– Alan CoxYouはとにかくプライバシーがありません。  
– SCOTT MCNEALY 10。  
1。  
2。  
 密猟に対抗するゲームレンジャーやその他の人々は、あらゆるレベルで組織犯罪、暴力、インサイダーの脅威に直面していますが、国家諜報機関とは異なり、クリアランスや対諜報活動を管理する中央の権限はありません。  
 医療サービスであまりにも多くの人々に患者の記録を見せさせると、有名人のデータを検索するスキャンダルが発生します。  
32210。  
 はじめに4。  
 データ共有は頻繁に呼び出されますが、実際にそれを行おうとすると、あらゆる種類の問題が発生します。  
 銀行または会計事務所のすべての人にすべての顧客レコードを表示させると、悪質なマネージャーは、クライアントの競合他社の機密の財務情報を見て、クライアントに本当に良いアドバイスを与えることができます。  
 ネットワークのメリットが直線的に拡大するのと同じように、害も拡大します。  
 上記の5つの例の場合：1。  
 ゲームの保護をサポートするシステムは同様のことを行う必要がありますが、アクセス制御は、複数の保守、研究者、レンジャー、およびその他のアクターが関与するフェデレーションエフォートでなければなりません。3。  
 システムがより複雑になり、オペレーターがその努力をするインセンティブを欠いているため、どちらも実装が難しくなっています。  
 それでも、情報の共有や、学校やその他の機関が疑わしいクラウドサービスを使用することで発生するあらゆる種類の問題に常に圧力がかかっています。5。  
この章では、これらの種類のアクセス制御について説明します。  
前の章では、マルチレベルのセキュリティについて説明し、メカニズムを正しく理解するのが難しい場合があることを確認しました。  
 グループまたは役割は静的ですか、それとも動的ですか？国の方針、商法、職業倫理、またはFacebookSecurity Engineering323Ross Anderson10のグループのように設定されていますか。  
 はじめに友達–システムのユーザーによるものですか？人々がルールを無視したり、お互いを欺いたりするとどうなりますか？誰もが同じ上司のために働いている場合でも、組織のさまざまな部分がまったく異なるインセンティブを持つ可能性があります。  
より単純なケースから始めるために、徴収現場でセキュリティポリシーを設定しようとしていると仮定します。  
 それを止めるにはどうしたらよいでしょうか？TOP SECRETSECRETCONFIDENTIALOPEN図9。  
 したがって、図9の従来の公務員モデルで見たような、情報フローの制御境界が水平である代わりに、  
2。  
2-多国間セキュリティ横情報管理は組織的である可能性があります。これは、諜報機関が、ある外国で働いているエージェントの名前を、他のスパイの責任を負う部門から秘密にしておく場合などです。  
 それらは、患者の機密性が法律で患者の権利に基づいている医療のように、特定の病院部門または医療行為へのアクセスを制限することによって施行される場合があるように、2つの混合物である場合があります。  
医師、銀行家、スパイはすべて、明白な情報フローを防止するだけでなく、請求データなどのサイドチャネルを介した情報漏えいも防止する必要があることを学びました。  
セキュリティエンジニアリング324ロスアンダーソン10。  
 コンパートメントと格子モデル10。  
 これらは、第二次世界大戦のコードワードウルトラなど、アクセス制御グループを表現するためのプレコンピュータメカニズムであり、ドイツ語のエニグママシンを使用して暗号化されたメッセージのイギリスおよびアメリカの復号化を指していました。  
 そのため、ウルトラクリアランスは、暗号学者、翻訳者、アナリストに加えて、少数の人々にのみ与えられました。リストには、連合国の指導者とその上級将軍が含まれていました。  
 そのため、ウルトラが北アフリカへのイタリアの護送などの標的について語ったとき、連合軍は攻撃の1時間ほど前に飛行機で「発見」しました。  
 （ウルトラセキュリティは、David Kahn [1002]およびGordon Welchman [2007]によって記述されています。  
 妥協がインテリジェンスソースまたはメソッドを公開する可能性のある情報は、「TopSecret –特別なコンパートメントインテリジェンス」のTS / SCIとしてマークされ、1つ以上のコードワードを含む場合があります。  
 したがって、N個のコードワードがある場合、2N個のコンパートメントを持つことができます。一部の諜報機関では、100万人以上が活動しています。  
 長い勤続年数と年功のおかげで多数のコンパートメントへのアクセスを蓄積していたCIAのAldrich Amesは、彼が対諜報活動で働いていたため、ロシアのほぼすべての米国エージェントネットワークを裏切ることができました。ウォーカーのスパイ事件のさらに前例がありました。  
 したがって、アメリカ海軍の800隻の船はすべて同じ暗号鍵のセットで終わりました。ウォーカー一家はそれをロシア人に販売しました[876]。  
 分類はコードワードと一緒にラティスを形成します。これは、任意の2つのオブジェクトAとBが支配関係A> BまたはB> Aになる数学的な構造です。  
 例として、「Crypto」などのコードワードがあるとします。  
 これは、図10のように表すことができます。  
偶然にも、Bell-LaPadulaモデルは多かれ少なかれ変更なしで機能することができます。  
2。  
3：–一連のセキュリティラベル以前と同じように、HighとLowの間に情報フローがあります。HighはLowを支配するコンパートメントです。  
3 –次に、それらの間の情報フローはまったくないはずです。  
 20世紀にマルチレベルの安全な市場向けに構築されたほとんどの製品は、コンパートメントモードで使用できます。  
実際には、必須のアクセス制御製品は、区画化には効果がないことが判明しました。  
。  
）。  
 ラティスセキュリティモデルは、ここではほとんど役に立ちません。  
 指導者たちは、数百万の区画がテロとの戦争の邪魔になり、コミュニティが攻撃を未然に防ぐことができるようになったため、ブッシュ大統領が諜報コミュニティ内でより多くの情報共有を命じたと主張した。  
 そのため、今日では、政府システムは必須のアクセス制御を使用して、機密システムを未分類から、また最高機密システムを前の章で説明したデータダイオードやその他のメカニズムを使用して、両方から分離しています。  
Snowdenの啓示は、XKeyscoreなど、以前は多くのコンパートメントを持っていたシステムを検索する検索システムについてすべてを教えてくれました。  
 そのような世界では、地元のレーベルが邪魔をするだけです。しかし、それらがなければ、この本の第2版で尋ねたように、将来のアルドリッチエイムスをどうやって防ぐのですか？おそらく米国の諜報機関セキュリティエンジニアリング326ロスアンダーソン10。  
 TIVACのプライバシーは、失敗モードが代わりにEd Snowdenだったので幸運でした。  
その後、CIAでもコンパートメントが必ずしも有効であるとは限らなかったことがわかりました。  
 最も機密性の高いサイバー兵器はコンパートメント化されておらず、ユーザーはsysadminパスワードを共有し、ユーザーアクティビティの監視は行われず、履歴データが無制限に利用可能であることが明らかになりました。  
 実際、IntelコミュニティがTop Secretデータに使用するJointworldwide Intel Communications System（JWICS）は、まだ2要素認証を使用していません[2051]。  
 商業企業は、未発表の財務結果などの資料を保護するための特別なメカニズムを備えている場合もあります。私の大学では、ネットワークに接続されていないマシンでも試験問題をまとめています。  
10。  
脅威は、生息地への侵入から小規模な密猟密猟、産業規模での象牙、サイの角、トラの体の一部を収穫する組織犯罪のギャングにまで及びます。  
 そして、多くの場合、最良の密猟者は元レンジャーです。  
 そして、テクノロジーが問題を悪化させています。携帯電話のマストが発展途上国で普及し、密猟も増加しています。  
 重要な相違点は、擁護者がNGO、パークレンジャー、法執行機関の緩やかな連合であるということです。  
WildbookのリーダーであるTanya Berger-Wolfとのプロジェクトがありました。これは、画像認識を使用して、観光写真、カメラトラップ、ドローンなどのデータソースを通じて動物について収集したデータを照合および分析する生態学的情報管理システムです[92]。  
 現代のセキュリティエンジニアリング327ロスアンダーソン10。  
 TIGERSのプライバシー画像認識ソフトウェアは、特に象、キリン、シマウマなどの特徴的なマーキングが施された大きな動物の場合に、これを実現可能にします。  
2015年、スペインの2人の市民がナミビアのKnersvlagte自然保護区で49の小さな多肉植物で逮捕されました。ホテルの部屋を検索したところ、2000以上が発見され、そのうち数百が絶滅危惧種でした。  
 彼らは有罪を認め、160,000ドルの罰金を支払い、その国では一生禁止されました。  
 このような事件は、野生生物のアグリゲーターがアクセス制御を必要としていることを示しており、植物学者、動物学者などの間でオープンデータについての再考につながっています[1166]。希少な植物では、泥棒が単一の標本のGPS位置を学習することを望んでいません。  
 そこでの目標は、すべての既知のカメの公開データベースであり、修復家は、メキシコの360 km2の地域に生息するすべての野生の標本を撮影するのに忙しい。  
 ユキヒョウを使用して、Wildbookは1つのネパール保守派からの3年間のカメラトラップデータを持っていて、ネパール、インド、パキスタンの5つの場所にこの規模を支援するセキュリティポリシーを望んでいました。  
 アフリカでも状況は似ています。 Wildbookは、シマウマを追跡することから始まりました。シマウマの中で、Gr´evyのシマウマは絶滅の危機に瀕しています。  
 一部の観光客は、タグ付けの方法を知らないだけです。馬鹿げている人もいて、車から降りて食べられます。  
新しい野生生物集約サイトは、画像認識を使用して個体内の動物を識別し、目撃情報をロケーション履歴にリンクできます。次に、他の機械学習技術がこれらの履歴を動きモデルに集約します。  
 これは、人間の多様性から動物のプライバシーを保護する方法の1つです。高度に抽象化されたデータは、多くの場合、少ないよりも敏感です。  
 そのような個人は、ダークサイドに行く場合に最高の密猟者を作り、密猟者の手から自分のスキルを学ぶモデルを維持する必要があります。  
私たちの主な保護目標は、「種Aの動物は場所Xの時間Tにいる可能性が高い」など、野生生物犯罪者に行動可能なインテリジェンスを与えないことです。  
4。  
 私たちの出発点は、運用調査モデルをガイドとして使用して、（a）最近のジオタグ付き写真、（b）予測モデル、および（c）写真コレクションのアクセスルールを導き出すことです。  
アクセスには4つのレベルがあります。  
 レベル1では管理者が1種あたり20人程度になる可能性があります。アクセス制御が委任されているため、保護区または保護区ごとにさらに管理者がいます。  
 レベル3では、写真を投稿した無数の市民が無数にあり、機密ではない出力にアクセスできます。  
インサイダーによる脅威の軽減の焦点は、欠陥を残そうとする可能性のある保守的な立場です。  
 利用可能な最も力強い抑止力は、保守的な同業他社からの社会的圧力です。忠誠心のある同僚、チームワークの感覚、使命感です。  
 発展途上国（LDC）の条件で低賃金で10名または20名を雇う経済的に伸びたコンサーヴァンシーでは、いつでも全員の肩を監視する部署の警備員を雇うという公務員のアプローチは、とにかく実現不可能です。 。  
 すでに種ごと、場所ごとに管理者がいます。  
 私たちのコアストラテジーは、2次元の透明性に基づく、状況認識と抑止のための地域の公的監査能力です。  
 rhinoグループのSta↵は、個々の目撃記録やモデルなど、rhinoのレコードを誰が見ていたかを確認しながら、Serengetiで作業しているSta↵が、そこでデータやモデルに関心のある人を確認します。  
レベル1のスタッフは、レベル2のスタッフを登録して、他のコンサーバンシーとのピアリングの手配を行うことができますが、それらの関連するアクションはレベル2の同僚に表示されます。  
10。  
 ヘルスケアセクターは、ミリセキュリティエンジニアリング329ロスアンダーソンよりもはるかに大きな国民所得のシェアを費やしています10。  
 すべての先進国での医療記録のプライバシー、および病院はまだ自動化されていませんが、彼らは急速に追いついています。  
多くの国には医療の安全性とプライバシーを規制する法律があり、医療ITセクターの形成に役立ちます。  
 悪名高い事件の1つとして、マサチューセッツ州ニュートンにあるニュートンウェルズリー病院で整形外科技師として働いていた有罪判決を受けた児童強姦は、元従業員のパスワードを使用して、954人の患者（主に若い女性）の記録を調べ、それから彼はわいせつな電話をかけました[317]。  
HIPAA規制は時間とともに変化しました。  
 ルール作成の前段階で、HHSはプライバシーの懸念により、586,000人のアメリカ人ががん治療の模索を遅らせ、200万人以上がメンタルヘルス治療の模索を遅らせたと推定しました。  
 2002年、ブッシュ大統領はそれらを書き直して「プライバシールール」に緩和しました。これには、病院や保険会社などの対象エンティティが、保護された健康情報（PHI）の特定のセキュリティ基準と手順を維持することを要求します（違反に対する民事罰と刑事罰の両方）（ただし、最初の数年間に課された罰はほとんどありません）。対象となる事業体は、治療または支払いをサポートするために情報を開示できますが、他の開示では患者の同意が必要です。これは研究者による不満につながった。  
オバマ大統領の法案が医療ITに数十億ドルを割り当てたとき、これはさらに後押しされ、プライバシー違反の罰則をわずかに増やしました。 2013年に、彼の管理はルールを対象事業体のビジネスアソシエイトに拡張しました。  
医療プライバシー擁護者は、保護された健康情報を自由かつ密かに集約および仲介することを健康データホルダーに権限を与えた一方、病院はそれがコストに追加することを訴え、患者擁護者は10年以上の間病院の病院が言い訳としてしばしば使用していると不平を言っています役に立たない-負傷した親族を追跡する人々を防ぐことなどによって[827]。  
S  
 もう1つの要因は、地域の市場効果です。たとえば、米国では、請求レコードを生成する必要があるため、システムはある程度推進されています。また、2019年には、Epicが電子医療記録システムの市場シェアを29％も持つ市場に集中しています。 Cernerは26％でした[1351]。  
 1995年、英国政府はすべての医療記録を一元化しようとしましたが、これが医師の専門機関である英国医師会（BMA）との対立につながりました。  
4。  
 25年にわたる医療プライバシーの進化は、貴重なケーススタディです。テクノロジーの大幅な変化にもかかわらず、問題がほとんど変化していないことは注目に値します。  
 居住者が携帯する医療保険カードの現在の処方箋やアレルギーなどのドイツ語の要約データ。他の国々は、緊急データが人間が読めるMedAlertブレスレットからスマートカードに移されると、飛行機や外国の休日に病気になる患者を危険にさらす可能性があると推論し、これを阻止しました。  
 プライバシーの問題からか、宗教的な理由からか、研究に使用されている記録を人々が止めることができるかどうかについても、激しい議論がありました。  
 申立人はフィンランドの病院の看護師で、HIV陽性でした。  
病院のアクセス制御は、同僚が彼女の記録にアクセスするのを防ぐのに十分ではなく、その監査証跡は、プライバシーを侵害した人物を特定するのに十分ではありませんでした。  
「この判断は2010年に最終的になり、それ以来、医療提供者は患者がデータの二次使用から効果的にオプトアウトできるようにシステムを設計することを想定されてきました。  
4。  
 主な目的は安全であり、プライバシーはしばしば劣悪です。  
医療システムにはさまざまな危険があり、特に安全性のユーザビリティの障害があり、道路事故と同じくらい多くの人々を殺すと考えられています。  
 セキュリティと直接対話します。脆弱性は特に、輸液ポンプなどの製品のリコールをFDAに義務付ける結果となる可能性があります。  
2番目の危険は、医療プライバシーの信頼が失われると、人々が治療を回避したり、治療を遅らせたりすることです。  
 最も包括的なデータは、Pres-Security Engineering331Ross Anderson10の下でのHIPAAルールの作成前に、米国保健社会福祉省によって収集されました。  
 健康記録プライバシープライバシークリントン。  
 一方、100万人以上が性感染症の治療を求めていなかった[873]; 2。  
 最も権威のある文献レビューは、多くの患者、特に10代の若者、同性愛者の男性および売春婦が情報を差し控えた、または機密保持の懸念のために単に治療を求めることができなかったと結論付けました。  
したがって、プライバシーが不十分であることは安全上の問題であり、退役軍人からリスクのある疎外されたグループまで、さまざまな市民に平等医療へのアクセスを提供する上で重要な要素です。  
 病院のコンピューターで日付の記録を調べている不気味な医師から政治家や有名人をストーカーしているジャーナリストまで、特定の個人に対する標的型攻撃があります。  
 政府または病院が数百万の記録を製薬会社に販売する場合、時には秘密に、時には記録が「匿名化」されて個人の健康情報ではなくなったという主張を伴って、大量攻撃があります。3。医療提供者には報告義務があるため、これらは民間企業における違反の割合の5倍で報告されます。  
結果としての報道は、主に大量の攻撃と事故であり、直接危険にさらされているわけではないかもしれませんが、多くの人が健康データのプライバシーを恐れています。  
では、直接的なリスクはどのくらいですか？そして、リスクがどれほど技術に起因するのでしょうか？物事が一元化されると、私たちは根本的なスケーリングの問題に直面します。  
 個人情報を大きなデータベースに集約すると、これらの両方のリスク要因が同時に増加します。  
4。  
 一部の共有システムでは、多くの患者のデータにアクセスでき、乱用されています。  
 ローカルシステムでも大規模なデータを公開できます。大規模な地区の病院では、100万人を超える元患者の記録がある可能性があります。  
乱用スケーリングを防止するために、横方向の情報フロー制御が必要です。  
 あらゆる種類のアドホックプライバシーメカニズムが試されていましたが、1990年代の半ばまでに、適切なアクセス制御ポリシーの必要性を感じました。  
4。  
 病院には請求を処理するための中央管理システムがあり、一部の記録は紙からコンピューターに移動していました。  
 1991年にマーガレットサッチャーの政府が行った最後のことの1つは、地域のコミッショナーが保険会社のように行動し、病院が治療費を請求する医療サービスの「内部市場」を作成することでした。これを実装することは、厄介で論争の多い、進行中の作業でした。  
 インターネットブームが始まったばかりで、医療関係者は個人の電子メールで情報を送信し始め、熱心な人々は病院から医療機関まで電子的にテスト結果を取得するシステムを構築し始めていました。  
2。  
その物語のための3）。  
 私は彼らのスタッフやメンバーと協力して開発しました。  
 政府の戦略では、異なる病院や医師の同じ患者に関する異なる記録を保持する従来のシステムではなく、患者の脳梗塞から剖検までを追跡する単一の電子患者記録（EPR）を想定していました。紹介状と退院書簡の形で情報を流します。  
 異なる人々はセキュリティエンジニアリング333ロスアンダーソン10を持っています。  
 健康記録プライバシーあなたの人生のさまざまな段階であなたの記録にアクセスできます;あなたの出生記録はまたあなたの母親の記録の一部であり、あなたが軍にいる間または刑務所にいる間のあなたの記録は政府に属します、そしてあなたが性感染症の治療を受けるとき、あなたはそれを完全に秘密に保つ権利を持つかもしれません。  
しかし、これは明らかにスターターではありませんでした。  
 それは他のあらゆる種類の点でも間違っていました。 HIVに感染している人の中には、自分の状態についてオープンである人もいれば、軽度の状態にある人は、HIVに非常に敏感です。  
 患者の同意は中心的です。記録は、患者が同意した場合、または結核などの感染症の接触追跡などの限られた範囲の法的例外でのみ、第三者と共有できます。  
 同じ人々がアクセスできる最大のファクトセットとしてレコードを定義しました。患者+医師、患者+医師と手術の状態、患者+患者の母親+医師+状態などです。  
本当に難しい問題は、レコードの二次利用でした。  
’1995年までに、製薬会社によるリモートクエリが匿名の可能性のあるデータを返すことを許可する見返りに、補助金付きのコンピュータを一般開業医（GP）1に提供している会社がすでに見られました。  
新しいことは何も試みず、既存のベストプラクティスを体系化し、それを要約して、医師、エンジニア、または管理者の誰もが理解できるテキストのページにまとめました。  
1。  
2。  
また、患者の代弁者としての役割も果たし、医療、病院、コミュニティの間のケアに参加します。  
セキュリティエンジニアリング334ロスアンダーソン10。  
 アクセス制御リストの「健康記録プライバシー」。  
3。  
 アクセス制御リストを変更できるのは彼女だけであり、他の医療専門家を追加できるだけです。  
 同意と通知：責任のある臨床医は、レコードが開かれたとき、その後のすべての追加、および責任が移されたときはいつでも、患者のレコードのアクセス制御リストにある名前を患者に通知する必要があります。5。  
6。  
 すべての削除の監査証跡も保持する必要があります。  
 情報フロー：Bのアクセス制御リストがAに含まれている場合にのみ、レコードAから派生した情報をレコードBに追加できます。  
 集約管理：個人の健康情報の集約を防ぐための効果的な対策がなければならない。  
9。  
 その有効性は、独立した専門家による評価の対象となります。  
実際、コンパートメントは患者よりも多いため、コンパートメントは論理的な限界に達します。  
 完全なポリシーは、強制されている可能性のある脆弱な患者によるレコードへのアクセスなど、より多くの問題に対処しました[58]。  
 BMAモデルは1996年に欧州医療機関連合（UEMO）によって採用され、ポリシーに関する公的協議からのフィードバックは[60]にあります。  
4。  
4。  
 病院規模でアクセス制御を行う実用的な方法は、「病棟の看護師は、病棟に来てから90日以内に来たすべての患者の記録を見ることができる」、「主治医はすべての記録を見ることができる」などのルールによることが判明しました彼女の部門で治療を受けた患者」、および「主治医はすべての患者の記録を見ることができますが、彼女がその部門で治療されたことがない患者の記録にアクセスすると、その患者のケアを担当する主任医師通知されます '2。  
 後から考えると、BMAモデルは医師が言ったことを無損失で圧縮したものであり、役割ベースのモデルは少し損失の多いバージョンでしたが、実際に病院が行うものを実装し、そのコンテキストでうまく機能しました。  
 GPは、サプライヤから入手したすべてのアプリケーションコードを信頼する必要があり、その進化に影響を与える可能性はありましたが、信頼できる有用なサブセットはありませんでした。  
PASは不安定で、しばしばダウンしていたため、安全が重要なシステムをそれに依存させることは受け入れられませんでした。  
保健省からの政策対応は、フィオナ・カルディコットダムの下で調査委員会を設置することでした。  
 これは少なくとも始まりでしたが、モラルハザードが発生しました。通常、上級看護師であるプライバシー担当者は、問題が発生すると非難されましたが、実際のポリシーは大臣によって設定されました。アリスが失敗の代償を支払う間、システムを守るボブの第8章で。  
 匿名化の限界については、次の章で説明します。  
4。  
 知られているように、ITのための国家プログラム（NPfIT）は、世界で最も高価であることが判明しました。2Hastingsシステムは、当初BMAプロジェクトとは独立して設計されました。  
3英国の法律は、EUデータ保護指令（95/46 / EC）を英国の法律に置き換えて、プライバシーに関する平等な立場を提供することになっていた。この抜け穴は、英国の企業に多くのくねくねした部屋を許したいくつかの1つであり、フランス人とドイツ人を悩ませました[597]。  
セキュリティエンジニアリング336ロスアンダーソン10。  
 健康記録プライバシー民間人のIT災害。  
 キャメロンはプロジェクトを正式に殺害しましたが、根強いサプライヤー契約のためにその影響は何年も続き、医療ITは10年間維持されました[1559]。  
セキュリティポリシーには3つの主要なメカニズムがありました。  
 ヘイスティングスで開拓されたような役割ベースのアクセス制御があります。  
 患者のデータにアクセスするために、sta↵メンバーは正当な関係も必要です。  
3。  
 ただし、プロバイダーはこれを実装するためのラウンドを決してしませんでした。  
 2007年に遅く、議会の健康委員会は、サプライヤーがまだ仕様を取得していないことを指摘しました[925]。  
 以前は、メモは精神科医のファイリングキャビネットに紙で保管されていました。スミス夫人が月に一度、ジョーンズ博士に会ったことだけが、受付係にわかった。  
 したがって、すべての人がすべてにアクセスできました。  
プロジェクトの管理ミスのおかげで、イギリスの病院の10％未満が実際にこれらのシステムをインストールしましたが、「RBAC +関係」の教義が他の組織に影響を与えています。  
4。  
10。  
4。  
 政治家がNPfITを販売するために使用した話の1つは、「あなたがアバディーンで病気になり、病院がロンドンのレコードへのアクセスを望んでいるとします。  
。  
 これは、そして今も変わらず偽物です。  
 しかし、ポリシーはポリシーであり、セキュリティエンジニアリング337ロスアンダーソン10。健康記録のプライバシースコットランドでは、政府が処方箋とアレルギーの「救急医療記録」を作成しました。これは、緊急治療室の臨床医、救急隊員、および時間外医療ヘルプラインサービスのオペレーターが使用するために中央データベースに保存されます。  
500万人が数万人に利用可能になり、必然的に起こりました。ダンファームリンにあるクイーンマーガレット病院の1人の医師が逮捕され、当時のゴードンブラウン首相、アレックスサーモンド首相、およびさまざまなスポーツやテレビの人物の健康記録を閲覧したとして起訴されました。  
 患者はこのシステムをオプトアウトする権利を求められていましたが、それは非常に奇妙なオプトアウトでした：あなたが何もしなかった場合、あなたのデータはあなたのGPから収集され、エディンバラの保健省と救急車にも利用可能になりましたサービス。  
これはイギリスでもポリシーであり、「表示同意」と呼ばれていました。州はすべてを収集し、許可されたものだけをユーザーに表示していました。  
 これはNPfITを構築するための唯一の実用的な方法であると議会は保証した。彼らはこれを「現状の電子版」[925]と表現した。  
 オランダでも同様のことが起こり、市民の医療保険詳細のデータベースは、医師や薬剤師だけでなく、代わりの治療者やタクシー会社でもアクセスできるようになり、完全に予測可能な結果が得られました[186]。  
4。  
2レジリエンス集中型システムへの移行により、通常、障害はまれですが大きくなり、健康システムも例外ではありません。  
 2005年12月11日に脆弱性の早期警告があり、バンセフィールド油田貯蔵所での25万リットルのガソリンの漏出が蒸気雲を形成し、爆発しました。これはヨーロッパで最大の平時の爆発です。  
 私たちの地元の病院は、クラウドサービスへのプライマリネットワーク接続とバックアップネットワーク接続の両方が近くを通過したため、X線サービスを失いました。  
 ネットワークがなければ、X線を撮影することはできませんでした（また、病院の研究室からの病理検査結果も得られませんでした）。  
4コロナウイルスの危機において、SCRはGPレコードから大量のデータを追加し、それを計画者が利用できるようにし、デフォルトでオプトアウトすることによって「強化」されました。  
セキュリティエンジニアリング338ロスアンダーソン10。  
 健康記録のプライバシー10。  
4。  
 これらの記録は、完全な記録の匿名化が非現実的であるだけでなく、研究者によるアクセスに対する激しい政治的圧力のために、保護することが不可能であることが証明されています。  
Cameronは、以前はヘルスITビジネスを経営していた「透明性のある皇帝」を雇い、2011年にすべてのNHSpatientが研究の患者になることを目標に、英国を医薬品研究の世界的リーダーにするための「オープンデータメジャー」を発表しました。  
 匿名化は、あなたの個人情報があなたの郵便番号と生年月日まで編集されたことを意味します。次の章で説明するように、これは非常に不十分です。  
これにより、プライバシーキャンペーンの参加者、GP、その他の人々が集まり、医療用プライバシーキャンペーングループであるmedConfidentialを設立するのに十分な反論が生じました。  
 最初の推進力は同意でした、そして特にそのようなシステムをオプトアウトするために彼らのヨーロッパの法律の権利を行使しようとした患者は、結局、無視されるか、あるいは医療サービスから登録解除さえされました。  
いくつかの記録をアップロードできなかった場合、医師のボーナスはどのように計算されますか？2014年1月に、いくつかの調査により、HESデータが世界中の1000以上の製薬会社、大学などに販売されたことが明らかになりました-多くの場合、DVDのセットの形で1998年に遡る10億のエピソードが含まれています。  
この「ケア。  
 調査によると、ほとんどの人は、求められている限り、データを学術研究に使用できるように準備されています。しかし、ほとんどの人はそれを営利目的の研究者と共有する準備ができていません。  
 財務スキャンダルがありました。大臣が医療サービスに対する研究データの莫大な価値について話しているにもかかわらず、データはコスト回収ベースで販売されていました。a5HESは、「すべての入院、外来の予定、およびAの詳細を含むデータウェアハウスとして宣伝されています。イギリスのNHS病院でのE出席、NHS病院で治療された私立および外国の患者、およびNHSが支払う私立病院での治療これにより、少数を抑制し、人々が自分自身や他者を特定するのを防ぎ、患者の機密性が確実に維持されるようにします。  
https：// digitalを参照してください。  
uk / data-and-information / data-tools-and-services / data-services / hospital-episode-statistics。  
4。  
 管轄権の問題もありました。20GBではExcelには大きすぎるため、PAコンサルティングがHESデータをGoogleクラウドシステムにロードしてクライアントに転売したことが判明しました。  
 また、ソーシャルデータはUKdataを海外で販売しないことを約束していましたが、米国では宣伝されていました。そして、規制当局である医薬品および医療製品規制庁（MHRA）6でさえ、個人データを販売していたことが判明しました[1645]。  
 閣僚は学んだ教訓について話し、すべてのデータ公開のレビューが委託された。しかしこれが現れたとき、それは合法的であるかどうかではなく、内部ガイドラインが守られたかどうかだけを調査した[1496]。  
ロンドンのRoyal Free Hospitalからの600万人の患者の記録。急性腎障害を検出するためにアプリを開発したいと主張した（腎臓の患者の記録だけでなく、すべての記録を取得した）。  
 情報コミッショナーは病院を懲戒処分にしたが、データを削除するようにGoogle Deepmindに命令することに失敗した。  
•また、2015年に、タブロイド紙がオンライン薬局Phar-macy2Uを発見しました。これは、数千人の患者の詳細を略奪的マーケティング担当者に販売しています。広告および無許可の健康強調表示[662]。  
 英国最大のGPソフトウェアサプライヤーであるEMISの主要な後援者が株式を売却しました。  
•2017年に、2,700人の患者の記録を備えた2,700のGPプラクティスの3,000を含む6,000の顧客を持つ主要なGPソフトウェアサプライヤーTPPは、「拡張データ共有」をオンにして、地元の病院の医師が記録を見ることができるようにしました。  
 記録はまた目に見えました6 MHRAはまた、それを望んでいる医療関係者が有害な臨床試験結果に関するデータを利用できるようにすることにそれほど熱心ではありませんでした。  
セキュリティエンジニアリング340ロスアンダーソン10。  
 介護施設、刑務所、入国管理センターにいる健康記録プライバシーの顧客。  
•2018年に、2008年から2013年にかけてイギリスで診断された18万人すべての肺がん患者の記録が、がん登録データは「医療目的」でのみ販売されると主張していたPublic HealthEnglandによってタバコ会社に提出されました。  
 米国では、退役軍人管理局がそのようなシステムを病院のネットワークに運用しています。ハリケーンカトリーナの後、テキサスまたはフロリダ、あるいはミネソタで難民となったルイジアナ出身の退役軍人は、地元のVA病院に直接行き、医師の指先でメモを見つけることができました。ニューオーリンズの他の多くの病院の患者が亡くなったとき彼らのメモはすべて一緒に。  
 2019年11月、GoogleがAscensionに代わって5,000万人のアメリカ人の医療記録を処理するためのアウトソーシング契約を結んだことを指摘し、内部告発者はデータが匿名化されていないことさえ明らかにした。 GoogleとAscensionの両方のスタッフが患者データへの完全なアクセス権を持っていました。  
Googleは米国からVAデータも取得しました。これは、ICOが米国に対してそれを決定した後、ロンドンのデータの代わりに使用しました。  
 EUの一般データ保護規則には、市場調査を排除する製薬会社のロビーによる「研究」に対する便利な免除があります。  
 これは、1990年代に麻薬処方記録の収集から始まり、大幅に拡大しました。  
4。  
 私たちは第2章で、サイバー犯罪のエコシステムは過去10年間の巨大な技術変化によってあまり変化していなかったことに言及しました。健康プライバシーエコシステムについても同様です。  
 ますます複雑なアウトソーシングへの移行も容赦ないようです。専門の企業がX線画像や病理検査などを処理し、対象の専門家が糖尿病などの特定の疾患の治療を支援することを期待できます。  
 セキュリティエンジニアリングはこの標準の範囲外です。たとえば、DeepmindのスマートフォンアプリはOAuth2を使用します。アメリカでは、新しい連邦情報共有規則により、プロバイダーがあなたの記録をサードセキュリティエンジニアリング341ロスアンダーソン10に送信するように要求される場合があります。  
 データ交換を承認した後の健康記録プライバシーアップルの健康記録などのパーティーアプリ。  
 薬物乱用などのデータは、保険へのアクセスを制限するだけでなく、雇用主などからも要求される可能性があります。  
 人々がマイクロソフト、アマゾン、グーグルの健康データを信頼するかどうかは別として、あなたはそれをすべて共有する必要があるか、まったく共有しない必要があります。全期間の記録よりもきめの細かいアクセス制御のための規定はありません。  
英国では、医学教授と製薬会社がすべてのGPデータを収集するための新たな機会を得て、医療記録、AI、ゲノミクスに基づいた3つの大きな新しい医療産業について話しています。  
 2019年に、5つの病院が前大臣が経営する製薬会社と取引を行ったことが発表されました。これらの病院は、出資の見返りとして「匿名化」されたデータを研究に提供しています[500]。  
データ。  
 この茂みをどのようにナビゲートできるでしょうか？英国のキャンペーングループmedConfidentialの見解では、3つのことが必要です。  
 まず、ヨーロッパの法律に基づいて権利を行使できるようにするには、実際の患者の同意が必要です。  
2。  
 誤って説明されている、またはまったく言及されていないセカンダリデータの使用を静かにオプトインしてはなりません。特に患者が失敗した場合に、患者に真実を伝える適切なセキュリティメカニズムが必要です。  
 第三に、本当の透明性がまだあるはずです。  
 数千万人の患者がアクセスを監査できれば、実際に数十万人が実際にそうしたとしても、これは虐待の大部分を抑止するはずです。  
 英国では、20年を無駄にしてきました。NPfITでの10年と、データを売ろうとしないふりをしてさらに10年。  
4。  
 同意した他の患者から収集された100,000のゲノムのさらなる研究データベースがあります。  
 彼らは死亡通知のリストをインポートし、死亡率を、年齢や性別だけでなく、社会統計のようにだけでなく、社会的剥奪、人種、喫煙歴、ボディマス指数、特定の併存疾患によって分析し、1700万人を超える患者と2020年2月から4月にかけて6,000人以上が死亡[2025]。  
 データのコピーが少なく、患者のオプトアウトを強制できるため、プライバシーリスクはより制御しやすくなる可能性があります。  
 コンピュータが登場する前の時代、観察疫学とは、病院や外科のライブラリに座って、何千もの紙の記録を調べて関心のある診断を探し、数週間から数か月後に特定可能な個人情報ではなく統計表を使って作業を終えることを意味していました。  
4。  
1倫理したがって、健康データを扱う研究者は倫理に注意を払うべきです。  
 歴史的に、それは医学研究における一連の倫理的虐待であり、研究倫理の発展をより一般的にした。  
 実験は1932年から1972年まで実施されましたが、効果的な抗生物質治療が1947年に利用可能になった後でも、感染した男性は治療されませんでした。  
 彼はまた、1943年から5月にビルケナウで双子の実験を行った同僚のヨーゼフメンゲレ博士と同様に、同意なしに戦争捕虜と占領国の民間人に対して人間の実験を行いました。その後、被験者はしばしば殺されて解剖されました。  
セキュリティエンジニアリング343ロスアンダーソン10。  
 健康記録のプライバシー•英国のアルダーヘイスキャンダルで、報道機関は、病理医がいかなる種類の同意もなく、生きている患者と死んでいる患者の「興味深い」身体サンプルを日常的に保存していることを発見しました。  
 これは国民の信頼に深刻な損害を与え、その結果は英国の悲劇学の研究を損なった。  
ナチス医師の裁判は1948年にニュルンベルク法に至り、その下では被験者の自発的かつインフォームドコンセントが不可欠でした。  
これは後に1964年に医学研究における倫理に関するヘルシンキ宣言につながった。それは独立した制度的審査委員会倫理委員会の必要性を組み込むために1975年にタスケギーの後に改訂され、その後1983年、1989年、1996年、2000年および2008年に改訂された。  
 宣言は、最初とその後の両方で、研究への参加について情報に基づいた決定を行う患者の権利を支持します。道徳的に合理的な一連の期待は、4つの原則を具体化する必要があります。  
 データイニシアチブでデータがどのように使用されるかについての一連の期待は、個人の尊重の原則に基づいている必要があります。  
2。  
 これには、公共の利益における個人市民のプライバシーを妨害する（他者の利益を保護することを含む）国家および他の人々の権限に対する制限が含まれます。  
 データイニシアチブでデータがどのように使用（または再利用）されるかについての一連の期待、およびこれらの期待が確実に満たされるようにするための適切な手段と手順は、道徳的に関連する関心を持つ人々の参加を得て決定する必要があります。  
4。  
 すべての価値と利益が公正に表される必要があります-実際には多くの場合、関連する関心を持つすべての人々を関与させることが実行可能ではない場合。  
 データイニシアチブは、それ自体が道徳的に正当化されるガバナンスと説明責任の効果的なシステムに従う必要があります。  
 効果的な説明責任の維持には、影響を受ける人々や社会に対して、ガバナンス、実行、管理の期待と失敗を伝えるための効果的な対策を含める必要があります。  
ただし、倫理プロセスにはモラルハザードがたくさんあることに注意してください。データを乱用する大手企業は、日常的に倫理団体を設立して、自分たちの行動を許しません。  
4。  
それ以来、このモデルを使用して、サイバー犯罪に関する私たち自身の研究を導きました。これは、多くの点で類似しています。  
 ただし、多くの場合、調査のための倫理的な訴訟を起こすことができますが、そのような決定を下し、記録するためのプロセスには、慎重な検討が必要です。  
同じ原理は、機械学習の倫理について考えるための良い出発点になるかもしれません。  
10。  
6社会的ケアと教育同じ問題が教育と社会的ケアにも波及しています。  
 2006年、英国の情報コミッショナーは私たちのグループにこの安全とプライバシーの側面を研究するように依頼しました。  
 そして、麻薬中毒サービスや売春サービスとの接触の記録は非常に非難されています。  
これは、2007年11月に税セキュリティエンジニアリング345ロスアンダーソン10が行われたときに、さらに深刻な政治問題となりました。  
 HEALTH RECORD PRIVACY当局は、英国の子どもの恩恵データベース全体、つまり子どもを持つ英国のすべての家族に関する個人情報を含む2枚のDVDを失いました。  
 さらに見直した結果、児童保護に関わるソーシャルワーカーを編成する新しい「eCaf」システムの計画も放棄しました。  
直接電子アクセスによって医学と社会医療の間でデータを共有しようとする試みは、完全性とプライバシーの問題を引き起こしました。  
 医療記録は追加専用であるため、TheGPはこれを阻止するために彼らの仕事をカットするでしょう。また、糖尿病患者の視力検査をスケジュールするための目標を達成できなくなり、収入が減る可能性があります。  
「データベースの状態」レポートでは、教育におけるプライバシーも強調されました。  
 さらに、学校は指紋スキャナーから出席記録や図書館の本の貸付、さらにCCTVが教室を継続的に録画する（教師が子供による誤った非難から身を守ることができる）まで、さらに監視を追加し始めました。  
 ソーシャルワーカーがいる貧しい子供たちを非難するのではなく、皆に与えてみませんか？この大規模な反対を呼び覚まし、2016年の最高裁判所で敗北し、法的にも政治的にも容認できる方法を大臣が見つけ出せなかったため、最終的に2019年に放棄されました。  
両親による散発的な抗議に続いて、現在、少なくとも1つのNGOが子どもの権利のために働いています7。  
 プライバシー規制当局である情報コミッショナーでさえ、7https：// www。  
orgSecurity Engineering346Ross Anderson 10。  
 健康記録プライバシービーメンは、子供の利用規約が13歳未満のユーザーによって使用が禁止されている場合、たとえばVimeoを使用して彼女のWebサイトで説明ビデオを公開するなど、子供の問題を知らないことを非難しました。  
医療ITの安全性とプライバシーに関する四半世紀近くの闘争と、教育とソーシャルケアにおけるITの関連主題を振り返ると、政治的ステレオタイプに準拠した失敗が見られます。彼らは意味がありましたがナイーブでした。彼らは官僚的な中央集権と数十億ポンドの契約の面でしか考えられなかった（一部は、彼らのオフィスの期間の前または後に大臣を雇った）。彼らはどのように仕様書を書くべきか全く知りませんでした。物事がうまくいかなかったとき、彼らは怒って嘘をついた。そして彼らはすべてにアクセスすることを要求する医学研究者のような特別な利益のための吸盤でした。  
10。  
7チャイナウォール多国間安全保障の最終的な風味は、デビッドブリューワーとマイケルナッシュによって公式化されたチャイニーズウォールモデルです[319]。  
モデルのスコープはファイナンスよりも広いです。  
典型的なルールは、「最近1つの会社で働いたパートナーは、同じセクターの他の会社の書類を見ることはできない」ということです。  
したがって、チャイニーズウォールモデルでは、自由な選択と必須のアクセス制御が混在しています。パートナーはどの石油会社のために働くかを選択できますが、いったんその決定が行われると、そのセクターでの行動は制約されます。  
したがって、アクセス制御はステートフルになります。  
 各オブジェクトcに対して、cの会社のy（c）とcの利益相反クラスのx（c）を書くと、BLPのようにそれが可能になります。これは、2010–15政府が自由民主党連合のパートナーであるセキュリティエンジニアリング347ロスであるにもかかわらず、アンダーソン10。  
 HEALTH RECORD PRIVACYbeは2つのプロパティで表されます。•シンプルなセキュリティプロパティ：サブジェクトsは、sが読み取り可能なすべてのc0、y（c）/ 2 x（c0）またはy（c）=の場合に限り、cにアクセスできます。 y（c0）•\*-プロパティ：sがx（c0）=↵およびy（c）= y（c0）でc0を読み取れない場合にのみ、サブジェクトsがc​​に書き込むことができます。  
隠れチャネルに関するいくつかの興味深い新しい質問もあります。  
 1つの大規模なソフトウェアコンサルタントは、各従業員がサニタイズされ、お客様と合意した「分類されていない」CVを含むエントリを維持しています。  
 コンサルタントのマネージャーは、起こり得る競合を認識し、疑わしい場合はCVをクライアントに転送しないでください。これが失敗した場合、クライアントはCVから潜在的な競合を発見できます。これも失敗した場合、コンサルタントは、発生する可能性のある競合が発生したらすぐに報告する義務があります。  
 銀行のマネージャーが最高の顧客の競争相手の銀行の声明を単に見るとどうなりますか？ここでは、たとえば、顧客にいくつかの認証用の質問に答えさせるなどして、sta gettingメンバーがその顧客のセキュリティコンテキストを確立している場合を除いて、現代のシステムはアクセスを制限する傾向があります。  
中国の壁の1つの顕著な失敗モードは、紛争期間が短すぎる場合です。  
これは少なすぎます。  
 5年のほうが賢明かもしれませんが、地元の議会にそのような法律を通過させることができると思うなら、幸運を祈ります。  
静けさの実際的な解決策は、通常、冷却期間です。ある石油会社で働いていた場合、別の会社で2年間働くことは禁じられている可能性があります。セキュリティエンジニアリング348ロスアンダーソン10。  
 概要10。  
 これは、密猟の危険にさらされている野生生物に関するデータや国の情報データの保護から、医療情報やソーシャルケア情報のプライバシーや機密性、一般的な専門的業務に至るまで、多くの情報セキュリティ問題の問題です。  
 このようなシステムは、既存の作業慣行を自動化することによって設計でき、役割ベースのアクセス制御は、それらを実装するための自然な方法です。  
 プライバシーへの従来のアプローチは、「同意または匿名」として要約される場合があり、医師（患者はもちろんのこと）に対してさえ不透明であることが多い多くの外部委託システムの複雑さの増大によって損なわれています。  
 ここでも、ガバナンスの問題は技術的な問題よりも扱いにくいものです。  
 ヨーロッパは、市民に個人の健康情報を直接事件に関係する臨床医に制限する権利を与えます。アメリカはそうではありません。  
 アメリカとヨーロッパの両方は、麻薬会社やすべてのデータを必要とする他の人からの巨大なロビーと金銭的なプレッシャーを持っています。政治家は業界に寄り添い、規制当局を弱体化させる傾向があります。  
 野生生物犯罪との闘いのように、これが完全な出発点ではないいくつかのアプリケーションがあります。そこでは、集計データは密猟者にとって、個々の目撃よりもさらに価値があります。  
 これについては、次の章で説明します。マルチレベルのセキュリティが情報セキュリティへの「ヘッジホッグ」アプローチであったのと同じように、1つの大きなことを正しく行うだけで良い結果が得られることを望んでいるのと同じように、多国間セキュリティには「フォックス」アプローチが必要です。過去に何がうまくいかなかったのか–また、将来何がうまくいかないかを予測したい場合は、敵対的思考にも長けている。  
5。  
 それには何が必要で、技術的および政策的メカニズムはどのように進化して対処する必要がありますか？また、近い将来、ますます多くの医療が遺伝情報を含むようになります。  
 あなたの親戚には知る権利があり、他の人に言うかもしれません–したがって、歓迎されないニュースが間接的にあなたに届くかもしれません。  
 情報の権利をめぐるこうした緊張は、インターネットよりも古くからあり、純粋に技術的なメカニズムによって管理することはできません。  
 長期的な解決策には、法律、社会規範、技術サポートのいくつかの組み合わせが含まれる場合があります。しかし、彼らは解決するのに何年もかかる可能性が高く、異なる文化で異なる​​ソリューションになってしまう可能性が高いです。  
 他の場所でその態度が変わる可能性はありますか？さらに読むコンパートメントモードのセキュリティに関する文献は散在しています。パブリックドメインの論文のほとんどはNCSC / NISSCとACSACの会議の議事録にありますが、Amoroso [47]とGollmann [779]はラティスとチャイニーズウォールモデルの基礎。  
 NHS ITの全国プログラムのケーススタディについては、[379]を参照してください。英国議会の公会計委員会による総コストに関する後のレポートについては、[1559]を参照してください。  
 アメリカの医療プライバシーに関する全米研究評議会の調査については、[1412]を参照してください。 [1191]には、研究における匿名化されたデータの使用に関するHHSレポートもあります。  
セキュリティエンジニアリング350ロスアンダーソン