資料2

医療関係データベースを活用した
医薬品等安全対策に係る提言作成のための資料（案）

1　医療関係データベースの利用に係る現状とその必要性について

（1）我が国の医薬品等安全対策の現在の課題

・我が国の医薬品の安全対策は、医療機関及び製薬企業からの副作用の自発報告に基づくものが中心であり、また、新薬の承認・販売後に行われる使用成績調査等による副作用の発生頻度等の確認も行われてきている。しかし、規制当局みずからが副作用情報を収集する仕組みの構築や、処方数の正確な把握に基づく副作用発現頻度等の定量的な情報の収集、それらのデータを基にした薬剤疫学的手法の活用は欧米諸国に比べ不十分である。

・「薬害肝炎事件の検証及び再発防止のための医薬品行政のあり方検討委員会」がとりまとめた最終提言（平成22年4月28日）（以下、「検証検討委最終提言」）で、今後の我が国の安全対策において、個人情報の保護等に配慮しながら、電子レセプト等のデータベースを活用し、医薬品使用者数の把握、投薬情報と疾病（副作用によるもの等を含む）発生情報の双方を含む頻度情報、安全対策措置の効果の評価のための情報基盤の整備、薬剤疫学的な評価基盤の整備が求められている。

（2）欧米等諸外国におけるデータベースを活用した医薬品等安全対策の現状

・欧米等の諸外国では、レセプトデータや電子診療録等の医療関連情報を数百万～数千万件規模でデータベース化し、薬剤疫学的手法を医薬品等安全対策に活用している。

・米国では、2004 年に長期使用による心血管リスクの増加が確認されたため世界的な回収が行われた消炎鎮痛薬である Vioxx（一般名 Rofecoxib)の対応が後手に回ったという批判が FDA に対してなされたこと等を受け、医学研究所（IOM）の勧告に基づき医薬食品庁（FDA）改革法(FDAAA)が制定された。FDA では、2008 年 5 月にセンチネル・イニシアティブを立ち上げ、民間保険会社も含む様々な関係機関の協力を得て、電子診療記録システムやレセプトデータベース等を活用した積極的な市販後安全性監視及びデータ解析を開始した。2010 年 7 月までに 2500 万人、2012 年 7 月までに1億人規模のデータへのアクセスを確立する目標を設

定している。
・また、欧米以外の国々、例えば、韓国や台湾においても、国家レベルのデータベースを構築し、医薬品等の安全対策に活用を開始している。

(3) 我が国における医療関係データベースの現状

・一部の医療機関において共同研究等により研究者・研究機関にレセプトデータや電子カルテによるデータが提供されているが、その規模や連携の程度は限定的である。
・一部の民間企業により、契約を結んでいる健康保険組合から提供されたレセプトから、匿名化され統計処理されたデータが提供されているが、数十万件の規模であり、前述の国々と比べると小規模なものである。
・2011 年度に我が国におけるレセプトデータを集約したナショナルデータベースを構築する計画が進行している。
・医療関係データベース等の利用に当たって技術面(薬剤疫学的研究の進展等)、社会・制度面(患者の権利、個人情報保護等)等で解決すべき課題がある。

(4)我が国でデータベースを活用した医薬品等安全対策を推進する必要性

・海外では、医薬品のみならず新たなデバイス、手技、手術法の有効性・安全性評価が可能となっているが、我が国においてはこのような評価を行うにあたって基盤となる医療関係データベースの整備が未だ進んでいない。医薬品や医療技術の有効性・安全性の評価は、国民が安心して医療を受けられるようにする上で重要であるのは勿論のこと、今後の医療リソース配分を考えていく上でも重要であり、実態調査や医療関係データベースの整備とこれを活用した有効性・安全性評価を推進していく必要がある。
(例)米国胸部外科学会における STS National Database
・前述のように、我が国において、レセプトデータを集約したナショナルデータベースを構築する計画が進行しているところであり、これらの大規模データを活用することにより、より早期に医薬品安全対策が実施できる可能性がある。

2 電子的な医療情報の活用の方向性について

(1)医療関係データベースの種類について

・「医療関係データベース」の明確な定義はないが、現在利用可能と考えられるデータソースとして、主に、①診療報酬請求のためのレセプトデータ、②診療等の情報を記録するための電子カルテの2つが挙げられる。それぞれの特徴は以下のとおり。

① レセプトデータ

電子レセプトのデータに関しては、2011 年度までに国家レベルのナショナルデータベースが構築されることが予定されており、「医療サービスの質の向上等のためのレセプト情報等の活用に関する検討会」で作成された「レセプト活用報告書」において、公益性の確保等を要件とした利用の可能性が指摘されている。

② 電子カルテ

電子カルテは、個々の患者の診療録として作成されており、投薬・処置や検体検査等の診療行為に関する詳細なデータを有している。しかし、現状では、医療機関又は情報ベンダー毎にデータ格納の方式等が異なっていることから、電子化が進んでいても、医療機関を超えたデータの活用には限界がある。

なお、上記データの他、将来的に利用が予想又は期待されるものとして、DPC、人口動態統計、予防接種、乳幼児検診等のデータがあげられる。

(2)各データベースにおける情報の活用可能な範囲と限界について

・レセプトデータと電子カルテから作成されるデータベースの主なメリット、デメリットは以下のとおり。他の種類のデータについては今後電子化の状況を踏まえつつ、検討を進める必要がある

	レセプト	電子カルテ
メリット	規模の大きさ、網羅性、形式的に比較的統一されている	転帰や病名の正確性、詳細な医療情報
デメリット	・医科レセプトでは傷病名、調	・データやデータの互換性に関

	剤レセプトでは処方の薬剤等の情報が得られる ・一方、検査データの結果や患者の転帰等の詳細な医療情報に欠ける。 ・レセプトに記載された病名の正確性、投与日等の詳細な情報が含まれていないとの指摘もある。	して、標準化が進んでいないため、規模に限界 ・データから、個人が特定されやすい等データの利用に抵抗感が生じやすい等、医療機関の協力を得るのが困難。

・長期間の調査にあたって、レセプトデータを用いてレトロスペクティブな調査研究（例えば、高血圧等の生活習慣病を対象とした予後調査？）を集団全体の動向を把握するという観点から行うことは可能である。
・一方、個人に着目してプロスペクティブな研究を行うことは、レセプトデータは匿名化され月毎の集計となっていることから、レセプト・データ（ナショナルデータベース）だけで対応することは現状では困難。

（3）医療関係データベースの医薬品安全対策への利用について

・医薬品の安全性を検討する際に、医療関係データベースの活用により可能と考えられる調査事例として、以下の3つが挙げられる。

①対象医薬品の特定の副作用の発生割合を正確かつリアルタイムにモニターするとともに、他剤と比較を行う

②ある有害事象について、医薬品服用群と非服用群における発生頻度を比較することで、当該有害事象が医薬品による副作用なのか、疾患による症状なのか判別することが可能となる

③緊急安全性情報等の安全対策措置の前後に副作用の発現頻度を比較することで、安全対策措置が副作用等の低減に効果があったのかが評価可能となる。また、禁忌等の適正使用が守られているかの確認が可能となる。

・レセプトのデータベースでは、その規模を活かして、発生頻度が非常に低い副作用の検出等への活用も期待される。
・電子カルテのデータの活用については、医薬品服用後の症状などが正確に記載されているため、未知の副作用の検出などが期待されるが、前述のとおり活用にむけて解決すべき課題が多い。

（例）データベースを用いた薬剤疫学的手法の活用の具体的な事例として、前述の Vioxx が挙げられる。Vioxx は 1999 年に発売され、回収までに 5 年を要した。一方、ハーバード大学の研究者らによるレセプトデータを用いた解析により、後ろ向き解析ではあるが、発売から 3 年程度の時点で、すなわち実際の回収が行われるよりも2年前に、心血管リスクの増加を明確に示す解析結果が得られ、薬剤疫学的手法を用いることにより、より早期に医薬品等安全対策が実施できる可能性が示された。

3 データベース利用時の社会的課題

（1）諸外国における個人情報の取り扱いに関する考え方

・国毎に医療関係のデータ利用に際した個人情報の取り扱いに関する考え方が異なる。例えば、北欧では国家レベルで個人情報を含んだデータ活用が当然のことと認識されている一方で、米国では個人情報を含んだデータの利用のみならず、個人を特定できる情報を除去した場合であっても、個人の病名等の医療記録を使用されることに警戒感がある。また、台湾、韓国では、当初、個人情報を含んだデータベースの利用が積極的に行われたが、近年は社会情勢の変化により、個人情報保護の意識が強まっている。

（2）個人情報の範囲と保護について

・電子カルテ情報の利用等により、密度の高い医療情報を取扱う場合、匿名化による個人情報の保護に努めることは重要であると同時に、データベース化に際しては、個人が特定される可能性がでてくる

（例）アイスランドの国民データベースでは、対象となる可能性のある患者が10人以下になった場合には、それ以上の検索が停止する仕組みになっている。

（3）国民的な理解を得るために

・医療関係データベースの利用促進には、臨床疫学的、薬剤疫学的研究の進展は必須であるが、同時に、国民（患者）の理解と医療従事者の協

力がきわめて重要である。
・現状、我が国においても医療に係る個人情報の適切な取り扱いについて懸念する声もある。
・これらの懸念も踏まえて、データベースを運用する場合の個人情報に関する一定のルールを示し、それが研究の実施において着実に担保される環境を作ることが重要である。

(4)データベース化と個人情報の保護

医療情報について、安全対策等の目的で利用可能なデータベース化する場合、本来医療情報は患者等の診療の目的で活用されるものであり、データの利用は、あくまで二次的な利用であることから、患者等の自己決定権や意図しない患者個人が特定できる情報の流出などについて、特段の注意を要するものである。

(ア)利用目的、必要とするデータの種類及び範囲

データソース	ナショナルデータベース	医療機関毎のレセプトデータ	保険組合、調剤薬局等の民間レセプトデータ
研究者に提供する者	国	医療機関	民間企業
データベースの状態	匿名化された情報としてデータベース化されている	個々の情報を匿名化し、データベースを構成する。	匿名化された情報としてデータベース化されている
患者同意	既存資料として事前同意不要	既存資料として事前同意不要	既存資料として事前同意不要
研究者(外部機関)への提供	——	匿名化がされていれば、事前同意不要。	——
計画審査	国において、研究計画審査が行われる予定(高確法)	・研究者の所属機関等の倫理審査委員会で研究計画の審査が必要 ・研究の実施情報の公開	・研究者の所属機関等の倫理審査委員会で研究計画の審査が必要 ・研究の実施情報の公開

データソース	医療機関の電子カルテ	医療機関の電子カルテ	医療機関の電子カルテ

研究者に提供する者	PMDA等が集積・データベース化	医療機関みずから	民間企業
データベースの状態	個々の情報を匿名化し、データベースを構成する。	個々の情報を匿名化し、データベースを構成する。	個々の情報を匿名化し、データベースを構成する。
患者同意	既存資料として事前同意不要	既存資料として事前同意不要	既存資料として事前同意不要
研究者(外部機関)への提供	——	匿名化がされていれば、事前同意不要。	——
計画審査	・研究者の所属機関等の倫理審査委員会で研究計画の審査が必要 ・研究の実施情報の公開	・研究者の所属機関等の倫理審査委員会で研究計画の審査が必要 ・研究の実施情報の公開	・研究者の所属機関等の倫理審査委員会で研究計画の審査が必要 ・研究の実施情報の公開

【注: 現行の疫学研究指針に沿って作成したものであり、表の内容については、懇談会での議論等を踏まえ、随時加筆修正等を行う】

(イ)情報のセキュリティーに関する規定等ついて

・統計法においては情報の漏洩が生じた場合は禁固刑も含む厳しい罰則規定が設けられているが、医療関係データベースが適用対象となるかは現時点では明確でない。

(ウ)研究に引用したデータの保存期間について

・疫学倫理指針では、あらかじめ研究計画書に資料の保存期間を定めておき、その保存期間を過ぎた場合には、匿名化し廃棄しなければならない旨定められている。

(5)個人の特定、患者個人への通知

・薬害肝炎検証検討委第一次提言において、以下の記述があり、個々の患者への副作用の伝達が求められている。

～個々の患者に副作用等の発現について知り得るような方策を検討すべきであること

～被害発生が確認された後の国民への情報伝達のあり方について被害者に配慮した公表のあり方を検討する必要があること
～電子レセプトデータベースが構築された場合には、緊急の安全性情報の提供が必要な場合において、レセプト情報を活用した患者本人への通知等に関する方法・問題等を検討する必要があること

・レセプトのナショナルデータベースは、匿名化されているため、国等から、患者本人への直接の通知は困難である。
・電子カルテから作成されるデータベースでは、個人の特定が可能な場合が想定されるが、個人を特定される可能性がある情報を第三者が取り扱うことになる。

4 データベース利用時の技術的課題

(1)現時点でのデータベースの状況

・各医療機関内において、診療情報や各種検査データ等の電子データを包括的に一括して管理する体制の整備が不十分。
・情報システムの規格・設計が医療機関毎、システムベンダー毎に異なっている。

(2)レセプトデータベースと電子カルテから作成されるデータベースの連結について

・レセプトのナショナルデータベースは匿名化されており、電子カルテから作成されるデータベースと連結させることはできない。
・レセプトデータと電子カルテにより作成されるデータを患者毎に連結することにより、それぞれに不足している情報を補完することが可能となる。個人情報の取り扱いにおける課題が解決されたことを前提として、連結によって情報量が豊富なデータベースの構築が可能となれば、調査検討の精度の向上が期待されるのみならず、個別の患者に対する安全対策も可能となる。

5 医療関係データを活用した研究のあり方について

(1)調査・研究の支援体制について

・すでに構築されているレセプトデータベースはもとより、電子カルテ等から構成されるデータベースは国内でも構築されていないため、活用可能な大規模な医療関係データベースの体制や技術基盤の整備に国は、さまざまな支援を行うべきである。
・研究費の枠組みに縛られない取り組みや、研究機関個々の対応を超えた連携など、例えば省庁や部局を超えた協力・支援を行うべきではないか。
・また、データベースを備える研究機関は、医薬品等の評価におけるレギュラトリーサイエンスに対する人材の育成、医薬品の規制当局との調査研究における連携や人材の交流ができるような体制を構築するべきである。

(2)行政の役割

・ データの提供者となる国民(患者)の理解・協力が得られ、社会全体として国民医療の質的向上や安全性確保のメリットを享受できるよう、臨床疫学、薬剤疫学等の利用による成果について、メリット及びデメリットの比較とともに、国民に分かりやすく説明するべき。
・ 薬剤疫学研究者及び医療関係者のデータ構築や活用体制の整備を支援するとともに、研究者の育成に努めるべきである。
・ そのため、日本国内での薬剤疫学等の医療安全を含む研究のための拠点整備を関係府省連携して行うべきである。
・ 中立・公平な研究の実施を促進するための研究費の提供、公的基金の整備などの経済的な支援を強化するべきである。
・ 医薬品等の安全対策において、国際的なガイドラインに沿って、安全対策上の課題に沿って必要な医薬品等に対して、薬剤疫学研究を組み込んだリスクマネジメントの実施を企業に課すこと、また、研究機関、医療機関の協力を得られるよう、指導力を発揮するべきである。

(3)大学・公的研究機関の役割

・臨床疫学的・薬剤疫学的手法を用いた調査分析の実施、データ連結技術等を研究することにより、医療関係データベースを利用したより高精度な調査・解析を可能にするため、臨床疫学分野、薬剤疫学分野、情報セキュリティー、患者の個人情報保護に係る分野の人材育成を図るべきである。

・また、医療関係データベースを活用して提供された医薬品の安全性等に係る情報をどのように解釈するか、リスクコミュニケーション分野の人材育成も重要である。

(4)医療従事者の役割

- 医療従事者や薬剤疫学関係者が、データ提供に協力することにより、医療関係データベースが充実、医薬品等の有効性、安全性の研究を通じて、自らも治療法の改善や提供する医療の質の向上に繋がるメリットを享受することを国民が認識できるような啓発に努めるとともに、情報の信頼性、研究の信頼性確保のための指針を示すその他の必要な行政的な措置を行うべきである。
- 薬剤疫学研究等に対する医療従事者の協力が求められると同時に、研究から得られたアウトカムに基づき、医療の質の向上を図る取組を行うべきである。このような対応に、職能団体も積極的に取り組むべきである。

(Reference)

- 「薬害肝炎事件の検証及び再発防止のための医薬品行政のあり方検討委員会」最終提言（平成22年3月30日） (今後掲載されるURLを記載する)
- FDAは2008年5月にセンチネル・イニシアティブを立ち上げ2010年7月までに2500万人のデータ、2012年7月までに1億人のデータへのアクセスを確立するという目標を設定 (http://www.fda.gov/Safety/FDAsSentinelInitiative/default.htm)
- 2004年9月、米国で関節炎治療薬であるVioxx（一般名rofecoxib）の長期使用による心血管リスクの増加が確認されたとして、メルク社はVioxxを自主回収 (http://www.fda.gov/Drugs/DrugSafety/PostmarketDrugSafetyInformationforPatientsandProviders/ucm103420.htm)
- ハーバード大学のグループらによるレセプトデータベースと薬剤疫学的手法を用いた解析により、後ろ向き解析ではあるものの、3年程度で、つまり実際に回収が行われるよりも2年も前に心血管リスクの増加を示唆するデータが得られている
  Brown JS, Kulldorff M, Chan KA, Davis RL, Graham D, Pettus PT, Andrade SE, Raebel MA, Herrinton L, Roblin D, Boudreau D, Smith D, Gurwitz JH, Gunter MH, and Platt R., Early detection of adverse drug events within population-based health networks: application of sequential testing methods, *Pharmacoepidemiology and Drug Safety*. 2007 Dec;16(12):1275-1284.,
- 「医療サービスの質の向上等のためのレセプト情報等の活用に関する検討会」 (http://www.mhlw.go.jp/shingi/2008/01/dl/s0130-16a.pdf)
- ICH E2Eガイドライン「医薬品安全監視の計画」 (http://www.pmda.go.jp/ich/e/e2e_05_9_16.pdf)
- 「高齢者の医療の確保に関する法律」（高確法）
- 統計法 (http://www.stat.go.jp/index/seido/1-1n.htm)
- 疫学研究に関する倫理指針（平成19年8月16日）（文部科学省、厚生労働省） (http://www.lifescience.mext.go.jp/files/pdf/37_139.pdf)

資料３

今後のスケジュール（案）

(これまでに実施した懇談会の日程)

・第1回:　平成21年8月21日:フリートーキング

・第2回:　平成21年10月29日:ヒアリング(1)

・勉強会:　平成21年11月19日

・第3回:　平成21年12月14日:ヒアリング(2)

・第4回:　平成22年2月15日:事務局原案について議論

・第5回:　平成22年4月14日:提言骨子案についての議論

・第6回:　平成22年5月19日:提言案についての議論

(今回の懇談会)

・第7回:　平成22年6月16日:有識者等へのヒアリング

＜パブリックコメントの募集＞

★第８回：平成22年7月22日 提言の最終とりまとめ

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。

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。