彼らは常に外から内の闇から逃げようとします。システムを夢見て、誰もが良い人である必要はないほど完璧なシステムを夢見ています。  
それを乗り越えなさい。  
  
10.1はじめに  
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、国家情報機関とは異なり、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、スタッフが有名人のデータを調べるスキャンダルが発生します。  
4。  
データの共有が頻繁に求められますが、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も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、その他の関係者が関与する連合の取り組みでなければなりません。 3。  
システムが複雑になり、そのオペレーターが努力をするインセンティブを欠いているため、どちらも実装がより困難になっています。 4。  
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際の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、動的ですか？  
 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？  
一部の問題は技術的には複雑ですが、ポリシーの観点からは単純です（野生生物）  
。  
スタッフは過去に、有名人の記録への不適切なアクセスを行い、部外者にデータを販売し、慰謝料のケースで収入の詳細を漏らしていたことがある[188]。  
 TOP SECRET SECRET CONFIDENTIAL OPEN図9.1 –マルチレベルのセキュリティ要件は、厳格な管理を除き、スタッフが別の地理的地域または別の業界に属する税務記録を見ないようにすることです。  
A B C D E共有データ図9.2 –多国間セキュリティ横方向の情報フロー管理は組織化されている場合があります。これは、情報機関が、ある外国で働いているエージェントの名前を、別のスパイの責任を負う部門から秘密にしている場合です。  
これらは、患者の機密性が法律で患者の権利に基づいているが、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医療の場合のように、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、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すべて知っています。  
  
米国とその同盟国は、コードワードと分類による秘密情報へのアクセスを制限しています。  
エニグマが壊れていたという事実は、ほとんどどんな犠牲を払っても保護する価値がありました。  
これまでにウルトラクリアランスを保持したことのある人が捕獲される危険にさらされることはありません。そして、その知性は、ヒトラーに彼の主要な暗号が破られたと疑わせるような方法で決して使用することができませんでした。  
このポリシーは、特別な処理規則によって実施されました。たとえば、チャーチルはウルトラの概要を特別な発送用の箱に入れましたが、鍵は持っていましたが、スタッフは持っていませんでした。  
 ほぼ同じ予防策が今日実施されています。  
分類と一連のコードワードは、コンパートメントまたはセキュリティコンテキストを提供します。  
この警告は、一連の悲惨な内部関係者の脅威に対する反応でした。  
KGBの海外での活動も同様に、共産主義に幻滅し、年金を待つ間アーカイブで働くために派遣された士官であるヴァシリーミトロキンによって危うくされた[118]。  
そこでは、海軍艦艇をコンパートメントに保管する試みはうまくいかなかった。船は予告なしにどこにでも送られる可能性があり、船が現地の鍵となる材料を持たないことは、運用上許容できなかった。誰もがアクセスしすぎないようにしたいのは明らかですが、どうすればそれができますか？  
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。  
。  
次に、「トップシークレット」にクリアされた人は、「トップシークレット」と「シークレット」に分類されたファイルを読むことができますが、クリプトクリアランスがない限り、「シークレットクリプト」に分類されたファイルにはアクセスできません。  
偶然にも、Bell-LaPadulaモデルはほぼ変更なく機能します。  
 （TOP SECRET、{CRYPTO}）  
 （秘密の、 {}）  
 （秘密、{暗号、外国}）  
 図10.3：–セキュリティラベルの格子前と同じように、HighとLowの間に情報フローがありますが、HighはLowを支配するコンパートメントです。  
実際、ラティスモデルとBell-LaPadulaモデルは基本的に同等であり、並行して開発されました。  
完全な歴史については、この本の第2版を参照してください。  
このようなシステムを使用して、さまざまなコンパートメントにデータを分けておくのは簡単です。互換性のないラベル（「Secret Tulip」、「Secret Daffodil」、「Secret Crocus」など）を付けるだけです。  
しかし、現在、オペレーティングシステムは共有メカニズムではなく、分離メカニズムになっています。また、インテリジェンスシステムのユーザーが直面している実際の問題は、異なるコンパートメントのデータを組み合わせ、サニタイズ後にダウングレードすることと関係があります。  
9/11以降、アメリカの諜報機関には大きな変化がありました。  
NSAのディレクターであるキースアレクサンダーが「すべてを収集」しようとする動きがあり、データ収集を最小化して最大化してすべてを検索可能にするのではなく、  
Top Secretの上にあるものは、主に随意アクセス制御を使用して管理されているようです。  
多くのコードワードが添付された検索結果が表示される可能性がある場合、その結果を読み取るには、それらすべてのクリアランスが必要になります。  
 おそらく、米国の諜報機関は、失敗モードが代わりにエドスノーデンであったことを幸運でした。  
その後、CIAでもコンパートメント化が必ずしも効果的では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がコンパートメント化されておらず、ユーザーがsysadminパスワードを共有していること、ユーザーアクティビティの監視が行われていないこと、履歴データが無期限に利用可能であることが明らかになりました。  
実際、世界的な共同インテルコミュニケーションシステム（JWICS）  
NSAが利用できる暗号化システムの詳細や方法など、エドスノーデンが到達できなかったいくつかのコンパートメントがあります。これは「非常にコンパートメント化された情報」（ECI）とマークされていました  
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編集しています。  
  
野生生物犯罪との闘いにかかわる人々は、さまざまな興味深い問題に直面しています。  
ギャングは不満を抱くコミュニティによって保護されるかもしれません。環境法を弱体化したり、密猟集団を保護したりする場合でも、政府の首長でさえ脅威になる可能性があります。  
ソブリンの脅威が存在しない場合でも、公共部門の擁護者はしばしば相互に疑わしい政府のために働きます。ユキヒョウを密猟者から保護するには、インド、パキスタン、中国、ネパール、タジキスタンのレンジャーが関与し、東アフリカでの違法な象牙取引は、ケニアから南アフリカまで国境を越えて流出します。  
したがって、その軍事的、内部脅威、および政治的側面は、多くの点で従来の安全保障および諜報活動と似ています。  
分類、クリアランス、対諜報活動を管理する中央官僚機構はありません。  
彼女のアイデアは、個々の野生動物の撮影した多くの写真をリンクできれば、それらに依存する資源管理、生物多様性、および保全の決定とともに、生態学および個体群生物学の科学を劇的に改善できるというものでした。  
Wildbookは現在、ダース以上の場所でダース以上の種に展開されています。  
彼らはウェブサイトを通じてこれらの植物を販売し、多数の収集旅行を行い、植物のリストサーブとソーシャルネットワークを介して珍しい標本を発見したことが判明しました。  
彼らはまた、別の市民科学のWebサイトであるiSpot [2009]も使用していることがわかりました。では、ポリシーはどうあるべきでしょうか？  
珍しい植物では、泥棒が1つの標本でもGPSの位置を知ることを望まない。  
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。  
アフリカでも同様です。 Wildbookは、シマウマを追跡することから始まりましたが、そのうちGr´evyのシマウマは絶滅の危機に瀕しています。  
タグ付けをオフにする方法がわからない観光客もいます。馬鹿げている人もいて、車から降りて食べられます。  
新しい野生生物の集合場所では、画像認識を使用して個々の動物を識別し、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、動物のプライバシーが人間の多様性と異なる点の1つです。高度に抽象化されたデータは、多くの場合、機密ではなく機密性が高くなります。  
そのような個人がダークサイドに行く場合、最高の密猟者を作るので、私たちは密猟者の手から彼ら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の動物は時間Tの場所Xにいる可能性が高い」など、野生生物の犯罪者に実用的な情報を与えないことです。  
まず、（a）のアクセスルールを導き出すためのガイドとして、運用研究モデルを使用します。  
 予測モデルと（c）  
種や場所によってルールを微調整できる必要があります。  
中核となるWildbookチームはソフトウェアを保守し、ほとんどすべてに操作上のアクセス権を持っています。このレベルをゼロと呼ぶかもしれません。  
レベル2では、何百人もの人々が保守のためにデータを収集および提供しており、現在、Wildbookにはある程度知られています。システムが拡大するにつれて、委任された管理に対処する必要があります。  
私たちの脅威モデルでは、レベル3の市民科学者のセットには常に密猟者が含まれます。レベル2の保守管理スタッフのセットには、不注意または不忠実な少数派が含まれます。また、レベル1の管理者が密猟者との密談をしないようにしてください。  
保守主義はしばしば弱い州で活動していることを考えると、最終的な検出と投獄の脅威は遠く離れているように見えます。  
タスクは、グループの結束と忠誠心をサポートする技術的手段を見つけることです。  
 条件。  
すでに種ごと、場所ごとに管理者がいます。  
私たちの中心的な戦略は、2次元の透明性に基づく、状況認識と抑止のための地方公的監査能力です。  
したがって、サイグループのスタッフは、サイの記録（個々の目撃記録やモデルなど）を誰が見ていたかを確認し、セレンゲティで作業しているスタッフは、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、他の保守団体とピアリング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。  
  
おそらく、アクセス制御がプライバシーをサポートするセキュリティポリシーの最も複雑で有益な例は、臨床情報システムにあります。  
したがって、医療情報の保護は、豊富で複雑な多くのトレードオフを伴う、私たち全員にとって重要なケーススタディです。  
米国では、健康保険の相互運用性と説明責任に関する法律（HIPAA）  
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術者として働いていた有罪判決を受けた児童レイプ犯が、元従業員のパスワードを使用して、954人の患者（ほとんどは若い女性）の記録を調べて逮捕されました  
彼は結局刑務所の時間を過ごし、マサチューセッツ州上院議員エドワードケネディはHIPAAのスポンサーの1人でした。  
2000年12月にクリントン政権によって発行された最初のセットは、適度に堅牢であり、プライバシーの懸念のために時間内に治療を求めることを恐れすぎた人々に与えられた害の評価に基づいていました。  
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]。、違反に対する民事上および刑事上の両方の罰則（最初の数年間に課された罰はほとんどありませんが）  
この規則はまた、患者に記録のコピーを要求する権利を与えました。  
プライバシー規則に続き、2006年には医療システムの相互運用性を促進するための「管理上の簡素化」規則が続きました。  
しかし、不平は続きます。  
HIPAA規制はヨーロッパよりもプライバシーがはるかに低くなっていますが、米国の10％以上を占める医療における情報セキュリティの主な推進力です。  
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性によってシステムがある程度推進され、2019年にはEpicが電子カルテシステムで29％の市場シェアを獲得し、市場も集中しています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。  
BMAは私に、臨床情報の安全性とプライバシーに関する方針を考案するように依頼しました。これについては、この章の後半で説明します。  
医療情報に関連する安全性とプライバシーのトレードオフについての議論は、この頃ヨーロッパの他の国でも始まりました。  
有名人に関する情報を得るために初期の集中型システムが使用された一連のスキャンダルがありました。  
同意と記録へのアクセスに関するヨーロッパの法律は、フィンランドの場合、2010年に欧州人権裁判所により明確化されました。  
彼女の病状は同僚の間で広がり、彼女の契約は更新されなかった。  
裁判所の見解では、患者のケアに関与していないヘルスケアスタッフは、その患者の電子カルテにアクセスできないようにする必要があります。「この接続で必要なのは、最初の場所です。」この判断は2010年に確定し、それ以降、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になっています。  
10.4.1脅威モデル  
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、特に安全性の障害は、交通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義務付けるFDAをもたらす可能性があります。  
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、大統領クリントン政権下でのHIPAAの規則策定の前に、米国保健社会福祉省によって収集されました。  
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。  
これは、退役軍人の自殺率が同等の民間人の自殺率の約2倍であると考えられています-機密扱いへのアクセスが大きな障壁となっています[1861]。 3。  
匿名のHIV検査により、同性愛者の検査率は2倍以上になりました[1650]。  
プライバシーの主な脅威は、過失と悪意が混在する内部関係者によるもので、およそ3つのカテゴリに分類されます。1。  
これらは個人に直接害を及ぼします。 2。  
報告された違反のほとんどは事故です。たとえば、医師がノートパソコンを電車の中に置いたままにしたり、誤って構成されたクラウドサーバーが何百万もの人々の記録をオンラインに残したりします[767]。  
偶発的なリークが日和見攻撃につながることもあります。  
大量攻撃はまた、多くの人々の正義感を傷つけ、自治と主体性を侵害し、システムへの信頼を損ないます。  
 そして、リスクのどれくらいがテクノロジーによるものですか？  
リソースが悪用される可能性は、その価値とリソースにアクセスできる人数に依存します。  
過去25年間、私たちは、各医師の受付担当者がペーパーライブラリまたは診療用PCで5,000の患者の記録にアクセスできる世界から、何千もの医療行為の記録がホストされている世界に移動しました共通プラットフォーム。人々が救急医療、請求、研究をサポートするための集中型システムを構築し始めて以来、これはすでに懸念事項でしたが、それが現実のものとなりました。  
また、プライバシーの問題は、患者を直接治療する組織に限定されるものではありません。個人の健康情報の最大のコレクションのいくつかは、医療保険会社や研究組織の手に渡っています。  
すべてのスタッフがすべての記録にアクセスできるようにした初期の病院システムは、多くのプライバシーインシデントを引き起こしました。その中で最も注目すべきものは、欧州裁判所のフィンランドに対する判決につながったものです。しかし、英国では1990年代半ばにさかのぼる同様の事件がありました。  
  
1995年までに、ほとんどの医療行為には記録を保存するためのコンピューターシステムがありました。サプライヤーは、ゴルフやヨットではなくコンピューティングを趣味とする医師によって開始された小規模な会社であり、医師の実際のニーズに合わせて調整されていました。  
英国からの医療の約90％を国民健康保険を通じて支払う政府からの圧力がありました。当局は、もしすべての情報にアクセスできれば物事をより良く管理できると信じており、これは専門家の自治を気遣う医師との緊張を引き起こした。  
そこで保健省は、すべての医療記録を一元化したいと発表しました。  
BMAは個人の健康情報をネットワーク上で暗号化する必要があるかどうか尋ねましたが、政府はこれを考慮することさえ拒否しました（暗号戦争が進行中です;その話については26.2.7.3を参照してください）  
これが最後のストローでした。 BMAは、専門家を雇うほうがよいことに気付き、セキュリティポリシーについて教えてください。  
私たちは急速に問題にぶつかった。  
 これは、異なる病院や診療所で同じ患者に関する異なる記録を持ち、紹介状や退院式の形で情報を流すという従来のシステムではなく、患者を妊娠から剖検まで追跡することになります。  
さまざまな人々が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母親の記録の一部でもあり、軍または刑務所にいる間の記録は政府に属している可能性があり、性感染症の治療を受けると、あなたはそれを完全に非公開にする権利を有する場合があります。  
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。  
 これは処方箋であるため、制限する必要があります。しかし、人をHIV陽性と特定するため、秘密にする必要があります。  
感度は首相ではなく患者が決める問題です。  
医療関係者と私は、生涯の記録よりも細かいセキュリティコンテキストが必要であることを理解したので、既存の法律と実務に粒度を設定させ、その上でポリシーを構築することにしました。  
したがって、患者には通常複数のレコードがあり、これはEPRの擁護者を怒らせます。  
昔は、これは研究者や臨床監査人が病院や診療所の図書館に座って辛抱強く統計を収集することを意味していました。同意は、待合室で次のような通知を行うことで構成されています。記録をこのように使用したくない場合は、医師にご相談ください。」1995年までに、一般開業医（GP）に補助コンピュータを提供している会社が1社見られました。  
したがって、BMAセキュリティポリシーの目的は、同意の原則を適用し、あまりに多くの人々があまりにも多くのレコードにアクセスできないようにすることでした。  
これらの原則と洞察から始めて、私たちは9つの原則の方針を提案しました。  
アクセス制御：識別可能な各臨床記録には、それを読んでそれにデータを追加する可能性のある人々を示すアクセス制御リストでマークを付けるものとします。  
レコードを開く：臨床医は自分でレコードを開くことができ、患者1BritainのGPは米国のかかりつけの医師と同等です。彼らは歴史的にシステムへの門番として、そして各患者の生涯の医療記録の管理者として行動してきました。  
これにより、米国と比較して、英国では医療費を抑えることができます。患者が紹介された場合、彼女は自分自身、患者、紹介する臨床医と一緒に記録を開くことができます。  
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することしかできません。  
同意と通知：担当の臨床医は、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。  
実際には、患者よりもコンパートメントが多いため、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記録へのアクセスなど、より多くの問題に対処しました[58]。  
。  
 1996年に発表され、政策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。  
10.4.3最初の実用的なステップ  
病院規模でアクセス制御を行う実際的な方法は、「病棟の看護師は過去90日以内に病棟にいたすべての患者の記録を見ることができる」、「主治医は彼女の部門で治療されたすべての患者の記録」、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、彼女が彼女の部門で治療されたことのない患者の記録にアクセスする場合、主治医その患者のケアに責任があることが通知されます。  
後から考えると、BMAモデルは医師が言ったことの無損失圧縮でしたが、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、病院が実際に行うことを実装し、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ことはできましたが、信頼できる有用なサブセットはありませんでした。  
 どの患者、どの看護師がどの病棟にいるのかを伝えます。  
次のイテレーションは、各病院スタッフに、各部署または病棟の資格情報を含むスマートカードを提供することでした。  
彼女は、NHS内で確立された約60の情報フローが違法であることを認め、各ヘルスケア組織の責任あるプライバシー担当者の任命を推奨しました[367]。  
とにかく、政府が変わり、トニーブレア政権の新政権は技術的な修正ではなく法的な修正を行いました。データ保護法により、データ管理者はデータを再識別できない限り匿名であると偽ることができました。 、たとえ他のデータと照合することで他の人がそれらを再識別できる場合でも。  
  
トニーブレア首相としての2期目として、英国の医療サービスコンピューティングを近代化するための60億ポンドの計画を発表しました。  
知られているように、世界で最も高価な2The Hastingsシステムは、当初BMAプロジェクトとは別に設計されました。  
3英国の法律は、EUデータ保護指令（95/46 / EC）を置き換えることになっています  
EUは最終的に、より厳しい一般データ保護規則（2016/679）を推進しました  
民間IT災害。  
キャメロンはプロジェクトを正式に中止しましたが、サプライヤーとの契約が定着したため、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。  
患者データにアクセスするには、スタッフメンバーも正当な関係を持っている必要があります。  
3。  
ただし、プロバイダーはこれを実装するためにラウンドを決してしませんでした。  
遅くとも2007年に、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。受付係が知ったのは、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だった。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、実際にこれらのシステムをインストールしたイングランドの病院は10％未満でしたが、「RBAC +関係」の教義が他の組織に影響を与えています。  
  
次に問題になるのは、緊急医療記録です。  
これは、そして今も変わらず、偽物でした。  
しかし、ポリシーはポリシーであり、スコットランドでは、政府が処方箋とアレルギーの「緊急医療記録」を作成し、緊急データベースの臨床医、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できるように中央データベースに保管しています。 。  
訴訟は最終的に「公益ではない」として起訴され、[1741]。  
オプトアウトしても、データは引き続きGPから収集され、保健省が利用できるようになりました。彼らは救急隊員と共有されなかっただけです。  
すべての人の記録はオンラインになり、医師は患者が同意したと主張した場合にのみそれらを見ることができます。  
英語の緊急システム、Summary Care Record（SCR）  
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]。  
10.4.4.2回復力  
NPfITの唯一の真の成果は、デジタルマシンとクラウドストレージを使用してイギリスのすべてのX線イメージングを標準化することでした。  
石油会社は後に、安全違反のために数百万ポンドを調達しました。  
2017年に近くの別の病院でWannacryワームがマシンに感染したときに、さらに警告が出されました。マネージャーは、さらなる感染を防ぐために愚かにネットワークを閉鎖し、緊急治療室を閉鎖して患者を別の場所に送らなければならないことに気付きました。  
。  
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、それを計画担当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。  
  
支払いに関連するデータベースは通常、実際のオプトアウトを許可していません。英国の例は病院エピソード統計（HES）です。  
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への強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判明しました。  
Cameronは、以前はヘルスITビジネスを経営していた「透明性の高い皇帝」を雇い、英国を製薬研究の世界的リーダーにするために、すべてのNHS患者が研究患者になることを目標とする「オープンデータメジャー」を2011年に発表しました。  
匿名化とは、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。  
これは十分な不穏を引き起こし、プライバシーキャンペーン活動家、GP、その他が集まり、医療プライバシーキャンペーングループmedConfidential.orgを立ち上げました。  
運動家たちは政府に同意を得て新たに明確化されたヨーロッパの法律に従うように要求した。政府はくねくねと回避しました。  
 2014年1月、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、その他に販売されていたことが明らかになりました-多くの場合、1998年に遡る10億回のエピソードを含むDVDのセットの形で。  
この「care.data」スキャンダルは、すべてのGPデータを収集するという提案の後に知られるようになったため、主流になりました。  
検査の結果、郵便番号と生年月日がデータセットに含まれていなくても、患者を簡単に特定できることがわかりました。技術的な詳細については、次の章で説明します。  
現在、「NHSデジタルプロトコルに準拠した厳密な統計的開示管理を、公開されているすべてのHESデータに適用しています。  
https://digital.nhs.uk/data-and-information/data-tools-and-services/ data-services / hospital-episode-statisticsを参照してください。  
管轄権の問題もありました。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、クライアントに再販したためです。20GbではExcelには大きすぎるためです。  
 Googleには英国にデータセンターがありませんでした。NHSデータを海外に持ち出すことに対するあらゆる種類の規制があります[1573]。6、個人データを販売していた[1645]。  
閣僚は学んだ教訓について話し、すべてのデータリリースのレビューが委託された。しかし、これが現れたとき、それは彼らが合法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]。  
。  
情報コミッショナーは病院を懲戒処分にしたが、Google Deepmindにデータの削除を命じることに失敗した。  
•2015年にも、タブロイド紙がオンライン薬局Pharmacy2U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、体調不良の高齢男性を対象とした宝くじ詐欺師や、誤解を招くためにすでに認可されているヘルスケアサプリメントベンダーを含みます。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EMISである主要な後援者が、その持ち株を売却しました。  
•2017年、2,700人のGPプラクティスを含む6,000人の顧客を擁する大手GPソフトウェアサプライヤーTPP –イングランドの全プラクティスの3分の1、2,600万人の患者の記録–は、ローカルの医師が記録を見ることができるように「拡張データ共有」をオン病院。  
記録も6に表示されました。  
介護施設、刑務所、入国管理センターのTPP顧客。  
•2018年、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は、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公衆衛生イングランドから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ネットワークを病院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、テキサスやフロリダ、またはミネソタでさえも難民となったルイジアナ出身の退役軍人は、直接地元のVA病院に行き、医師の指先でメモを見つけることができました。オーリンズはメモを完全に失った。  
2019年11月に、Googleがアセンションに代わって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が明らかになり、内部告発者はデータが明確に特定されていないことさえ明らかにしました。グーグルとアセンション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が米国を統治すると、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、「研究」に対する便利な免除規定があり、製薬業界のロビーによってそこに定められています。これは、市場調査を除外していません。  
これは、1990年代にアヘン剤の処方記録の収集から始まり、大幅に拡大しました。  
10.4.5守秘義務–将来  
 ええと、いくつかは変化しますが、驚くほど多くのものが同じままです。  
クラウドベースの医療記録への移行は、個々の医療提供者がサーバーとバックアップを維持する手間と費用を節約できるため、抵抗するのが困難です。  
2014年以降、Fast Healthcare Interoperability Resources（FHIR、発音は「火災」）の標準草案が登場しました。  
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OAuth 2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、データ交換を承認した後、プロバイダーがAppleのHealth Recordなどのサードパーティのアプリにレコードを送信するように要求される場合があります。  
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か、まったく共有しなければなりません。全期間の記録よりもきめの細かいアクセス制御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推進力を持ち、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契約を結んだことが発表されました。彼らは株式の見返りとして500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。確かにデータによると、約80％の人が医師の健康データを信頼していますが、これは医療保険会社と薬局では50％強、研究者では約40％、製薬会社では20％、技術では10％にまで下がります[1100] 。  
 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、患者の同意が必要です。  
2。  
誤って説明されたり、まったく言及されなかったりする二次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、患者に真実が伝えられる適切なセキュリティメカニズムがなければなりません。  
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る場合、たとえ実際に数十万人が監査を行ったとしても、これは虐待の大部分を抑止するはずです。  
英国では、NPfITでの10年間と、そうではないふりをしながらデータを販売しようとする10年間で、20年間を無駄にしてきました。  
同意した他の患者から収集された100,000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、公式統計のように年齢や性別だけでなく、社会的剥奪、人種、喫煙歴、ボディマス指数、特定の併存症によって死亡率を分析し、1700万以上の危険因子を確立しました2020年2月から4月にかけての患者数と6,000人を超える死者数[2025]。  
。  
そして、これは「新しい」研究手法と見なされるかもしれませんが、クラウドベースの医療記録の出現によって可能になりましたが、実際には非常に古い手法です。  
  
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月にかけてビルケナウで双子の実験を行った同僚のヨセフメンゲレ博士と同様に、同意なしに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。  
•英国のアルダーヘイスキャンダルで、マスコミは、病理学者がいかなる種類の同意もなく、生死の患者から「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。  
これは公衆の信頼に深刻な損害を与え、その結果、英国の病理学の研究が損なわれた。  
ナチスの医師の裁判は1948年にニュルンベルク法に至りました。  
これは後に1964年に医学研究の倫理に関するヘルシンキ宣言につながり、1975年にタスキーギの後に独立した組織審査委員会または倫理委員会の必要性を組み込むために改訂され、その後1983、1989、1996、2000、および2008年に改訂されました。  
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。  
 そして、市民や医療サービスがそれらを買う余裕がないならば、発展途上国で薬物をテストすることは倫理的でしたか？  
 そして、ヒトゲノムの低コストの配列決定から生じる倫理的問題は何ですか？  
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（他者の利益を保護することを含む）における個々の市民のプライバシーを妨害する国家および他者の権限に対する制限が含まれます  
3。  
 データイニシアチブにおいて、そしてそれらの期待が確実に満たされることを確実にするための適切な措置と手順は、道徳的に関連する関心を持つ人々の参加によって決定されるべきです。  
関連する利害関係を持つすべての人々を関与させることが現実的でない場合（実際にはそうなることがよくあります）、すべての範囲の価値と利害を公平に表す必要があります。  
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アカウンタビリティ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より広く伝えるための効果的な対策が含まれていなければなりません。  
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。  
それ以来、私たちはこのモデルを使用して、さまざまな点で類似しているサイバー犯罪に関する私たち自身の研究を導きました。  
ただし、多くの場合、調査の倫理的なケースを作成できますが、そのような決定を行って記録するプロセスには注意深い検討が必要です。  
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。  
  
同じ問題が教育やソーシャル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れの安全性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月にさらに深刻な政治問題になり、税務当局は英国の子どもの福利厚生データベース全体、つまり子どもを持つ英国のすべての家族の個人情報を含む2枚のDVDを失いました。  
さらに見直した後、児童保護に関わるソーシャルワーカーを編成するための新しい「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ソーシャルケア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。  
」を直接GPシステムに入力します。これは診断として解釈され、残りのすべての糖尿病ケア機構のスケジュールを立て始めます。  
介護サービスと学校との間の自動交換にも問題があります。実際、さまざまなタイプの専門家間の自動化された相互作用は、多くのエッジケースの広範なコンサルティングと調査を考慮して設計する必要があります。  
イギリスでは、教育省は国勢調査のデータを最初に保持していましたが、試験結果、行動、および出席のデータ、子供が無料で学校の食事をとるのに十分な貧困層であるかどうか、そしてケア。  
。  
 彼らの健康を促進し、保護するため。  
 この反対運動は広まり、2016年に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考え出せなかったため、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、子どもの権利のために活動しているNGOが少なくとも1つあります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も、https：//www.defenddigitalme.orgは子供の問題を知らされていないと非難されています。たとえば、Vimeoを使用してWebサイトで教育用ビデオを利用できるようにしている場合、 -13秒。  
 より根本的に、学校は各生徒を市民/顧客（責任があり、管理下にある）、または追跡、スキャン、フィンガープリントが必要な容疑者/再犯者として扱う必要がありますか？  
医療ITの安全性とプライバシー、および教育とソーシャルケアにおけるITの関連主題をめぐる約四半世紀の闘争を振り返ると、政治的ステレオタイプに準拠した失敗が見られます。  
それらは意味がありましたがナイーブです。彼らは官僚的な中央集権と数十億ポンドの契約（一部は任期の前後に大臣を雇った会社との契約）の観点からしか考えられなかった  
2010年以来、保守政権は典型的な右翼的なやり方で失敗しました8。権利と自由について話しているが、皮肉にも製薬会社の友人たちにデータを売り込んでいる。物事がうまくいかなかったとき、狂ったように横たわっていました。規制当局を弱体化させ、リーダーを任命しながら、安全とプライバシーの両方の失敗に目を向けないようにした。  
10.4.7チャイニーズウォール  
投資銀行から会計士までの金融サービス会社は、規制当局から、2つのクライアントが競争相手である場合に利益相反を防止するように設計された内部ルールを設ける必要があり、これらのコントロールはチャイニーズウォールと呼ばれます。クライアントが互いに競争している可能性がある多くのサービス会社があります。広告代理店は別の例です。  
したがって、コピーライターがシェルアカウントで作業すると、一定の期間、別の石油会社のアカウントで作業することはできなくなります。  
また、アクセス制御への職務分離の概念も紹介します。特定のユーザーがトランザクションAまたはトランザクションBを実行できますが、両方は実行できません。  
チャイニーズウォールモデルが安全保障研究コミュニティに魅力を感じている理由の1つは、形式化が容易なことです。実際、ベルラパデュラと同じように表現できます。  
 cの会社とx（c）  
 / 2 x（c0）  
 = y（c0）  
 = ffおよびy（c）  
。  
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。  
 実際には、チャイニーズウォールはまだ手動の方法で実装されています。  
典型的なエントリは次のようになります。9月17日から4月18日：主要な米国の小売銀行の新しい支店会計システムのセキュリティ要件について相談これは唯一のコントロールではありません。  
マイクロレベルのアクセスの問題が残っています。  
 ここで、最新のシステムでは、スタッフがその顧客のセキュリティコンテキストを確立した場合を除き、アクセスを制限する傾向があります。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です。  
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、クーリングオフ期間です。ある石油会社で働いていた場合、別の石油会社で2年間働くことを禁じられる場合があります。  
この章では、システムをスケールアップして大量の機密情報を収集するときに境界を設定する際の問題について検討しました。これらの情報には、多くの人が仕事をするためにアクセスする必要があります。  
私たちは医療記録を詳細に調査しましたが、簡単な問題は、直接的なケアの設定でアクセス制御を設定して、各記録へのアクセスを賢明な数のスタッフに制限することです。  
ただし、ヘルスケアシステムのインセンティブは、実装が不十分であることが多く、コンプライアンスを実施するための規制が必要です。  
。  
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その訴訟に関与する臨床医に制限する権利を与えています。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、製薬会社や私たちのすべてのデータを求めている他の企業からの巨大なロビー活動と金銭的な圧力を受けています。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。  
 研究者が個人のプライバシーを損なうことなく統計調査を行えるようにするため。  
医療記録の場合、コンピュータサイエンティストは、1980年代以降、匿名の豊富なデータは見かけよりもはるかに難しいことを認識しており、近年、これが機能し、いつ機能するかを判断できる強力な理論を取得しています。それはしません。  
別の重要なメッセージはこれです。  
研究の問題コロナウイルスのパンデミックは、健康監視をより広範囲に行き渡らせる可能性が高いので、個人の健康情報がより広くなり、ここで議論された紛争は医療セクターを超えて広がっていきます。  
 また、近い将来、ますます多くの医療が遺伝子情報を必要とするでしょう。  
 たとえば、多くの国では、ハンチントン舞踏病などの遺伝性疾患に対する近親者のDNAテストの結果を知らない権利があります。これは、あなたが持っている確率にも影響する可能性があるためです。  
私が書いているように、ハンティントンのと診断された人々の子供たちの権利を異なる方向に押し進める英国とドイツの裁判所を通過する事件があります[606]。  
しかし、ソーシャルメディアは、スケールファクターを変化させて、より広く、より鋭敏にするようにしています。  
たとえば、東アジアの国々は、より侵入的な監視を容認し、少なくとも今のところパンデミックでの死者ははるかに少ない。参考資料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]はラティスの基本をカバーしています。と中国壁モデル。  
NHS ITの全国プログラムの事例研究については、[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。  
米国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]の研究での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。