cpl.thalesgroup.com

THALES
Building a future we can all trust

医療ITセキュリティについて知っておくべき10項目

患者データの保護は、複雑な課題です。医療施設の全従業員から、施設のITシステムの全領域、医療提供者と連携する全ベンダー、パートナー、保険会社にまで影響が及びます。
多くの施設がHIPAA、HITRUST、その他のプライバシー規制への完全準拠の達成に取り組んでいます。しかし施設への全体的なリスクに対処するには、コンプライアンスの問題を超える多様な要素を考慮しなければなりません。それを念頭に置いた上での、医療ITセキュリティについて知っておくべき10項目をご紹介します。

10

PHI(Protected Health Information; 保護医療情報)は第一の標的である。

PHIの記録には通常、名前、生年月日、社会保障番号、保健情報、病歴などの機密データが含まれています。この情報は極めて有益なため、格好の標的となっています。情報漏えい危険度指数(Breach Level Index)によると、2018年で最多のデータ漏えいの種類が個人情報の盗難でしたが、これは驚くことではありません。

09

医療業界は最大のセキュリティ脅威に直面している。

情報漏えい危険度指数（Breach Level Index）によると、全業種の中で2018年上半期にセキュリティを脅かされる事象が最も多かったのは医療会社でした。

ほとんどの情報漏えいは内部から発生している。

医療業界における情報漏えいの73%は、従業員の不正または不注意な行為の結果です。特権の悪用から、電子メールやファクスの誤送信、ノートパソコンの紛失や盗難まで、機密情報はプロセスのどの時点でも漏えいする可能性があります。悪意がなくとも、データが保護されていない環境に入り込んでしまう場合があります。

08

コストが莫大になる可能性がある。

Ponemon Instituteの2019年データ漏えいコストに関する調査報告書によると、医療業界は全業界で漏えい記録1件あたりのコストが最も高く、429ドルに達しています。また情報漏えいに対処するための直接コストだけでは済まず、患者データを保護できなかったことにより、患者や利害関係者、コミュニティの信頼損失、組織の評判の失墜、患者や収益源の損失、さらには責任の拡大につながる可能性があります。

07

オンライン情報には年中無休の保護が必要である。

オンライン情報は年中無休で保護が必要です。医療記録と処方箋がオンライン化し、病院のネットワークでこのデータを医師と患者と保険会社が共有しているため、確実に決められた人物のみが情報やアプリケーションにアクセスできるようにし、強力な2要素認証で適切なアクセスポイントを保護し、データが移動中と保管時の両方で暗号化されているようにしなければなりません。たとえば、DEAのEPCS規制は、規制物質の電子処方箋を発行する際に強力な2要素認証を使用してEHRアプリケーションに対し再認証を行うことを医療従事者に義務付けています。

06

05

ルールは常に変化する。

連邦および州による法律は、1996年のHIPAAから2018年のGDPRまで、患者データを保護して情報漏えいを報告するように医療ITシステムへの要求を増やし続けており、罰金も増加しています。そのため、今すぐ対策を講じることで、州および国の遵守期限を守ることができ、連邦政府によるインセンティブプログラムを受けながら、セキュリティ予算を最大限に活用できます。

04

機密情報がいたるところに存在する。

医療提供者と医療従事者は、スマートフォン、PDA、ノートパソコンでモバイルコンピューティングを利用しており、医療ITシステムに新たな脆弱性を生み出しています。コピーを簡単に作成でき、バックアップは従来のデータセンターの境界を越えて仮想環境やクラウドに保管されるため、さらなるデータが漏えいのリスクにさらされています。

03

時間は最も重要な要素である。

2015年以降、電子医療記録を使用しない病院は、罰金の対象となっています。逆に、メディケアまたはメディケイドEHRの補助金の資格を得るには、病院とCAHは、ステージ2およびステージ3の目標に設定されている電子医療記録の「Meaningful Use（意義ある利用）」を実証する必要があります。EPCSの期限は州によって異なりますが、一部はすでに効力が生じています。

暗号化なしには、保護は不可能である。

暗号化されていないデータは、データベース内でも、最も離れたエンドユーザーによる使用中でも、その間のどの時点でも、盗難や悪用に対して脆弱です。暗号化の有無は、情報漏えいが発生した場合の責任を判断する決定的要因にもなります。

02

個人的に責任を問われる場合がある。

患者データの安全性への注力が高まり続けるにつれ、規制は個人的な責任も企業の責任に付け加える方向にシフトしており、データ保護の責任者に罰金や懲役が科される可能性があります。

01

これらはすべて恐ろしいことに聞こえるかもしれませんし、実際に怖れるべきです。
しかし、この10項目のリスト全体に対処するために知っておくべきことは1つだけです。
それが、タレスです。簡素化した拡張可能な患者データ保護を提供します。

医療業界で最も完全で一元化されたエンドツーエンドソリューションによって患者データのセキュリティを簡素化

タレスは、患者データの記録と健康歴、請求先アカウント情報、知的財産（医療および医薬特許など）、組織が保護する必要のあるその他のデータまたは取引情報を保護するための、柔軟で一元化されたソリューションを提供します。

タレスのアイデンティティ&データ保護（IDP）ソリューションは、暗号化、アクセスポリシー、鍵管理、認証を組み合わせた一元化されたアイデンティティ&データ保護フレームワークを使用することにより、包括的で、インテリジェントで、永続的で、拡張可能なアプローチによって医療組織がIT戦略を将来の事業成長に合わせることを可能にします。重要な暗号化と鍵管理の要件はすべて一元的に実装されているため、さまざまなベンダーの異なるシステムに投資する必要はありません。

単一の包括的なプラットフォームで、医療組織はコンプライアンスを確保し、重要なアプリケーションとePHIへのローカルアクセスとリモートアクセスを保護できます。Gemalto IDPは、アイデンティティ、トランザクション、およびアプリケーションのエンドツーエンドの保護を提供し、運用効率の確保に役立ちます。

中断のないアクセスのための最高のパフォーマンス

タレスのIDPを構成するすべてのコンポーネントは、優れた暗号化パフォーマンスを実現するように設計されており、ビジネスプロセスや患者の体験とシームレスに統合できます。高度に特殊化されたハードウェアアプライアンスへのデータ暗号化処理のオフロードと一元化により、最も要求の厳しい処理環境を簡単にサポートするパフォーマンスレベルを実現します。

- **ハードウェアセキュリティモジュール**（HSM）での強力な多要素認証により、ユーザーのアイデンティティを保護し、データへの物理的および論理的アクセスを制御して、組織の利害関係者の信頼を構築します。
- **ハードウェアトークンまたはソフトウェアトークン**（OTPアプリ）による強力な多要素認証により、さまざまな医療システムへのアクセスを制御し、DEAのEPCS規制の遵守を可能にします。同じトークンを使用して、規制物質のeRxを発行する際のEHRシステムに対する再認証だけでなく、施設外で働く医療従事者のEHRへのリモートアクセスを保護することもできます。
- **業界で検証済みのハードウェアベースの暗号化および鍵保管**プラットフォームにより、トランザクションとアプリケーションを保護し、データの整合性（紙からデジタルへの移行プロセスを含む）を確保し、監査証跡を維持します。
- **データ暗号化および制御**ソリューションにより、データセンターからエンドポイント（医師、臨床医、管理者が使用するモバイルデバイスを含む）、クラウドまで、ライフサイクル全体にわたってデータの所有権を保護および維持します。
- **高パフォーマンスの通信暗号化**ソリューションにより、情報を永続的に保護し、場所や境界を越えた制御の確保、運用の合理化、ディザスタリカバリの簡素化、コンプライアンスコストの削減を実現します。

合理化された実装で遵守期限を守り、罰金を回避

タレスのIDPソリューションは、既存のITインフラストラクチャに迅速かつ簡単に統合できるように設計されています。すぐに使用できるコネクタと統合機能、一元化された導入機能により、タレスは実装時間とコストを劇的に削減して、遵守期限を守り、罰金を回避できるようにします。

モジュール式の柔軟性と拡張性により、特定のコンプライアンスとデータセキュリティのニーズに対応

進化するセキュリティの脅威には、進化するソリューションが必要です。タレスは、共通の統合フレームワーク内でセキュリティモジュールの包括的な基盤を提供します。これにより、独自の戦略的データ保護要件に適合するセキュリティコントロールを選択して追加できます。この統合アプローチにより、最高レベルの保証と最小の所有コストで、現在そして将来のすべてのデータ資産を保護できます。

お問い合わせ先 – cpl.ipsales@thalesgroup.com すべてのオフィスの所在地と連絡先情報につきましては 、cpl.thalesgroup.com/ja/contact-usをご覧ください。