての倫理観や判断を負う。

HIPAAプライバシールール (7)

許諾・認定による使用又は開示

- データ保持者は、治療、支払い、ヘルスケア、それ以外のプライバシールールにより許可された使用以外に保護対象の保健情報を使用又は開示する際には、個人の書面による許諾を得なくてはならない。

- 許諾には特定の条件が記載されなくてはならない。許諾によりデータ保持者が第三者にデータを使用又は提供することが許可される場合がある。

- 全ての許諾は、明瞭に(in plain language)記載され、かつ、開示又は使用される情報についての特定の情報、情報を開示又は提供される個人等の情報、期間、文書により無効化できる権利、その他の情報についてを服務ことが必要である。

HIPAAプライバシールール (8)

必要最小限の限定的な使用又は開示

- プライバシーポリシーの主要な観点は、「必要最小限」の使用と開示である。データ保持者は、使用や開示目的に照らして最小限利用や開示とするよう努める必要がある。
  - アクセスと使用
    - データ保持者は作業員の特定の目的に応じて、データの使用や開示を制限するポリシーや手順を設定しなくてはならない。
  - 開示と開示のリクエスト
    - データ保持者は開示目的に照らして保護対象の個人情報が必要最小限の開示となるよう、ルーチンの又は求めが開示の求めがあった場合に対応するポリシーや手順を設定し実施しなくてはならない。
  - 合理的な信頼性
    - 他のデータ保持者から保護対象の個人情報の開示のリクエストが有った場合、データ保持者は、それが合理的な状況であれば、この必要最小限のアクセス基準をリクエストに要求することができる。

HIPAAプライバシールール (9)

管理上の要求（１）

- 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。