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)

## 保護対象

- 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。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 (5)

◆ 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)

- 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)

- 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。