情報セキュリティとプライバシーに関するホワイトペーパー

本資料は Information Security and Privacy White Paper (ver.2017.5) を便宜のために日本語翻訳した資料であり、英文の文書との間に齟齬がある場合には英文の内容が優先するものとします。

バージョン ：2017.5
日付 ：2017 年 7 月 27 日
著者 ：Glenn Watt、企業情報セキュリティ責任者 (CISO)
ページ数 ：26

意図的な空白ページ

目次

メディデータの情報セキュリティとプライバシー 4
概要 4
ポリシー 4
役割と責任 4
レポート、認証、および独立機関による証明 5
物理的セキュリティ 5
ネットワーク セキュリティ 5
アプリケーションセキュリティ 5
データ プライバシー 7
認証と運用認可 8
ISO 27001:2013 8
SOC 2 Type 2 8
SOC-1 Type 1 8
FISMA / FedRAMP 9
Privacy Shield 9
FIPS 140-2 9
HIPAA 9
物理的セキュリティ 10
目立たない外観のビル 10
制服警備員 10
顔写真付き ID スマート カード 10
生体認証ドア ロック 10
ビデオ監視 10
ネットワーク セキュリティ 11
ファイアウォール 11
侵入検知と防御 11
情報セキュリティ 12
ウイルス、スパイボット、スパムのスキャン 12
セキュリティ管理 12
データ転送時の暗号化 13
システム管理 14
クラウド セキュリティ 14
ストレージ デバイスの使用停止 15
構成管理 16
セキュリティ パッチとインシデント対応 16
データベース セキュリティ 16
ビジネス継続性とディザスタ リカバリ 17
ビジネス継続性 (BCP) とディザスタ リカバリ (DRP) 17
計画の構成要素 17
ディザスタ リカバリ (DR) 18
ポリシー 18
POL-IS-001 情報セキュリティ 18
POL-CORP-006 企業インシデント管理ポリシー 18
POL-ISP-004 組織のセキュリティ ポリシー 18

POL-IS-005 物理および環境セキュリティ ポリシー **18**
POL-IS-006 資産の分類および管理ポリシー **19**
POL-IS-007 スタッフ メンバーに関する情報セキュリティおよびプライバシー ポリシー **19**
POL-ISP-008 ネットワークおよびコンピュータ運用セキュリティ ポリシー **19**
POL-ISP-009 アクセス制御セキュリティ ポリシー **19**
POL-IS-010 システム開発および保守セキュリティ ポリシー **19**
POL-ISP-011 セキュリティ インシデントと誤動作への対応 **19**
POL-ISP-013 コンプライアンス セキュリティ ポリシー **19**
POL-ISP-014 モバイル デバイスのセキュリティ ポリシー **20**
Patient Cloud のセキュリティ **20**
Medidata Imaging のセキュリティとプライバシーの管理策 **20**
メディデータ Regulated Content Management (RCM) **22**
よく寄せられる質問 **22**

図

図 1. アプリケーション セキュリティ 6
図 2. アプリケーション セキュリティ 7
図 3. データ センターのセキュリティ 11
図 4. 転送の暗号化 14
図 5. AWS の仮想化 15
図 6. 仮想データベース 16

メディデータの情報セキュリティとプライバシー

メディデータのソリューションは、革新的な臨床クラウドテクノロジーを通じて臨床開発プロセス全体を提供する。最初の試験であれ、複数のフェーズや疾患領域にまたがるエンタープライズソリューションであれ、メディデータの製品スイーツは、重要な臨床開発業務を効率化する。これには、プロトコル開発、治験の計画と管理、治験施設との共同作業、無作為化と治験の供給管理、モニタリング、安全性に関する事象の収集、電子データ収集 (EDC) と管理、高度なレポートとビジネス分析などが含まれる。メディデータは、高可用性、完全性、機密性、信頼性、および柔軟性を備えた臨床クラウドコンピューティングソリューションを提供しており、これによって顧客は広範なアプリケーションにアクセスできる。エンドツーエンドのセキュリティとエンドツーエンドのプライバシーを確保するため、メディデータは、セキュリティのベストプラクティスに従って各種サービスを構築し、適切なセキュリティ機能を提供する。顧客データの機密性、完全性、および可用性を確保することは、信頼と信用を保つことと同じくメディデータにとって最も重要である。

メディデータは、さまざまなホワイトペーパー、レポート、認証、およびサード パーティによる証明を通じ、メディデータのホストされた IT 環境に関する広範な情報を顧客に提供する。この情報は、顧客が使用するメディデータの製品とサービスに関連して実施されている管理策と、独立監査人がこれらの管理策をどのように検証しているかを顧客が理解するのに役立つ。さらに、顧客の広範囲にわたる IT 環境において管理策が効果的に運用されていることを説明、検証する取り組みにおいても役立つ。

概要

ポリシー

情報セキュリティポリシーは、システム、組織、または他のエンティティ向けに、セキュリティの意味を定義する。メディデータにおいては、情報セキュリティポリシーは、全スタッフの行動に課す制約であると同時に、ドア、ロック、ファイアウォール、スキャナーなどのメカニズムによって潜在的な敵対者に課す制約にも対処します。メディデータは、プログラムを含む外部のシステムや敵対者によるアクセス、および人間によるデータへのアクセスを制限する。セキュリティポリシーの完全性を保証するため、メディデータは、ベースラインとして ISO 27001 アーキテクチャに従い、定評ある他のセキュリティ アーキテクチャの各種要素によってこれを補足する。

役割と責任

メディデータは、SaaS (Software as a Service) リソースの管理のため、業務ニーズに基づいて職務を明確に分掌している。以下に、代表的なリソースグループと、それらが責任を持つタスクの一覧を示す。

1. 技術 ： 技術部門の Executive Vice President および最高技術責任者 (CTO: Chief Technology Officer) が、メディデータ アプリケーションの技術的運用の執行マネージャである。その管理の範囲には、開発、運用、および情報セキュリティが含まれる。このポジションは、アーキテクチャ、エンジニアリング、テスト、および実装から保守までのアプリケーション管理を監督する。CTO は、クライアントの技術レビュー、事前評価、および監査要求への確実な対応にも責任を持つ。
2. DevOps： このチームは、メディデータ アプリケーションの継続動作の保証を専門に担当する個人で構成される。
3. Service Delivery：Service Delivery チームは、メディデータ アプリケーションをサポートするための、ハードウェア、ソフトウェア、およびインフラストラクチャに関連するすべての活動のインストール、構成、変更、および保守を担当する個人で構成される。
4. ネットワークオペレーションセンター (NOC)： このシステム監視グループは、アラートの設定、維持、監視を担当し、メディデータのアプリケーションとインフラストラクチャの稼働時間と正常性を確保する上で、重要なアラート通知を担当する。
5. 情報セキュリティ ： このグループは、Vice President Information Securit と企業情報セキュリティ責任者 (CISO: Chief Information Security Officer) が統括し、技術環境のセキュリティ、拡張性、および安定性が維持されるよう、

広く受け入れられている標準、規制、およびフレームワークに則したポリシーの管理と、それらの管理策の実装を担当する。

6. エンタープライズサポート : この Corporate IT チームは、メディデータが日常のビジネス活動を運営、遂行できるようエンタープライズ IT サービスをサポートする。エンタープライズサポートチームは、最高技術責任者 (CTO) の直属の管理下のチームである。エンタープライズ サポート チームは、顧客向けのメディデータアプリケーションには一切アクセスできない。

レポート、認証、および独立機関による証明

2011 年、メディデータは SSAE 16 プロフェッショナル基準に従い、Service Organization Control 2 (SOC 2) 報告書を正常に完了した。2017 年 4 月には、「Medidata Payments」アプリケーションについて Service Organization Control 1 (SOC 1) 報告書を正常に完了している。当社の米国政府クライアントに対しては、2009 年に初期の FISMA の認証および運用認可を完了している。プライバシーに懸念のある米国以外のクライアントに対しては、2011 年に米国商務省より、セーフハーバープログラムへの参加許可を取得している。このプログラムは、当社が提供する保護が欧州連合 (EU 95/46) で求められる保護と同等であることを証明するものである。さらに 2016 年 11 月には、Privacy Shield プログラムに対するメディデータの自己認証が米国商務省によって承認されている。メディデータは、2016 年 10 月に ISO 27001:2013 認証も取得している。メディデータは、今後も適切なセキュリティ認証を取得し、当社の製品とサービスのセキュリティを実証するために監査を受ける。

物理的セキュリティ

メディデータは、データセンターの設計、構築、および運用において長年の経験を有している。当社の物理的セキュリティは、ミリタリグレードと言える。メディデータは、ビル警備員、電子アクセス機能付き Smart-ID バッジ、ビデオ監視、および生体認証スキャナーを組み合わせて使用している。当社のビルは目立たない外観で、データ センターの実際の所在地を知っているのは正当な業務ニーズを持つ人物のみである。

ネットワーク セキュリティ

メディデータにおけるネットワーク セキュリティは、24 時間を通じ常に優先事項である。分散型サービス拒否 (DDoS) 攻撃の際にも高可用性を提供するため、ルーターとロードバランサを対象とした境界防御を最優先にしている。境界防御は、業務上の目的が明確ではないすべての受信ポートのほか、送信ポートも拒否するファイアウォールによって強化されている。ファイアウォールを通過する許可データは、一連のマルウェア スキャナーのほか、侵入検知/防御システムで処理される。月 1 回、内部でネットワーク スキャンを実施している。さらに年 1 回、新たなインターネット脆弱性を特定するためにサード パーティによるネットワークの評価を受け、脆弱性が見つかった場合は修正している。

アプリケーションセキュリティ

メディデータのアプリケーションは、当社の成功にとって極めて重要であり、そのアプリケーションが顧客にとって安心、安全であると確認することは最重要課題である。そのため、開発プロセス中にソフトウェアに対して VeraCode© を使用し、さまざまな内部テストを実施している。その後、実稼働製品を対象にした内部ハッキング (ブラックハット) 用の時間を設けている。この段階で、ソースコードを熟知していなければ検出できない細かな問題の発見と修正を試みる。続いて、製品スイーツの相互運用性を評価して次のレベルへと進み、製品の回復力を向上させる。また、サードパーティにソフトウェア評価を依頼し、ライフサイクルのこの段階まで見逃されていた可能性がある脆弱性を特定、修正する。内部テストまたは外部のサードパーティテストで見つかった脆弱性は、メディデータの JIRA™ トラブルチケットシステムに記録される。ここからは、内部のチームが脆弱性を分析、確認した上で、修復日を設定する。アサインされたチームには 90 日のレビューと期限延長猶予期間が与えられる。これを超過した場合、要求は CISO にエスカレートされてレビューを受け、期限の延長が可能かどうかが判断される。90 日後には、さらに延長が必要かどうかを CIO または COO が検討して承認する必要もある。延長が許可されるのは、一般に、ソフトウェアの製造元から修正パッチを入手できない場合や、導入時にさらに大きな問題が発生するのを避けるため、修復に大がかりな開発とテストが必要な場合である。

メディデータアプリケーションのセキュリティ

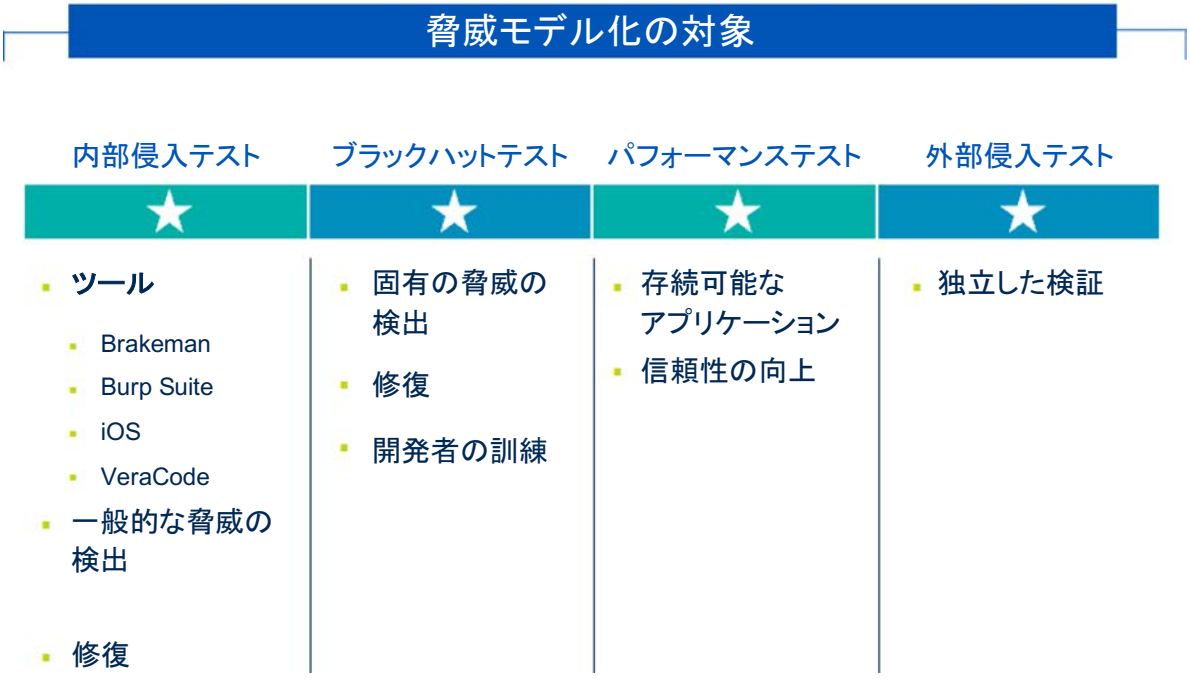


図 1. アプリケーションセキュリティ

データ プライバシー

メディデータは、顧客データのプライバシーを最優先事項として扱う。グローバルな各種プライバシー規制はそれぞれ大きく異なるため、メディデータは、最も厳密な標準に従った保護が最適であるというアプローチを取っている。メディデータは、プライバシー ポリシーを策定し、一般に公開している。また、トランスポート層セキュリティ (TLS) 暗号化を使用して 256 ビットの最小キー長でワークステーションから送信先までデータを保護している。メディデータは、世界各国のプライバシー ポリシーをレビューし、当社の管理策が米国内で転送、保存されるデータに関する最も厳密なポリシーに準拠していることを確認している。管理策の効果を証明するため、メディデータは 2011 年以降 EU - 米国間のセーフ ハーバー プログラムで自己認証済みであり、2016 年にはセーフ ハーバーに代わる Privacy Shield に参加した。

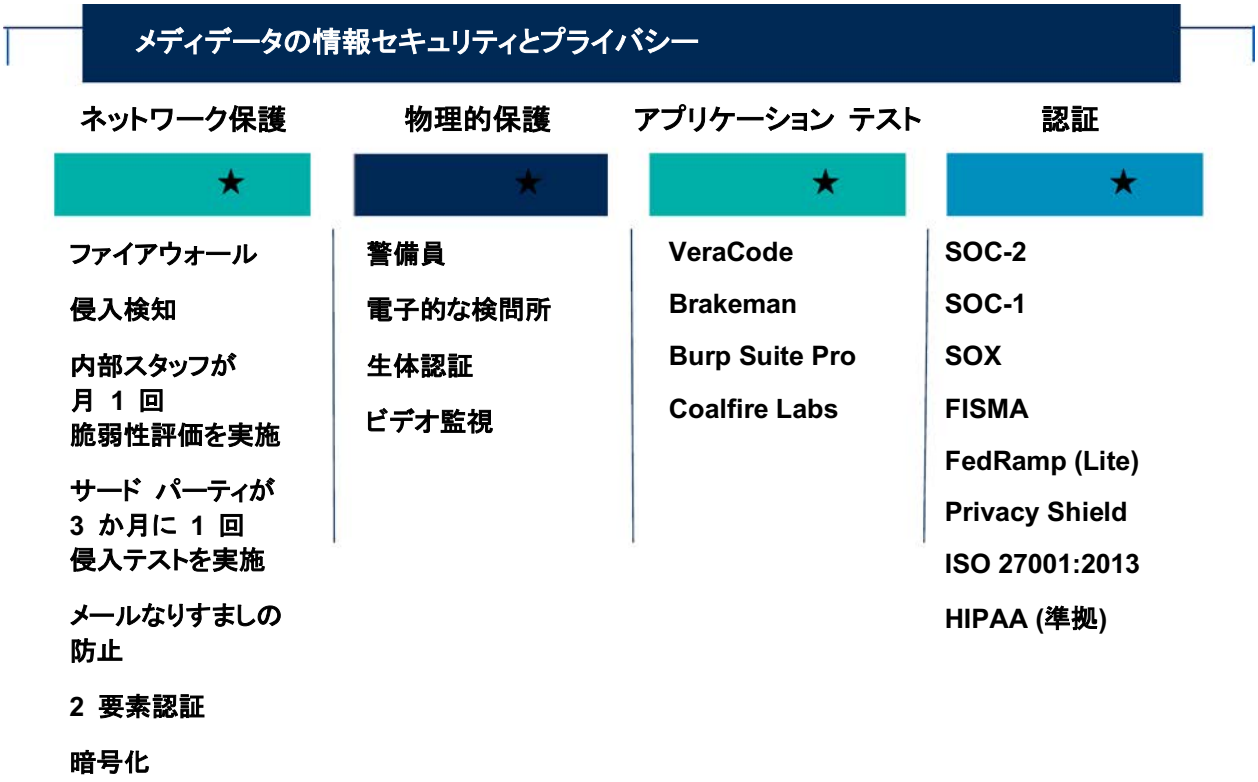


図 2. アプリケーション セキュリティ

認証と運用認可

ISO 27001:2013

ISO 27001:2013 は、ISO 27002 のベストプラクティスガイダンスに従った、セキュリティ管理のベストプラクティスと包括的なセキュリティ管理策を規定する、セキュリティ管理標準である。これは、メディデータの顧客が大きな関心を寄せている、認知度の高い国際的なセキュリティ標準である。この標準の認証では、以下が求められる。

- 企業の脅威と脆弱性の影響を考慮し、情報セキュリティ リスクを体系的に評価する
- 企業とアーキテクチャのセキュリティリスクに対処するため、一連の包括的な情報セキュリティ管理策と、その他の形式のリスク管理を設計、実装する
- 情報セキュリティ管理策が情報セキュリティ ニーズを継続的に満たすようにするため、包括的な管理プロセスを採用する

この標準の認証の鍵となるのは、厳格なセキュリティプログラムの効果的な管理である。この標準で要求される情報セキュリティ管理システム (ISMS) は、メディデータがどのようにしてセキュリティを総体的かつ包括的に継続管理するかを定義する。ISO 27001:2013 認証は、特にメディデータの ISMS に焦点を合わせたもので、当社の内部プロセスがどの程度 ISO 標準に従っているかを測定する。認証とは、独立監査人に認定されたサード パーティがメディデータのプロセスと管理策の評価を実施済みであることを意味し、メディデータが包括的な ISO 27001:2013 認証標準に沿って運営されていることを確認するものである。

SOC 2 Type 2

メディデータは、Service Organization Control 2 (SOC 2) 報告書を発行している。この監査は、米国監査基準書 70 号 (SAS 70) タイプ II 報告書に代わるものである。この報告書の監査は、Statement on Standards for Attestation Engagements No. 16 (SSAE 16) および International Standards for Assurance Engagements No. 3402 (ISAE 3402) の各職業基準に従って実施される。両基準に従ったこの報告書は、米国および国際的な監査機関の幅広い監査要件を満たすことができる。SOC 2 報告書の監査は、メディデータのデータ センターの管理目標が適切に設計されていること、および顧客データを保護するために定義された個々の管理策が効果的に運用されていることを証明する。SOC 2 報告書への取り組みは継続的なものであり、メディデータは定期監査プロセスを継続する予定である。

SOC-1 Type 1

メディデータは、2017 年に初の SOC1 Type 1 報告書を「Medidata Payments」アプリケーションについて発行した。SOC-1 Type 1 報告書は、サービス監査人 (CPA) が Statement on Standards for Attestation Engagements (SSAE) 16 「*Reporting on Controls at a Service Organization*」に従って実施する審査契約で、ユーザー エンティティの財務諸表の監査に関連すると考えられる、サービス組織における管理策の設計の適合性について報告するものである。**SOC 1® 報告書の使用は既存のユーザーエンティティ (潜在顧客ではない) とその監査人に制限される。**

FISMA / FedRAMP

メディデータは、米国政府機関の顧客が Federal Risk and Authorization Management Program (FedRAMP) および連邦情報セキュリティ マネジメント法 (FISMA) への準拠を達成、維持できるようにする。FedRAMP の評価プロセスでは、FISMA に準拠するクラウド製品とサービスのセキュリティ評価、認可、および継続監視の標準的なアプローチが必要である。FISMA では、連邦政府機関はそのデータとインフラストラクチャに関する情報セキュリティシステムを、米国国立標準技術研究所 (NIST) Special Publication 800-53, Revision 4 標準 (FedRAMP による変更) に基づいて開発、文書化、および実装する必要がある。FISMA の認証と運用認可では、メディデータは、一連の広範なセキュリティ構成と管理策を実装し、運用する必要がある。これには、管理の文書化、物理インフラストラクチャと仮想インフラストラクチャの保護に使用する運用プロセスと技術プロセス、確立されたプロセスと管理策の第三者監査などがある。メディデータは、SaaS に関する FISMA の認可を維持するため毎年評価を受けている。

Privacy Shield

EU-U.S. Privacy Shield は、米国企業に対し、欧州人の個人データを保護する強い義務を課すものである。ここには、以前のセーフ ハーバーの枠組みを無効と裁定した欧州司法裁判所の要件が反映されている。Privacy Shield では、米国はより確実な監視と適用、および欧州データ保護機関との協力強化が求められる。ここには初めて、公共企業体によるデータ アクセスに関するコミットメントと保証が文言化されて盛り込まれている。

実際には何を意図しているか?

- メディデータ ソリューションズの場合
  - 年 1 回、要件を満たしていることを自己認証する
  - Web サイトにプライバシーポリシーを表示する
  - あらゆる苦情に迅速に応答する
  - (人事データを扱う場合) 欧州データ保護機関と協力し、その指示に従う
- メディデータ ソリューションズの欧州のクライアントの場合
  - 米国への個人データの転送について透明性を高め、個人データの保護を強化する
  - 苦情が申し立てられた場合、より簡単で安価な救済が可能かどうかを、直接、または該当地域のデータ保護機関の支援により探る

FIPS 140-2

連邦情報処理規格 (FIPS) Publication 140-2 は、機密情報を保護する暗号モジュールのセキュリティ要件を規定した米国政府のセキュリティ標準である。FIPS 140-2 の要件を持つ顧客をサポートするため、メディデータプライベートクラウドの VPN エンドポイントと TL 終端ロードバランサは、メディデータ (米国) 内では FIPS 140-2 承認アルゴリズムを使用して動作する。FIPS-140-2 準拠モードでの動作には、接続のユーザー ブラウザ側にも同等の機能が必要である。メディデータは FIPS 140-2 認定ハードウェアは使用していないが、完全に承認された FIPS 140-2 ソフトウェアと同等の製造元とモデルを使用している。

HIPAA

メディデータは、米国における医療保険の携行性と責任に関する法律 (HIPAA) の対象事業者とその提携企業が、メディデータのセキュアな環境を利用し、保護された健康情報を処理、維持管理、および保管できるようにする。

物理的セキュリティ

目立たない外観のビル

各種システムは、メディデータのコンピュータが収容されていることを示す表示のない、目立たない外観のビルに収納されている。

制服警備員

メディデータがデータ センターとして使用する大半のビルでは、入口に配置された制服警備員が ID バッジをチェックしている。メディデータの敷地への来客はすべて、来客用のネームタグを着用し、メディデータの敷地内では付き添いが必要である。シンシナティの拠点には制服警備員を配置していないが、この拠点のデータ センターはそれほど大きくなく、スタッフが監視可能である。

顔写真付き ID スマート カード

メディデータのデータセンターでは、データベース サーバー ルームにアクセスするために顔写真付き ID カードを使用している。これらの ID カードは、確実な身分証明ツールであると同時に、電子ドア アクセス ロックの操作にも使用する。シンシナティの拠点にあるデータは限定されているため、この拠点では顔写真付き ID バッジによるアクセス方法にアップグレードしていない。

生体認証ドアロック

サーバールームのアクセス ドアの外には生体認証指紋スキャナーが設置されており、サーバールームにアクセスするには、このスキャナーと PIN コードおよび顔写真付き ID スマート カードを組み合わせて使用しなければならない。シンシナティでは生体認証アクセスは使用していない。

ビデオ監視

データセンターに近付く人物はすべて、ビデオ監視システムに記録される。ビデオは永久に保存され、さらにネットワーク オペレーションセンターの熟練スタッフにより、24 時間週 7 日、常時監視されている。

メディデータ データ センターのセキュリティ

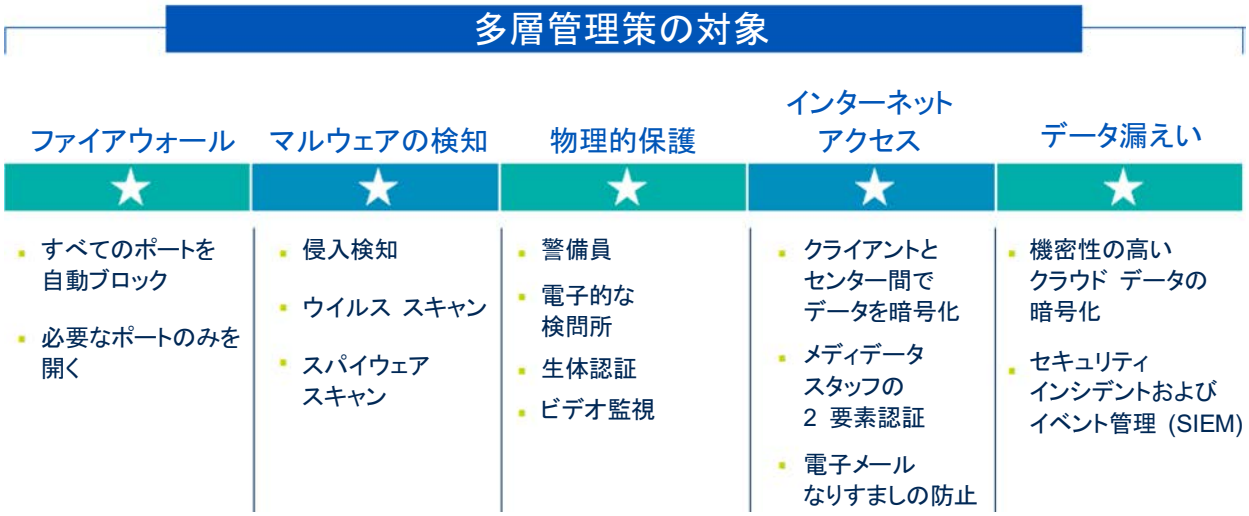


図 3. データ センターのセキュリティ

ネットワーク セキュリティ

Palo Alto Networks PA 5060 ファイアウォール、ウイルス スキャン、および IDP
認証 : [EAL4+、FIPS 140-2、USGV6、UC APL]

ファイアウォール

メディデータは、包括的なファイアウォールソリューションを提供している。受信ファイアウォールは、ポート 80 (HTTP) およびポート 443 (HTTPS) を除き、デフォルトの「すべて拒否」モードで構成される。送信ファイアウォールは、デフォルトの「すべて拒否」モードである。ファイアウォールは、メディデータの変更管理手順に合致するスケジュールに従って提供され、最新の定義で更新される。ファイアウォールは、OSI モデル第 2 層 (データ リンク) ～第 7 層 (アプリケーション) のセキュリティを提供するように構成される。

侵入検知と防御

侵入検知システム (IDS) は、ファイアウォール技術をネットワーク境界に導入した後、メディデータが論理的に取るべき次のステップであった。メディデータの IDS は、外部と内部の両方の攻撃者からの防御を提供し、トラフィックがファイアウォールを越えることは一切ない。メディデータのシステムは、シグネチャ分析のメカニズムを使用し、組織の外部からと考えられる敵意のある攻撃のほか、組織内部からのシステムの悪用や攻撃についても、すべてのトラフィックを分析する。アプリケーションとネットワークトラフィックのシグネチャパターンを照合し、セキュリティの潜在的な弱点を特定する。異常なプロトコルトラフィックの検知により、既知の攻撃とその攻撃の亜種がないかについてネットワーク トラフィックを分析する。ネットワークトラフィックのシグネチャファイルが更新された場合、ベンダーのリリースと同時に自動的に実装される。

情報セキュリティ

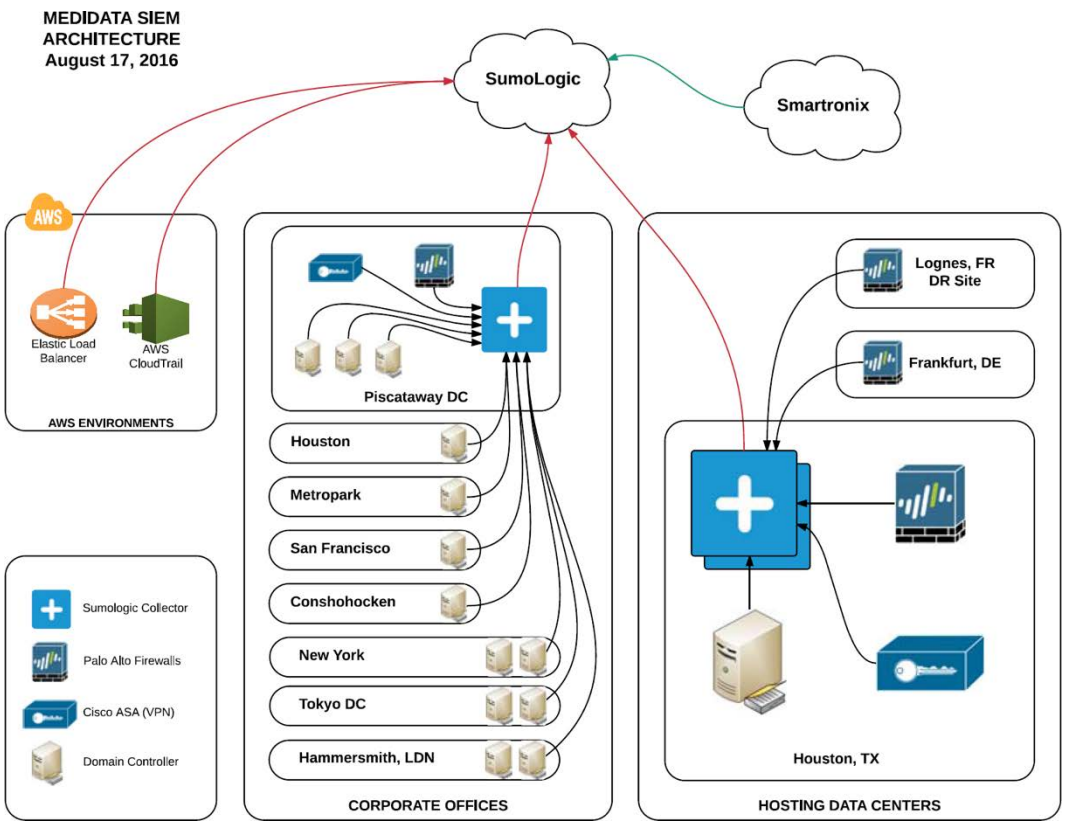
ウイルス、スパイボット、スパムのスキャン

IDS とファイアウォールに加え、メディデータは、広範なスキャン ツールを使用し、データがデータ センターのネットワークを移動する前にすべてのデータをさらにサニタイズしている。これらのスキャン ツールは、何らかの悪意のあるプログラムが防御を突破してシステムへのアクセスを試みた場合に通知を行う。メディデータのネットワーク セキュリティは、「予防は治療に勝る」という古いことわざを指針としている。この場合、ウイルス/スパイボットのスキャンが予防にあたる。

セキュリティ管理

セキュリティ インシデントおよびイベント管理 (SIEM)

- SumoLogic の SIEM システムがすべてのネットワーク デバイスからログとイベントデータを収集し、真にリアルタイムの相関付けと通知を 24 時間週 7 日実行する
- メディデータが自動的に脅威に対処することが可能になる
- NSA、NIST、および SANS の標準に基づく、カスタマイズ可能ですぐに使用できる 120 を超えるチェックを使用してセキュリティ監査を自動化する
- データ漏えいを検出する
- ファイアウォールの構成とログを分析し、冗長および未使用のルールとオブジェクトを分離する
- 実稼働デバイスを変更することなく、新しいルールまたは既存のルールの変更がファイアウォール ポリシーに及ぼす影響をモデル化する
- 数分でインベントリをスキャンして高リスクのファイアウォールを特定し、リスク プロファイルを評価する
- 以下の監査イベントをキャプチャする
    - ログオン (失敗と成功) およびログアウト (成功)
    - 不正なファイル アクセス試行 (失敗)
    - アプリケーションとセッションの開始 (失敗と成功)
    - システムの起動とシャットダウン (失敗と成功)
    - システム管理操作
    - セキュリティ担当者による操作
    - データ転送 (送信元、送信先、時刻、サイズ、および該当 URL の基準値との相関)



ルーター

アクセス制御リスト (ACL) を使用および管理して、Web サーバー、アプリケーション サーバー、およびデータベース サーバーを分離する。サーバー間の通信は、ACL の承認済みアドレスを通じて認証と組み合わせて実行される。

データ転送時の暗号化

すべてのデータはクライアントサイトからインターネット経由で米国本土にあるデータ センターの 1 つに転送される。最高レベルの機密性を維持し、メディデータの Privacy Shield 要件を満たすため、すべてのデータは TLS で 256 ビット以上のキーを利用して暗号化される。必要であれば、FIPS 140 の要件を満たすように転送を構成することもできる。

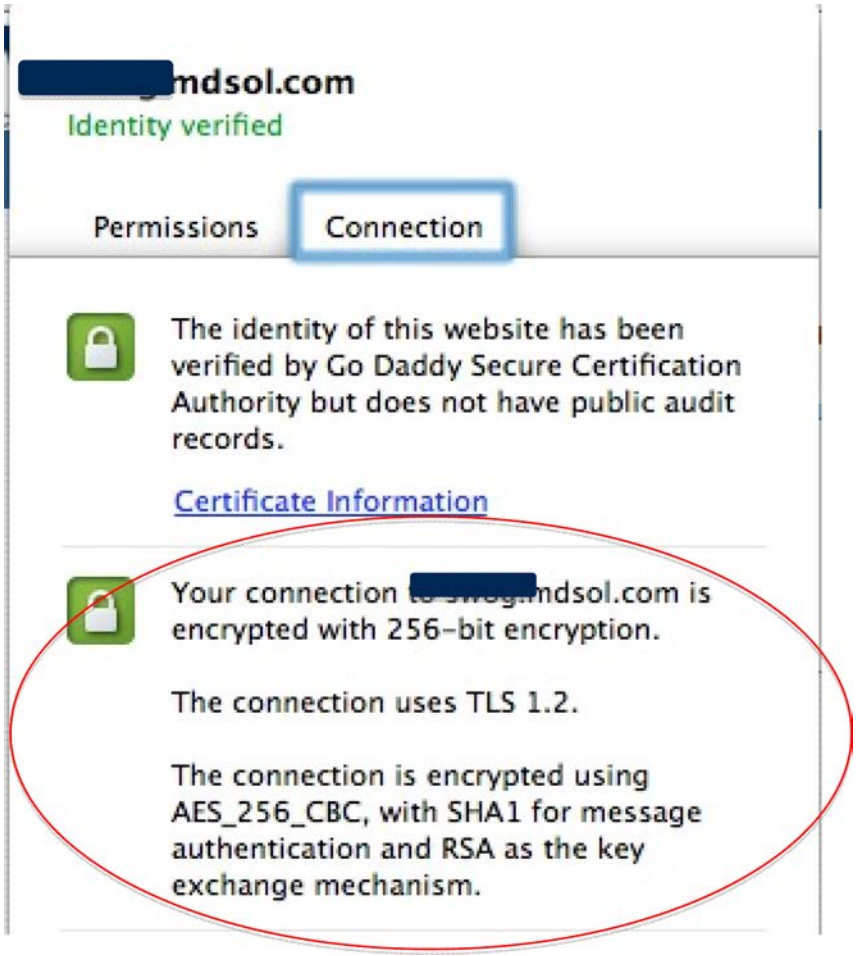


図 4. 転送の暗号化

システム管理

サーバーにアクセスする業務ニーズを持つ管理者は、ホスト サーバーにアクセスするために多要素認証を使用する必要がある。これらのサーバーは、クライアントのデータの分離を保護するために特別に設計、構築、構成、および強化されたシステムである。このようなアクセスは、すべてログに記録されて監査される。従業員が業務でサーバーにアクセスする必要がなくなった場合、該当するホストと関連システムに対する特権とアクセス権は取り消される。

クラウド セキュリティ

メディデータは、クラウドコンピューティングサービスとしてアマゾンウェブサービス (AWS) を使用している。一部の処理では、AWS はメディデータの従来のデータセンターと連携して動作する。AWS 内での顧客データのセキュリティを保証するため、メディデータは AWS セキュリティの包括的な評価を実施した。

- 物理的セキュリティ : 手動管理策と自動管理策による複数の層で構成されるミリタリ グレード
- 論理的セキュリティ : 優秀
  1) AWS は、米国保健福祉省 (HHS) など、多数のクライアントによるレビューを受けている
  2) AWS は、専門のセキュリティ チームによって 24 時間週 7 日監視される
  3) AWS には大量のクライアントがおり、そのすべてに対応するために最高レベルのセキュリティを実装する必要がある

4) AWS は、Ernst & Young によって年 1 回 SOC-1、SOC-2、および SOC-3 の監査を受けている

5) メディデータは、AWS のセキュリティを補足するため、クライアントと暗号化に対し、24 時間週 7 日の SIEM 監視を行っている

- 仮想化のセキュリティ： 業界のベスト プラクティス

1) データの処理中、同じ物理マシンで実行される異なるインスタンスは、Xen ハイパーバイザーによって相互に分離されている。

2) AWS のファイアウォールは、ハイパーバイザー層の内部にあり、物理ネットワーク インターフェイスとインスタンスの仮想インターフェイスの間に存在する。すべてのパケットがこの層を通過する必要がある。そのため、特定のインスタンスに隣接するインスタンスはインターネット上の他のホストからはそのインスタンスにアクセスできず、別個の物理ホストに存在するかのように扱うことができる。

3) 物理 RAM も同様のメカニズムを使用して分離される。

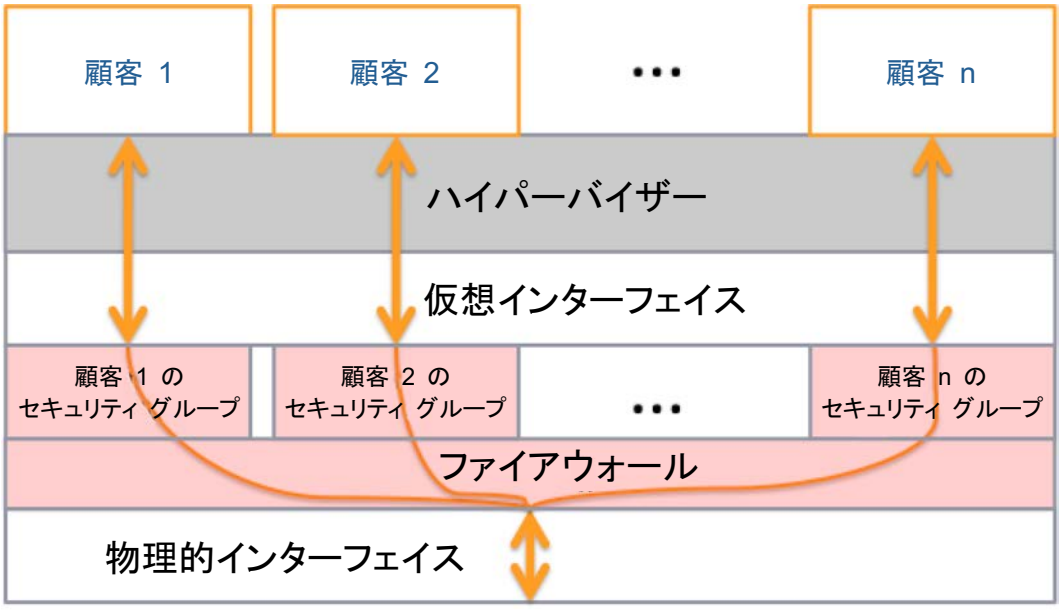
4) DDoS からの保護

5) MITM (仲介者) 攻撃からの保護

6) IP スプーフィングはホスト OS レベルで阻止される

7) パケット スニッフィング プロミスキャス モードは、ハイパーバイザー レベルでは効果がない

8) 変更に使用される構成管理



AWS の許可を得て使用

図 5. AWS の仮想化

ストレージ デバイスの使用停止

メディデータでは、ハードドライブが耐用年数に達した際の手順に使用停止プロセスを含めている。これは、権限を持たない個人に顧客データが漏えいするのを防止するためである。その際、DoD 5220.22-M (「National Industrial Security Program Operating Manual」) または NIST 800-88 (「Guidelines for Media Sanitization」) に詳述された業界標準の手法を使用し、使用停止プロセスの一環としてデータを破棄している。これらの手順でデバイスを使用停止できるまで、デバイスは、サーバールーム内の施錠された安全な環境に物理的に保管される。

構成管理

メディデータの既存インフラストラクチャに対する緊急の構成変更、突発的な構成変更、その他の構成変更は、類似システムの業界基準に従って許可、記録、テスト、承認、および文書化される。メディデータは、ソフトウェアの更新やインフラストラクチャの修理を行う場合は、顧客およびそのサービスの使用への影響を最小限に抑えるため、事前に電話または電子メールで顧客に連絡する。メディデータは、体系的な変更管理アプローチを適用し、顧客のサービスに対する変更が入念にレビュー、テスト、承認され、適切に伝達されるようにする。

セキュリティ パッチとインシデント対応

情報セキュリティのアラートは、メディデータのセキュリティオペレーションセンター (SOC) またはグローバルネットワーク オペレーションセンター (GNOC) のシステムから ISP のスタッフにエスカレートされ、さらにそこから企業情報セキュリティ責任者 (CISO) と上級管理職にエスカレートされる。顧客アラートをトリガーする状況と顧客への通知内容は、インシデント対応ポリシーに詳しく記載されている。またこのポリシーは、セキュリティインシデントのライフサイクルを管理するための対応についても参照する。この計画は、イベントやインシデントの特定、準備、封じ込めから復旧、通知、事後分析に至るまでの各段階と、その段階に関連するアクションを記述する。メディデータは、セキュリティインシデントの検出後妥当な時間内にインシデントを確認して影響分析を実施し、サービス契約で定められた連絡経路を通じてメディデータのクライアントに通知する。すべての問題は、オンラインのデータベース駆動型問題管理システムで追跡される。上級レベルの管理職は、情報セキュリティがメディデータの文化の一部になるよう徹底する。

一般的に、大きな脅威となる悪用が含まれるセキュリティの問題のうち、内部の Nessus スキャン ツールまたは権限のある外部ソースによって重大と評価された脆弱性タイプを伴うものには 30 日以内に対処する。恒久的な修正は、通常 90 日以内に実装される。ただし、関連パートナーと調整して完全なテストと合意を確認するまでは、パッチは適用されない。例えば、数時間以内に修復された大きな脅威と重大な脆弱性としては、最近世界的規模で発生した Heartbleed や Shellshock などの問題が挙げられる。

データベース セキュリティ

すべてのデータは定期的にバックアップされる。完全バックアップは少なくとも週 1 回実施され、増分バックアップは 1 日 1 回実行される。重要な臨床試験データは 15 分ごとにバックアップされる。バックアップデータは、暗号化された形式でテープに転送され、Iron Mountain が提供するオフサイトの場所に保管される。Rave の臨床データも毎日電子的に完全に複製され、メディデータのディザスタリカバリ用バックアップ施設に送られる。

Rave データベース内のクライアント情報は、仮想化を使用して分離される。各クライアントは仮想化されて、別個のデータベースで動作する。

図 6. 仮想データベース

メディデータのプラットフォームのその他の要素は、マルチテナント環境のアマゾンウェブサービス内で実行される。この環境では複数の顧客が同じアプリケーションを共有し、同じハードウェア上の同じオペレーティング システム上で、同じデータストレージメカニズムを使用してアプリケーションが実行される。各顧客はアプリケーションの設計時に区別されるため、顧客がお互いのデータを共有したり参照したりすることはない。

ビジネス継続性とディザスタリカバリ

ビジネス継続性 (BCP: Business Continuity Plan) とディザスタリカバリ (DRP: Disaster Recovery Plan)

ビジネス継続性およびディザスタリカバリ計画(DRP)は、ビジネス全体を対象にした二重のアプローチである。そのため、これらの活動では、管理、人事、IT サポート機能、顧客向け製品の DRP をはじめとするすべての部門とビジネス分野によるビジネス管理が必要となる。BCP チームは内部のビジネス プログラムの開発の監督を担当するのに対し、サービス提供部門はクライアントのディザスタリカバリ計画を監督する。両部門は、上級管理職が計画の立案、監視、および維持管理に十分なリソースを投入するよう図る。

メディデータのディザスタ リカバリ/ビジネス継続性計画は、障害発生時における企業の計画、手順、およびガイドラインを定義するものである。特に、想定外の出来事に直面してもメディデータを維持するため、事業運営、内部データ、システム、および重要な内部機能の回復手順を定める。

この計画の主要な目的は次のとおりである。

- 緊急事態または災害に対するメディデータの脆弱性と、それらの緩和、対応、および復旧に利用可能なリソースの特定、評価、および優先度を定義する
- メディデータの緊急事態への対応、復旧能力を向上させるための短期的、中期的および長期的な対策の概要を示す
- 緊急時に利用可能な全リソースを効率的に利用できるよう備える
- 緊急事態または災害の発生時にメディデータの業務の継続性を確保する

災害発生時にクライアントのデータを保護するため、メディデータは、従来のバックアップに加えてサイト間での電子的なデータ複製も実行する。実稼働するデータ センターから離れた場所にディザスタ リカバリ専用のサイトがある。BCP/DR テストを年 1 回実施する。

計画の構成要素

計画はさまざまな要素で構成される。そのすべての要素が協調し、メディデータが業界の既知の要件や規制要件をすべて満たすようにする。

ビジネス継続性計画 (BCP)

- 危機管理
- ビジネス センターの移転
- 代替ワークプレイスのオプション
- サービス プロバイダとの包括的な契約

パンデミック対応計画 (PRP: Pandemic Response Plan)

- 教育
- パンデミック封じ込めのための予防措置
- 責任、ガバナンス
- ポリシーと手順

ディザスタ リカバリ (DR)

- 年 1 回の訓練
- 復旧手順の文書化
- サービス プロバイダとの包括的な契約

ディザスタ リカバリ (DR)

メディデータはディザスタリカバリ計画を導入しており、アラートリスト、チームの責任分担、復旧と通知の手順、再開計画、インストールタスク、作業領域のチェックリスト、および緊急時対応手順を定めている。計画外のダウンタイムが発生する場合は、メディデータのサポート チーム、製品チーム、およびアカウント管理チームがすべての顧客にその旨を通知する。通知はまず、電子メールで行い、状況が悪化した場合は電話を使用する。計画の策定と維持管理には、サービス提供チームが上級管理職チームと協力して当たる。

データセンター限定の災害の場合は、メディデータのディザスタリカバリサイトの 1 つで業務を継続する。実稼働用、DR 用、およびテスト用の施設はすべて冗長電源と無停電電源装置 (UPS) で完全にサポートされる。これらの電源は、ディーゼル発電機が稼働するまでの間 (通常は 12 秒以内)、十分な電力を供給する。

ポリシー

POL-IS-001 Information Security

このポリシーは、さまざまな世界的プライバシー規制への準拠に必要な機密性を提供するため、メディデータのシステムをどのように構成する必要があるかを定める。EU 95/46、PIPA、FISMA などの法律や、他の国/地域の法的要件は、メディデータに対し、個人のプライバシーを保護し、クライアントの情報の機密性とセキュリティを確保することを要求している。

POL-CORP-006 Corporate Incident Management Policy

このポリシーは、業務中断インシデントの影響を防止、最小化し、メディデータがミッションとコミットメントを継続できるようにするための計画の作成と保守を指示する。このポリシーを受けて、メディデータは重要な企業システム、復旧アクション、および復旧タイムラインを詳述した企業インシデント管理計画を作成した。この計画により、ビジネス継続性計画は 2016 年 4 月 29 日をもって廃止された。また、この計画は施設チームによって管理される。

POL-ISP-004 Organizational Security Policy

このポリシーは、内部、外部の両方で情報保護を担当するメディデータの組織について詳述する。例えば、内部管理策は情報セキュリティの責任を割り当てるのに対し、外部管理策はサードパーティサービス契約のセキュリティを扱う。組織のセキュリティは、ビジネス継続性を確保するほか、セキュリティインシデントの影響を防止、最小化することによってビジネスへの被害を最小限に抑えるものである。

POL-IS-005 Physical and Environmental Security Policy

このポリシーの目的は、オフィスやサーバー ルームなど、機密情報が収められているメディデータのすべての作業エリアへのアクセスを制限するガイダンスを提供することである。さまざまな管理策により、業務ニーズを持つ人物に対する、アクセスを物理的に制限する要件を満足する。このポリシーは、中断なく顧客にサービスを提供できる回復力と柔軟性を備えた環境管理策の要件も強化する。

POL-IS-006 Asset Classification & Control Policy

このポリシーの目的は、資産の分類と管理についての重要な要件を詳述することである。これらの対策は、スタッフのミスや部外者による侵害が発生した後で、漏えい、利用不可、または破損からメディデータの情報を保護するために必要である。

POL-IS-007 Information Security & Privacy Policy Regarding Staff Members

このポリシーは HR 部門と協力して作成され、その目的は、メディデータのスタッフに適用される情報セキュリティ標準についてガイダンスを提供することである。メディデータは、当社が管理するデータの利用規程をスタッフが理解し、これに同意するよう徹底する。

POL-ISP-008 Network and Computer Operations Security Policy

このポリシーの目的は、適切なネットワーク運用セキュリティ ポリシーの要素を明らかにし、ネットワーク情報セキュリティの必要性について説明し、さらに、ネットワークおよび運用の情報セキュリティのさまざまなカテゴリを規定することである。この文書は、メディデータの包括的なネットワーク運用セキュリティポリシーを定める。

POL-ISP-009 Access Control Security Policy

アクセス制御セキュリティポリシーの目的は、コンピュータの接続に関する一連のルールを定義することである。これらのルールは、メディデータのコンピュータ システムがデータ (例 : 機密性およびプライバシー) の破壊、窃取、損失に遭うリスク、事業運営の中断、および電子リソースの不正使用によって引き起こされる可能性がある、メディデータのイメージへの被害を最小限に抑えることを意図している。

アクセス制御セキュリティポリシーは、メディデータのネットワークに接続される場合のサーバー、インターネットサーバー、およびクライアントコンピュータの役割を定義し、それらの間で許可される通信フローを定義する。

POL-IS-010 System Development and Maintenance Security Policy

メディデータは大量の情報を保有している。メディデータには、制定法上、契約上、規制上、および内部的に、常に機密性、品質、および可用性を確保してこの情報を処理する多様な義務がある。このようなシステムの設計や保守において脆弱性や欠点があると、セキュリティが侵害されるおそれがある。このポリシーの情報システムとは、あらゆる形式 (例 : 紙または電子的) のインフラストラクチャ、既製品パッケージ、外部システム、オペレーティングシステム、ビジネスアプリケーション、およびユーザーが開発したシステムを含む。

基本的なセキュリティ要件を特定して理由を明確化し、概念および設計から構築、保守に至るまで情報システムに組み込む必要がある。これは、すべての段階でリスクを堅実に評価して緩和することによって達成できる。

POL-ISP-011 Responding to Security Incidents and Malfunctions

このポリシーの目的は、侵入が発生する前にデータ侵害に対応する方法についての一般的なガイドラインを提供することである。メディデータは、メディデータのシステムが関係するコンピュータ セキュリティ インシデントに対応するため、標準ガイドラインの策定に取り組んでいる。攻撃は多種多様で絶えず変化しているため、攻撃への対処にはさまざまな法的および技術的な問題が含まれる可能性がある。このポリシーは、関係する問題の概要と、攻撃を防止して被害を軽減するための実践的なガイドラインを提供することを目的としている。メディデータは年 1 回データ侵害演習を実施して、計画の有効性を評価している。

POL-ISP-013 Compliance Security Policy

このポリシーの目的は、メディデータが運営されている場所の規制制度に準拠すると同時にイノベーションを促すことである。メディデータの目標は、情報セキュリティとデータプライバシーに関して規制法や国際法の義務に準拠できるよう、効果的な取り決めを確実に整備することである。メディデータ内の法律および規制の専門家のほか、外部の対象分野の専門家とも緊密に協力する。

POL-ISP-014 Mobile Device Security Policy

このポリシーは、メディデータ スタッフがスマートフォンやタブレット デバイスなどのモバイルデバイスでセキュアエージェント: OKTA を使用する上での要件を扱う。このエージェントは、メディデータの企業情報を分離し、デバイス上で暗号化する。さらに、該当データをメディデータがリモートで削除できるようにする。

Patient Cloud のセキュリティ

医療機器が相互接続、相互運用されることが増えると、患者が受けるケアを向上させ、臨床試験システムを効率化できる。システムの設計時に、メディデータは、医療機器に関係する可能性があるサイバー セキュリティリスクを慎重に考慮し、システム管理策またはソフトウェア更新を管理するための計画を策定する。この領域におけるメディデータのガイダンスは、NIST SP 800-53 および NIST 800-82 に由来する。FDA の勧告も同じ NIST Publications に基づいている。

Patient Cloud ソフトウェアの保護アプローチは、Clinical Cloud ソフトウェアの他の部分とは異なる。その一部はモバイルデバイスで実行されるためである。メディデータのセキュリティチームは、Patient Cloud の安全性を保証するため、以下のステップを実施した。

- アプリケーションの設計をレビューし、機器との通信がすべて暗号化されるようにした。当社のソフトウェアに組み込まれた暗号化は、その暗号化強度により、米国政府から評価と輸出許可を得ている。
- サード パーティ (Coalfire Labs) による製品の侵入テストを実施し、セキュリティの弱点を特定した。iOS バージョンには弱点はまったく見つからず、Android バージョンには弱点が 1 つ見つかったが修正した。
- 幾度もの設計ミーティングを通じて運用可能なアーキテクチャをレビューし、デバイスからデータセンター内のストレージに至るまですべての情報が保護されていることを確認した。このホワイトペーパーでは、全製品のデータセンターのセキュリティが対象である。

Medidata Imaging のセキュリティとプライバシーの管理策

2016 年 4 月、メディデータは医療用画像管理およびワークフローのプロバイダである Intelemage® を買収した。このホワイトペーパーで説明するポリシーと手順は一般的に、メディデータが現在管理している Intelemage (現在の名称は「Medidata Imaging」) に適用される。ただし、Medidata Imaging 製品 (例 : InteleGrid®) は、他のメディデータ製品に物理的に統合されていない。以下の追加情報は Medidata Imaging 製品に固有のものである。

セキュリティ管理策

メディデータの Imaging 製品は、オハイオ州シンシナティとアリゾナ州フェニックスにある 2 つのデータ センターで運用される。フェニックスはティア 4 の主要データセンターで、I/O データセンターのコロケーションプロバイダである。どちらのデータセンターも年 1 回、物理的セキュリティと環境維持についての管理策に焦点を当てた Service Organization Control (SOC1) の監査を受けている。監査に関する詳細は、メディデータの規制および監査ポリシーで参照できる。

(2017 年より、これらのデータセンターには ISO 27001:2013 および FISMA の認証も追加される予定である。Medidata Houston および New York はこれらの認証を取得済みであるため、その範囲を拡大して Medidata Imaging を対象に含めることは容易で、メディデータの認証戦略を論理的に延長するものである。)

Medidata Imaging のセキュリティ管理策戦略は、ISO 27001:2013、NIST 800-53、CoBIT など、定着したさまざまなセキュリティ モデルに基づく。管理策の具体的な領域には以下が含まれる。

1. インシデント管理
2. 変更管理
3. 暗号化 (伝送時および保存時)
4. ID およびアクセス管理
5. 脆弱性の評価と修復
6. コンフィグレーション管理
7. ソフトウェアとハードウェアのライフサイクル
8. 物理的セキュリティ
9. セキュリティに関するトレーニングと教育
10. ディザスタ リカバリとビジネス継続性

さらに、Medidata Imaging の情報セキュリティ管理システム (ISMS) は、メディデータの継続的改善への取り組みの一環として年 1 回レビューされる。

PHI および HIPAA の適用

注 : 以下の情報は、1996 年の医療保険の携行性と責任に関する法律 (「HIPAA」) で定義された電子的保護医療情報 (「PHI」) に関するもので、Medidata Imaging の顧客に情報を提供する目的で記載されており、法的勧告を目的としたものではない。

PHI は、特定の個人の健康情報を識別し得る 18 個の ID のセットと定義される。HIPAA および関連する規制に従い、特定の状況下で PHI を保護する必要があり、これには PHI を扱うエンティティが事業提携契約 (「BAA」) を施行する要件が含まれる。

Medidata Imaging に関しては、以下の場合には HIPAA は適用されない。

1. PHI を収集しない (Medidata Imaging サーバーに送信されない)
2. 患者の許可の下で PHI を収集する (例えば、臨床試験のインフォームド コンセントに含まれる場合など)
3. 患者の治療のために PHI を収集する (患者の治療の例外)

PHI の収集有無 (上記 #1) に関する詳細として、Medidata Imaging の製品を、そもそも PHI を収集しないように構成できる。メディデータの製品には、顧客システムにインストールできる「アプレット」が付属している。このアプレットを、データを Medidata Imaging へ安全に転送する前に PHI (DICOM ヘッダー情報など) を削除するように構成できる。その結果、Medidata Imaging のサーバーに安全に転送されるときには、データは PHI ではなくなっている。

さらに、DICOM ヘッダー情報があっても PHI が含まれないイメージ タイプもある。このようなイメージは HIPAA 要件の対象にはならない。

医療サイトや他のエンティティは、Medidata Imaging のセキュリティまたはプライバシーの管理策に関してさらに疑問がある場合、契約しているスポンサーや開発業務受託機関 (CRO) (Medidata Imaging の顧客)に確認する必要がある。

メディデータ Regulated Content Management (RCM)

メディデータは 2017 年 2 月に CHITA を買収し、その機能は現在、メディデータ RCM と呼ばれている。RCM は、1 つのアプリケーションで規制コンテンツと未規制コンテンツの両方を作成、保存、表示、編集、および共同作業する機能をユーザーに提供する。RCM のセキュリティ管理策戦略は ISO 27001:2013 に基づくため、このホワイト ペーパーで説明されているポリシーと手順はメディデータの RCM の管理にも適用される。

現在のところ、メディデータ RCM は、カリフォルニア州サンノゼとバージニア州アッシュバーンの 2 か所にある Equinix のコロケーションデータセンターで処理されている。これらのデータセンターのインフラストラクチャサポートサービスは、Synoptek によって提供される。Equinix のデータ センターは、年 1 回 Service Organization Control (SOC-1 および SOC-2) の監査を受けており、ISO 27001 認証を取得済みである。

メディデータは、RCM の処理を 2017 年第 3 四半期までにテキサス州ヒューストンのデータ センターへ移設する計画である。

よく寄せられる質問

1. アマゾンウェブサービスは従来のデータセンターと同様に安全かつ安心か?

クラウドのセキュリティはメディデータが所有するデータセンターと同様である。クライアントの観点からは、物理サーバーやストレージデバイスは存在せず、どちらもソフトウェアベースのセキュリティツールを使用してコンピューティングリソースに出入りする情報の流れを監視し、保護する。

共通点

- メディデータが社内のデータセンターで使用しているセキュリティツールと手法がクラウドでも使用されている。
- 使用されているオペレーティング システム (OS) とメディデータ アプリケーションも同じで、最新のセキュリティパッチ、データのバックアップ、ウイルス対策、侵入検知、セキュリティ インシデントおよびイベント管理 (SIEM) のツールで更新される。
- メディデータは、相互に分離を維持すべき環境を分離するためにサブネットを設定している。例えば、開発およびテスト環境を実稼働環境から分離した上で、ネットワーク アクセス制御リスト (ACL) を構成し、これらの環境間のトラフィックのルーティングを制御している。
- メディデータには、開発者、テスター、管理者といった複数のユーザーが存在し、そのそれぞれに AWS リソースにアクセスするための固有の資格情報を提供している。さらに、多要素認証を使用するよう要求している。
- SumoLogic のネットワーク監視ツールとセキュリティ管理ツールを使用し、各種リソースからログとネットワークトラフィック情報を収集して分析している。
- メディデータは、当社のシステムに対して脆弱性スキャンを実行している。
- データセンターからクラウドリソースまでの間に仮想プライベートクラウド (VPC) を設定し、伝送保護の層を追加する予定である。この VPC では、クライアントは従来のパブリックサブネットではなくプライベートサブネットで動作する。

相違点

- 管理者/開発者は、AWS リソースをローカルではなくリモートで管理する。
- ハードウェアベースのソリューションではなく、ソフトウェアベースのセキュリティメカニズムを使用する。
- 構成済みの機器を導入するのではなく、IT サポートメンバーが立ち上げと構成を行う。
- AWS で実行されるすべてのメディデータアプリケーションには、デジタル署名と暗号化キーを使用した認証が必要である。

- 1 つのファイアウォールですべてのリソースを保護する代わりに、第 2 のファイアウォールのように機能するセキュリティ グループがすべての仮想サーバーに含まれる。
- ソフトウェアは、仮想サーバー (EC2 インスタンス) のベースライン イメージによって強化される。OS、ライブラリ、アプリケーション、構成などが含まれるテンプレートである Amazon マシン イメージ (AMI) を作成する。これにより、そのベースラインイメージを保存しておいて、新しいインスタンスを起動するたびにそのイメージを自動的にロードできる。
- SaaS モデルでの運用とオンサイトのデータ センターは物理的に異なる。しかし、AWS データセンターはメディデータの特定のセキュリティ要件を満たす必要があり、SOC2、ISO 27001、セーフ ハーバーなどの認証を取得している。

セキュリティ面でのクラウドの利点

- **在庫の即時可視化**
  資産保護の第一歩は、何が資産に当たるかを判断することである。AWS Config やリソースのタグ付けなどのツールを使用することにより、特定の時点で使用しているクラウド資産を常に正確に確認できる。
- **追加のセキュリティ ツール**
  AWS は、メディデータが使用する AWS 仮想スペースの監視および構成専用のセキュリティツールのリストをメディデータに提供する。
- **DDoS からの保護の強化**
  AWS はそのサイズとスケールにより、処理能力が高く DDoS への耐性も高い。AWS インフラストラクチャは、極めて大量のトラフィックを処理する能力を備えており、ELB、Auto Scaling、CloudWatch、CloudFront などの AWS サービスを使用すれば、メディデータは DDoS 攻撃に耐えられる高可用性システムを設計できる。
- **セキュリティの規模の経済**
  AWS クラウドを利用している場合、メディデータとその顧客には大企業と同じセキュリティの利点がある。メディデータのセキュリティ専門チームに加え、AWS にも大規模なセキュリティ専門チームが存在し、基礎となるクラウド インフラストラクチャを継続的に監視、保護する多様なシステムとツールがある。
- **ハードウェアの継続的なリプレースとアップグレード**
  AWS は、常にインフラストラクチャの向上に取り組んでいる。寿命に達したハードウェアは、最新のプロセッサにリプレースされる。これにより、パフォーマンスと速度が向上するだけでなく、最新のセキュア プラットフォーム技術 (メディデータが使用する AES アルゴリズムの実行を大幅に高速化する Intel AES-NI 暗号化命令セットなど) も利用できるようになる。

2. *メディデータはなぜ SFTP ではなく FTPS を使用するのか?*

セキュア FTP 転送を利用する場合、SFTP (FTP over SSH) と FTPS (FTP over SSL) という 2 つの業界標準プロトコルがある。SFTP と FTPS は、どちらも転送データを暗号化するために AES や Triple DES などの強力なアルゴリズムを実装しているので、高いレベルの保護を提供する。また、さまざまな機能と、ファイルの転送および操作用の幅広いコマンド セットもサポートする。したがって、SFTP と FTPS の最も大きな違いは、接続の認証と管理の方法である。

SFTP の場合、ユーザー ID とパスワードだけで接続を認証し、SFTP サーバーに接続できる。パスワードに追加するか、またはパスワードの代わりに SSH キーを使用して SFTP 接続を認証することもできる。キーベースの認証の場合、ユーザーは前もって SSH 秘密鍵と公開鍵を生成しておく必要がある。SFTP サーバーに接続する際に、認証のためにソフトウェアからサーバーに公開鍵が転送される。キーと、入力したユーザー/パスワードが一致すれば、認証が成功する。

FTPS の場合、接続はユーザー ID、パスワード、および証明書で認証される。SFTP と同様に、FTPS 接続でもユーザーとパスワードは暗号化される。接続時にまず、FTPS クライアントは、サーバーの証明書が信頼されているかどうかをチェックする。証明書が VeriSign などの既知の証明機関 (CA) によって署名されているか、または (パートナーによって) 自己署名されていて、信頼できるキー ストア内にその公開証明書のコピーがあれば、その証明書は信頼できるとみなされる。

つまり、SFTP と FTPS はどちらも強力な認証オプションを備えており、非常に安全である。しかしながら、FTPS の方がずっと安全にファイアウォールを通過できるため、メディデータの全体的なセキュリティ アーキテクチャに適している。また、FTPS を採用するクライアントの割合が増えていることから、メディデータが求めるセキュア FTP としては FTPS が適切な選択肢である。

3. *どのようなサード パーティ製品を使用して処理を行っているか?*

製品 : **Google Analytics**

カテゴリ : サイト使用状況ツール

メディデータでの用途 : Web サイトの使用状況の追跡。ユーザーの場所、ユーザーが要求している言語、一部のパフォーマンス情報、サイトでの操作の内容、接続時間などの情報を提供する。Google Analytics は保存データを暗号化し、このデータを Google のセキュアなデータセンターに保存する。

製品 : **SocketLabs**

カテゴリ : サービスとしての電子メール

メディデータでの用途 : メディデータが SocketLabs に送信するユーザーデータには以下が含まれる。a) 試験と試験グループの名前。b) 試験と試験グループのカスタム電子メールプロパティの内容。これはユーザーが構成可能であるが、通常は単にサインアップ方法と、製薬会社および試験の詳細である。c) すべてのユーザーの電子メール アドレス。(d) 管理者であるユーザーの名前。(e) すべてのユーザーアカウントのアクティベーションコード。SocketLabs に送信するすべてのデータは電子メール内にも記述されるため、使用している電子メールプロバイダに関係なく、世界中のどこにあるサーバーでも処理できるデータである。無害なデータには、メディデータのロゴ、および試験への招待と電子メール アドレスの変更に関する定型表現などがある。

製品 : **New Relic**

カテゴリ : アプリケーション パフォーマンス管理

メディデータでの用途 : 実稼働環境と非実稼働環境の両方で展開済みアプリケーションのパフォーマンスメトリックを収集するため、New Relic を使用する。これらのメトリックには、トランザクション応答時間、Web トラフィックのスループット、Apdex スコアなどがある。これらのメトリックは展開済みのインスタンス別に分類され、ライブ トラフィックと履歴データの両方で利用できる。さらに、低速なトランザクションを New Relic によってキャプチャし、New Relic のシステムに保存されているこれらの低速なトランザクションに関する詳細情報をキャプチャする。これには、低速な要求の際に実行された呼び出し (Web サービスとデータベースの両方) の包括的なリストが含まれる。メディデータのサーバーからこれらのデータを収集するため、New Relic コレクタ デーモンをサーバーにインストールする。New Relic は、メディデータのデータを独自のセキュアなデータ センターでホストする。さらに、New Relic に送信されるデータは、送信中は TLS で保護される。

製品 : **SumoLogic**

カテゴリ : ログの集約と分析

メディデータでの用途 : メディデータの大半のアプリケーション スイーツは、アプリケーション、Web サーバー、およびアプリケーション サーバーのログを SumoLogic に定期的に送信する (一般的には、数秒ごとに新しいログ行が SumoLogic に送信される)。サーバー上で SumoLogic のコレクタを使用し、ログをバッファして SumoLogic に送信する。ユーザーのパスワード、サード パーティ資格情報などの機密情報は、サーバー上でも SumoLogic 内でもログに書き込まれない。SumoLogic は、メディデータの代わりに履歴ログ ファイルを AWS の Simple Storage Service (S3) に送信し、必要に応じてメディデータが MapReduce ツールなどでこの履歴データを分析できるようにする。SumoLogic では、ログ分析用の UI と API、アラート、およびカスタム ダッシュボードも利用できる。

4. どのプラットフォームがシングル インスタンス マルチテナント (SIMT) で、どれがマルチインスタンス シングル テナント (MIST) か?

製品	SIMT	データストア	場所
Balance	○	mySQL	AWS
Cloud Admin	○	MySQL	AWS
Coder	○	SQL Server	AWS
CSA	○	PostgreSQL	AWS
CTMS	×	mySQL	AWS
Grants Manager	○	SQL Server	AWS
Imaging	○	MySQL	メディデータ データセンター
iMedidata (authMedidata を含む)	○	mySQL および PostgreSQL	AWS
Insights	○	SQL Server	メディデータ データセンター
MCC Platform services (mAudit など)	○	AWS S3	AWS
Patient Cloud	○	mySQL	AWS
Payments	×	mySQL	AWS
Rave (Rave ウェブ サービス、SAS on Demand、ODM Adaptor、ファイル転送、JReview などを含む)	×	SQL Server	メディデータ データセンター
Rave アドホック レポート (BO4)	○	SQL Server	メディデータ データセンター
RaveX	○	SQL Server	メディデータ データセンター
RCM	○	mySQL	Equinix
Safety Gateway	○	SQL Server	メディデータ データセンター
SQM	○	SQL Server	メディデータ データセンター
TSDV	×	SQL Server	AWS

Information Security and Privacy White Paper

Version: 2017.5
Date: 27 Jul 2017
Author: Glenn Watt, Corporate Information Security Officer (CISO)
Pages: 26

This page intentionally left blank

Table of Contents

Policy 4
Roles and Responsibilities 4
Reports, Certifications and Independent Attestations 5
Physical Security 5
Network Security 5
Application Security 6
Data Privacy 7
ISO 27001:2013 8
SOC 2 Type 2 8
SOC-1 Type 1 8
FISMA / FedRAMP 9
Privacy Shield 9
FIPS 140-2 9
HIPAA 10
Non-descript buildings 10
Uniformed Guards 10
Photo-ID Smart Cards 10
Biometric Door Locks 10
Video Surveillance 10
Firewall 11
Intrusion Detection & Prevention 11
Virus, Spybot, Spam Scanning 12
Security Management 12
Encryption during data transmission 13
System Administration 14
Cloud Security 14
Storage Device Decommissioning 15
Configuration Management 16
Security Patches and Incident Response 16
Database Security 16
Business Continuity (BCP) and Disaster Recovery (DRP) 17
Plan Components 17
Disaster Recovery (DR) 18
POL-IS-001 Information Security 18
POL-CORP-006 Corporate Incident Management Policy 18
POL-ISP-004 Organizational Security Policy 18
POL-IS-005 Physical and Environmental Security Policy 19
POL-IS-006 Asset Classification & Control Policy 19
POL-IS-007 Information Security & Privacy Policy Regarding Staff Members 19
POL-ISP-008 Network and Computer Operations Security Policy 19
POL-ISP-009 Access Control Security Policy 19
POL-IS-010 System Development and Maintenance Security Policy 19
POL-ISP-011 Responding to Security Incidents and Malfunctions 20

POL-ISP-013 Compliance Security Policy **20**
POL-ISP-014 Mobile Device Security Policy **20**
Patient Cloud Security **21**
Medidata Imaging Security and Privacy Controls **21**
Medidata Regulated Content Management (RCM) **22**
Frequently Asked Questions **23**

Figures

Figure 1. Application Security 6
Figure 2. Data Privacy 7
Figure 3. Data Center Security 11
Figure 4. Transmission Encryption 14
Figure 5. AWS Virtualization 15
Figure 6. Virtual Databases 17

Medidata Information Security and Privacy

Medidata's solutions deliver an entire clinical development process through innovative clinical cloud technology. Whether for your first study or an enterprise solution across multiple phases and therapeutic areas, our suite of products streamlines key clinical development operations, including protocol development, trial planning and management, site collaboration, randomization and trial supply management, monitoring, safety event capture, electronic data capture (EDC) and management, advanced reporting and business analytics. Medidata delivers clinical cloud computing solutions with high availability, integrity, confidentiality, reliability and the flexibility to enable customers to access a wide range of applications. Medidata builds services in accordance with security best practices and provides the appropriate security features in order to ensure end-to-end security and end-to-end privacy. Ensuring the confidentiality, integrity and availability of customer data is of the highest importance to Medidata, as is maintaining trust and confidence.

Medidata provides a wide range of information regarding its hosted IT environment to customers through a variety of white papers, reports, certifications and third-party attestations. This information assists customers in understanding the controls in place relevant to the Medidata products and services they use and how independent auditors validate those controls. This information also assists customers in their efforts to account for and to validate that controls are operating effectively in their extended IT environment.

Overview

Policy

Information security policy defines what it means for a system, organization or other entity to be secure. At Medidata, it addresses the constraints on behavior of all staff as well as constraints imposed on potential adversaries by mechanisms such as doors, locks, firewalls and scanners. Medidata constrains access by external systems and adversaries including programs and access to data by people. To assure the completeness of our security policies, we follow the ISO 27001 architecture as a baseline, and then supplement this with portions of other recognized security architectures.

Roles and Responsibilities

Medidata has clearly segregated duties, based on business need, for management of the software-as-a-service (SaaS) resources. The following lists the typical resource groups and the tasks for which they are responsible.

1. Technology: The Executive Vice President, Technology and Chief Technology Officer (CTO) is the executive manager of Medidata applications' technical operations. The span of control covers development, operations and information security. This position oversees application management from architecture, engineering, testing and implementation to maintenance. CTO is also responsible for ensuring clients' technical review, pre-assessment and audit requests are addressed.
2. DevOps: This team is comprised of individuals who are dedicated to ensuring the continuous working of Medidata applications.
3. Service Delivery: The service delivery team is comprised of individuals tasked with the installation, configuration, change and maintenance of all hardware-, software- and infrastructure-related activities to support the Medidata applications.

4. Network Operations Center (NOC): The system-monitoring group is responsible for configuring, maintaining and monitoring alerts and notices critical to ensuring the uptime and health of Medidata applications and infrastructure.
5. Information Security: The group headed by the Vice President Information Security and Chief Information Security Officer (CISO) is tasked with the management of policies in the context of publicly accepted standards, regulations and frameworks as well as the implementation of those controls to ensure that the security, scalability and stability of the technical environment is maintained..
6. Enterprise Support: The corporate IT team helps support the enterprise IT services to enable Medidata to operate and conduct its daily business activities. The enterprise support team directly reports into the Chief Technical Officer (CTO). The enterprise support team does not have access to nor any access into customer-facing Medidata applications.

Reports, Certifications and Independent Attestations

In 2011, Medidata successfully completed a Service Organization Controls 2 (SOC 2) report in accordance with the SSAE 16 professional standards. In April 2017 Medidata successfully completed a Service Organization Controls 1 (SOC 1) report for our "Medidata Payments" application. For our United States (U.S.) government clients, Medidata completed our initial FISMA certification and accreditation in 2009. For international clients concerned with privacy, we received authorization in 2011 from the U.S. Department of Commerce to participate in the Safe Harbor program that certifies the protection we afford is equivalent to the protections required in the European Union (EU 95/46). In addition, in November 2016, the U.S. Department of Commerce approved Medidata's self-certification to the Privacy Shield program. Medidata also received an ISO 27001:2013 certification in October 2016. We will continue to obtain the appropriate security certifications and conduct audits to demonstrate the security of our products and services.

Physical Security

Medidata has many years of experience in designing, constructing and operating data centers. Our physical security can best be described as military grade. We employ a combination of building guards, smart-ID badges with electronic access, video surveillance and biometric scanners. Our buildings are non-descript and only those who have a legitimate business need know the actual location of these data centers.

Network Security

Network security is a 24-hour-a-day priority at Medidata. We start with border protection that includes routers and load balancers to provide high availability even during distributed denial of service (DDoS) attacks. Border protection is bolstered by our firewalls that deny all inbound ports with no identified business purpose as well as outbound ports. Authorized data that passes through the firewall is then subjected to a series of malware scanners as well an intrusion detection/prevention system. Monthly, we scan our networks internally; and once a year we submit our networks to a third-party assessment to identify and correct any new Internet vulnerabilities.

Application Security

Medidata's applications are critical to our success, and making sure they are safe and secure for our customers is paramount. Consequently, we perform numerous internal tests using VeraCode© on our software during the development process. Then we take our production products and dedicate time for internal hacking (Black Hat). During this phase, we attempt to uncover and then patch subtle issues that are only detectable with an intimate knowledge of our source code. Medidata then goes to the next level by evaluating the interoperability of the product suite to improve the resilience of our products. Medidata also submits our software to third-party assessments to identify and patch any vulnerability that may have made it to this point in the lifecycle. Vulnerabilities discovered during internal or external third party testing are logged into Medidata's JIRA™ trouble ticketing system. From there our internal teams analyze the vulnerability, confirm it and then estimate a remediation date. The assigned team has sixty (90) days to resolve the request before it is elevated to the CISO for review and possible deadline extension. After ninety (90) days, it also requires the CIO or the COO review and approval for further extensions. Extensions are generally granted for situations where a patch isn't available from a software manufacturer, or where a repair requires extensive development and testing to avoid creating a greater problem upon deployment.

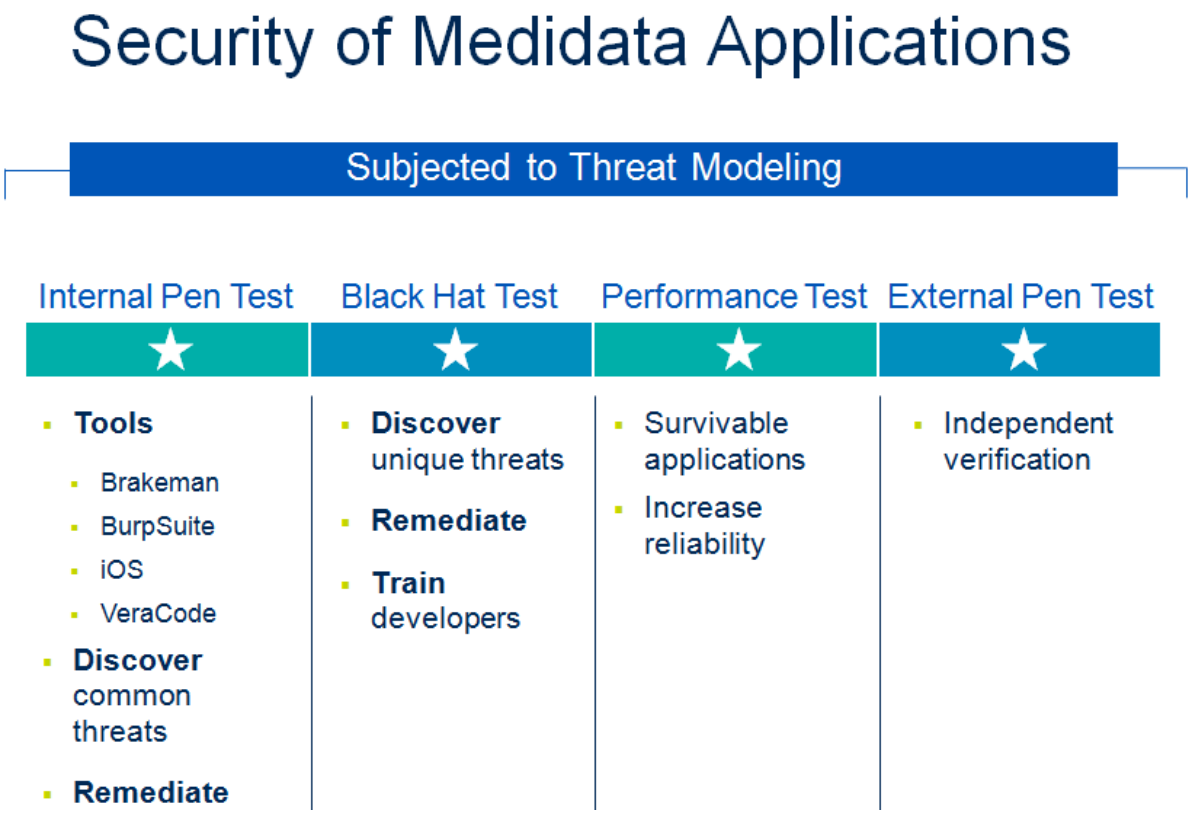


Figure 1. Application Security

Data Privacy

Medidata treats the privacy of our customers' data as a top priority. Global privacy regulations vary considerably, so our approach is that protecting to the most stringent standards is best. Medidata established a privacy policy and makes it publicly available. We also protect the data from workstation to destination through the use of a Transport Layer Security (TLS) encryption with a minimum key length of 256 bits. We review the privacy policies of countries around the world and make sure our controls comply with the most restrictive for data transferred and stored in the U.S. To attest to the efficacy of the controls, we have been self-certified in the EU-US Safe Harbor program since 2011 and in 2016 we joined the replacement for Safe Harbor – Privacy Shield.

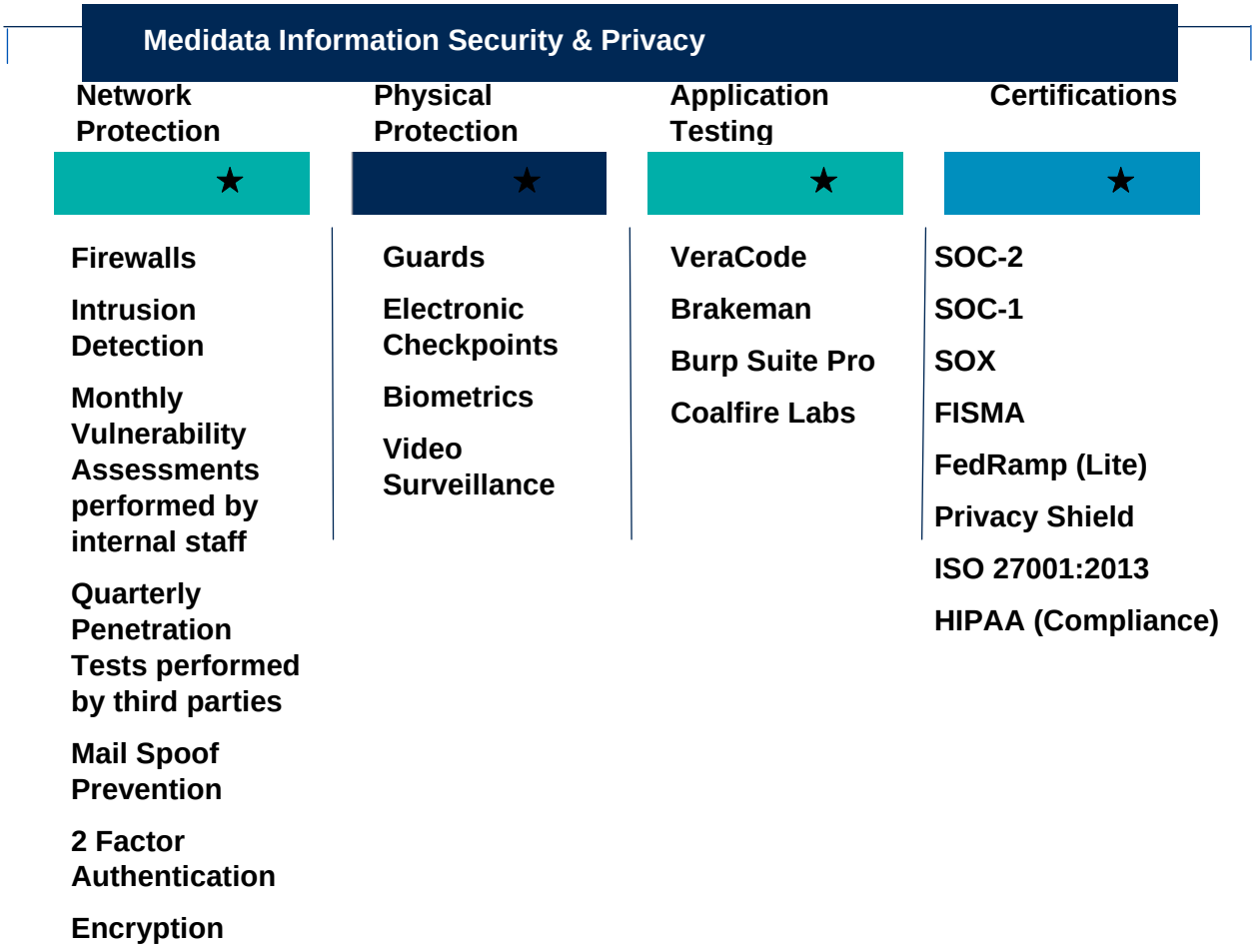


Figure 2. Data Privacy

Certifications and Accreditations

ISO 27001:2013

ISO 27001:2013 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. This is a widely recognized international security standard in which Medidata clients showed significant interest. Certification in the standard requires us to:

- Systematically evaluate our information security risks, taking into account the impact of company threats and vulnerabilities
- Design and implement a comprehensive suite of information security controls and other forms of risk management to address company and architecture security risks
- Adopt an overarching management process to ensure that the information security controls meet the our information security needs on an ongoing basis

The key to certification under this standard is the effective management of a rigorous security program. The Information Security Management System (ISMS) required under this standard defines how we continually manage security in a holistic, comprehensive way. The ISO 27001:2013 certification is specifically focused on the Medidata ISMS and measures how our internal processes follow the ISO standard. Certification means a third party accredited independent auditor has performed an assessment of our processes and controls and confirms we are operating in alignment with the comprehensive ISO 27001:2013 certification standard.

SOC 2 Type 2

Medidata publishes a Service Organization Controls 2 (SOC 2) report. This audit is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II report. The audit for this report is conducted in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402) professional standards. This dual-standard report can meet a broad range of auditing requirements for U.S. and international auditing bodies. The SOC 2 report audit attests that Medidata data center control objectives are appropriately designed and that the individual controls defined to safeguard customer data are operating effectively. Our commitment to the SOC 2 report is ongoing, and we plan to continue our process of periodic audits.

SOC-1 Type 1

Medidata published its first SOC1 Type 1 report for our “Medidata Payments” application in 2017. SOC-1 Type 1 reports are examination engagements performed by a service auditor (CPA) in accordance with Statement on Standards for Attestation Engagements (SSAE) 16, *Reporting on Controls at a Service Organization,* to report on the suitability of the design of the controls at a service organization that are likely to be relevant to an audit of a user entity’s financial statements. **Use of a SOC 1® report is restricted to existing user entities (not potential customers) and their auditors**.

FISMA / FedRAMP

Medidata enables U.S. government agency customers to achieve and sustain compliance with the Federal Risk and Authorization Management Program (FedRAMP) and the Federal Information Security Management Act (FISMA). The FedRAMP assessment process requires a standard approach to security assessment, authorization and continuous monitoring for cloud products and services which are FISMA compliant. FISMA requires federal agencies to develop, document, and implement an information security system for its data and infrastructure based on the National Institute of Standards and Technology Special Publication 800-53, Revision 4 standard (as modified by FedRAMP). FISMA Certification and Accreditation requires Medidata to implement and operate an extensive set of security configurations and controls. This includes documenting the management, operational and technical processes used to secure the physical and virtual infrastructure, as well as the third-party audit of the established processes and controls. Medidata is evaluated every year to maintain our FISMA authorization for Software as a Service.

Privacy Shield

The EU-U.S. Privacy Shield imposes strong obligations on U.S. companies to protect Europeans' personal data. It reflects the requirements of the European Court of Justice, which ruled the previous Safe Harbor framework invalid. The Privacy Shield requires the U.S. to monitor and enforce more robustly, and cooperate more with European Data Protection Authorities. It includes, for the first time, written commitments and assurance regarding access to data by public authorities.

What will it mean in practice?

- For Medidata Solutions
  - Self-certify annually that we meet the requirements.
  - Display a privacy policy on our website.
  - Reply promptly to any complaints.
  - (If handling human resources data) Cooperate and comply with European Data Protection Authorities.
- For European Clients of Medidata Solutions
  - More transparency about transfers of personal data to the U.S. and stronger protection of personal data.
  - Easier and cheaper redress possibilities in case of complaints —directly or with the help of your local Data Protection Authority.

FIPS 140-2

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. To support customers with FIPS 140-2 requirements, Medidata Private Cloud VPN endpoints and TLS-terminating load balancers in Medidata (U.S.) operate using FIPS 140-2 validated algorithms. Operating in FIPS-140-2 compliance mode does require comparable capabilities at the user browser side of the connection. While we do not employ FIPS 140-2 certified hardware, we do use the comparable make and model with fully approved FIPS 140-2 software.

HIPAA

Medidata enables covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) to leverage the secure Medidata environment to process, maintain, and store protected health information.

Physical Security

Non-descript buildings

Systems are housed in non-descript buildings that provide no indication that Medidata computers are within.

Uniformed Guards

The buildings we use for most of our data centers have uniformed guards at the entrances checking identification badges. All visitors to Medidata space must wear a visitor nametag and be escorted within the Medidata space. In our Cincinnati location uniformed guards are not used, but staff can monitor the modest data center at this location.

Photo-ID Smart Cards

Our data centers employ photo-ID cards to gain access to the database server rooms. In addition to being a positive identification tool, these ID cards also operate electronic door access locks. Cincinnati has not been upgraded to photo-ID badge access due to the limited data present at this location.

Biometric Door Locks

Outside of our server room access doors we have a biometric finger scanner that must be used in conjunction with a PIN code and the photo-ID smart card to gain access. Cincinnati does not employ biometric access.

Video Surveillance

Anyone approaching any of our data centers is recorded on a video surveillance system; the video is stored forever as well as constantly monitored by our skilled Network Operations Center staff 24x7.

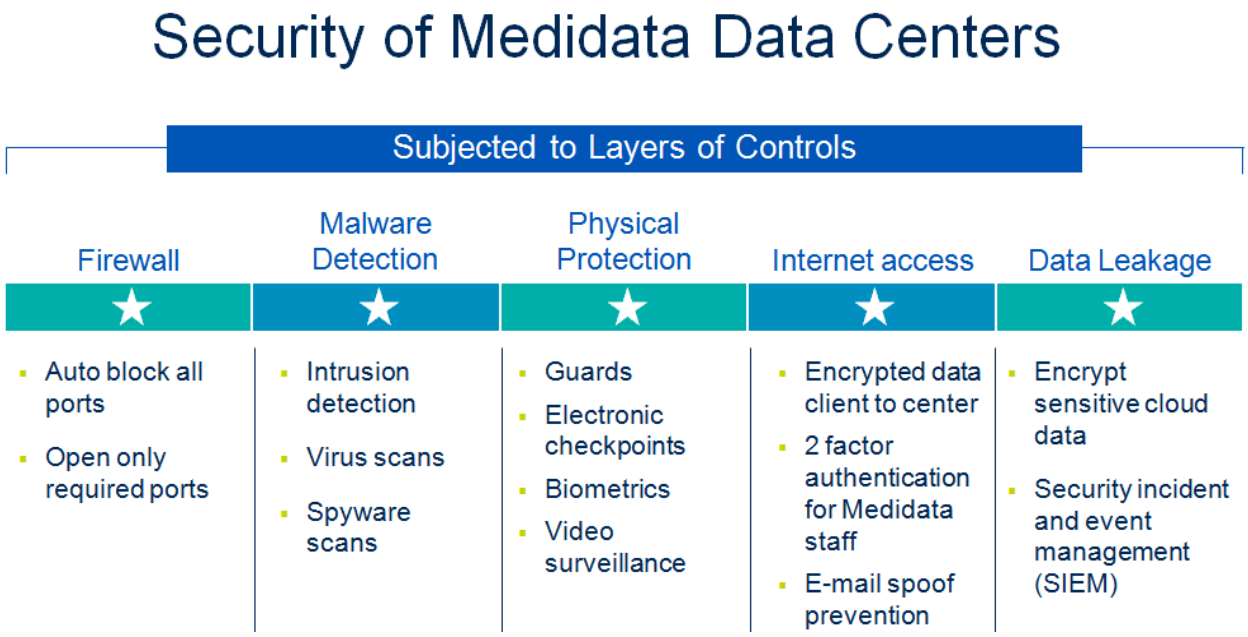


Figure 3. Data Center Security

Network Security

Palo Alto Networks PA 5060 Firewall, Virus Scan, & IDP
Certified: [EAL4+, FIPS 140-2, USGV6, UC APL]

Firewall

Medidata provides a comprehensive firewall solution. The inbound firewall is configured in a default deny-all mode except for ports 80 (HTTP) and/or port 443 (HTTPS). The outbound firewall is in a default deny-all mode. The firewalls are updated with the most current definitions available on scheduled basis consistent with our change management procedures. Firewalls are configured to provide OSI model layer 2 (Data Link) through layer 7 (Application) security.

Intrusion Detection & Prevention

An Intrusion Detection System (IDS) was the logical next step for Medidata after deploying firewall technology at the network perimeter. Medidata's IDS offers protection from both external and internal attackers—where traffic doesn't go past the firewall at all. Our systems use signature analysis mechanisms to analyze all traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization. Application and network traffic signature pattern matching is used to identify potential security weaknesses. Protocol anomaly traffic detection analyzes network traffic for known attacks and variations of those attacks. Updated network traffic signature files are automatically implemented upon release by the vendor.

Information Security

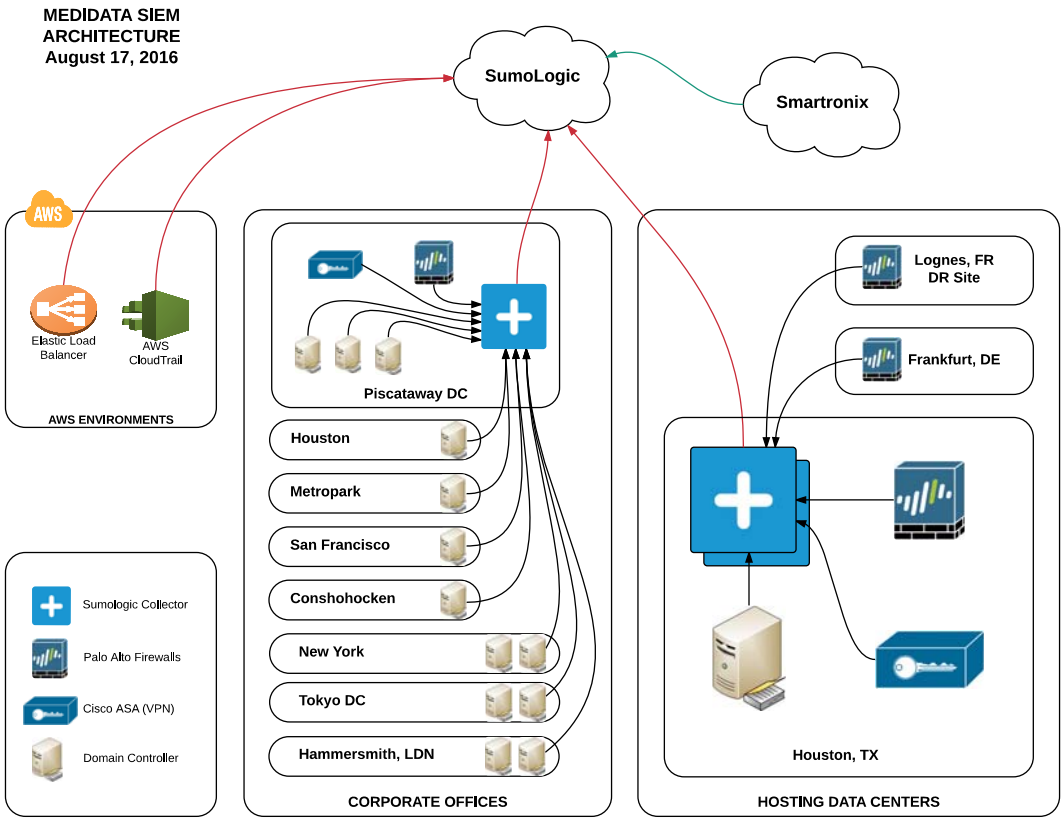
Virus, Spybot, Spam Scanning

In addition to our IDS and Firewall, Medidata uses a range of scanning tools to further sanitize all data prior to it traversing our data center networks. These scanning tools notify us in the event something malicious has made it through our defenses and may attempt to access our systems. Medidata network security lives by the old saying, “An ounce of prevention is better than a pound of cure.” In this case, a virus/Spybot scan is the prevention.

Security Management

Security Incident and Event Management (SIEM)

- SumoLogic SIEM System collects log and event data from all network devices and performs true real-time correlation and notification 24x7
- Enables Medidata to automatically take action against threats
- Automates security audits using over 120 customizable, out-of-the-box checks based on standards from NSA, NIST and SANS
- Detects data leakage
- Analyzes firewall configurations and logs to isolate redundant and unused rules and objects
- Models how a new rule, or change to an existing one, will impact our firewall policy—without touching production devices
- Scans our inventory for high-risk firewalls and assesses our risk profile in minutes
- Captures audit events:
    - Logon (unsuccessful and successful) and logout (successful)
    - Unauthorized access attempts to files (unsuccessful)
    - Application and session initiation (unsuccessful and successful)
    - System startup and shutdown (unsuccessful and successful)
    - System administration actions
    - Security personnel actions
    - Data transfers (from, to, time, size and correlation to norms for that URL)



Routers

Access Control Lists (ACL) are used and managed to segregate web, application and database servers. Communication between servers is accomplished via an approved ACL address and in conjunction with authentication.

Encryption during data transmission

All data is transmitted from the client site through the Internet to one of our data centers located in the continental United States. To maintain the highest level of confidentiality and meet our Privacy Shield requirements, all data is encrypted with at least 256 bits of key in a TLS. We can also configure the transmission to meet FIPS 140 requirements, if needed.

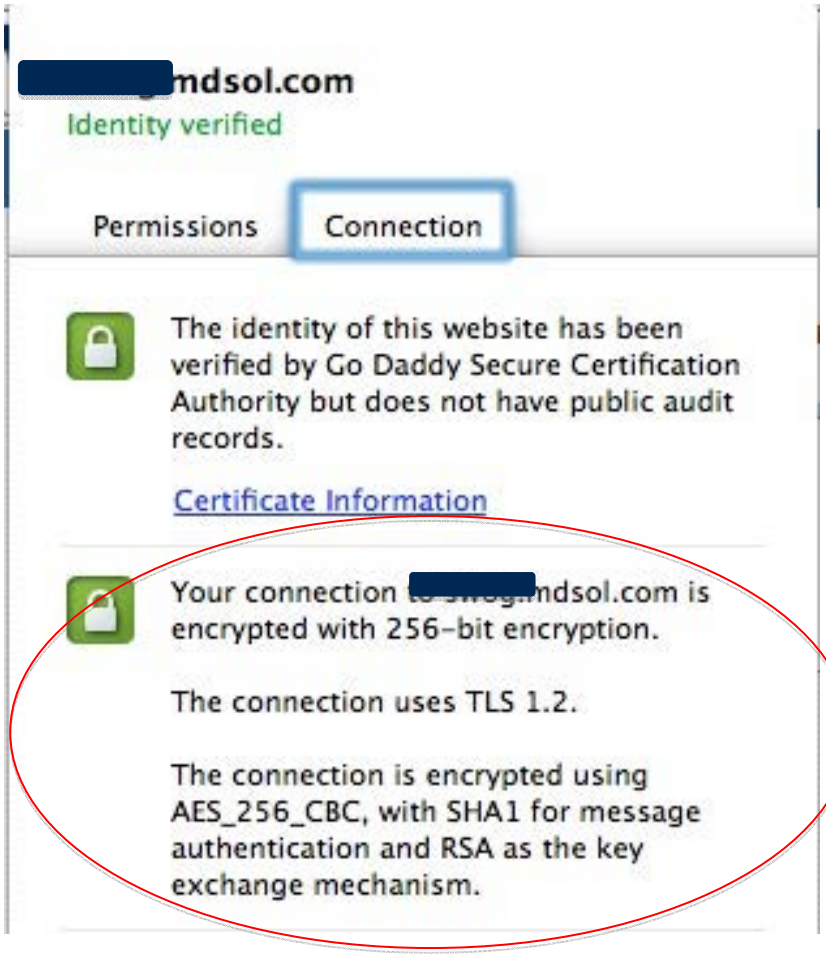


Figure 4. Transmission Encryption

System Administration

Administrators with a business need to access the servers are required to use multi-factor authentication to gain access to host servers. These servers are systems that are specifically designed, built, configured and hardened to protect our clients' separation of data. All such access is logged and audited. When an employee no longer has a business need to access the servers, the privileges and access to these hosts and relevant systems are revoked.

Cloud Security

We use Amazon Web Service (AWS) as our cloud computing service. AWS works with Medidata's traditional data center for some of our processing. To assure that our customer data is secure in AWS we have conducted a comprehensive assessment of the AWS security.

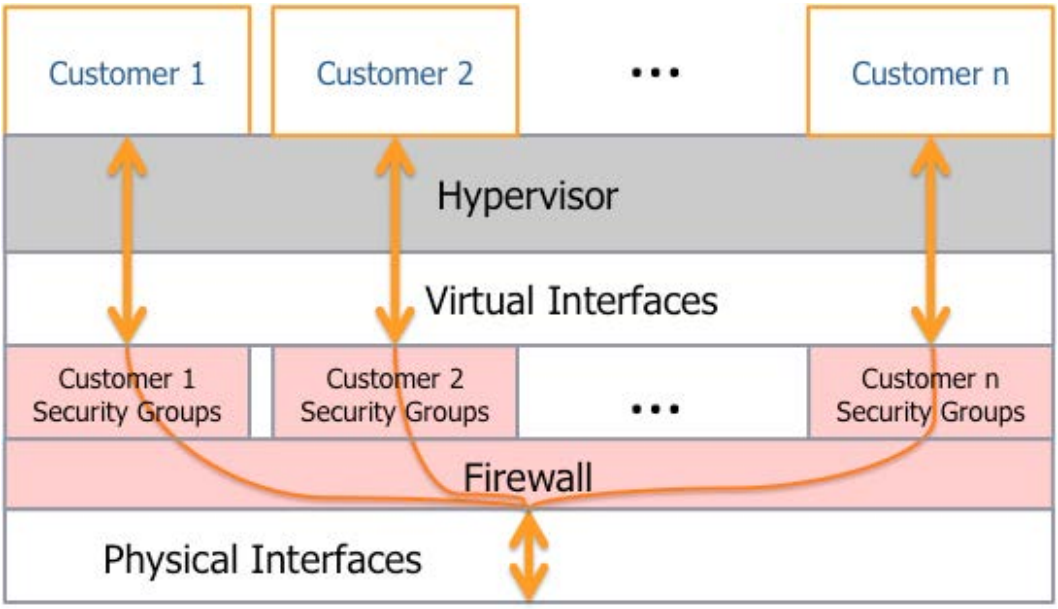
- Physical Security: Military grade with multiple layers of manual and automated controls
- Logical Security: Stellar

    1) AWS is subjected to reviews by a large number of clients, including U.S. Department of Health and Human Services (HHS)

2) AWS is monitored 24x7 by a dedicated security team
3) With a plethora of clients, they must implement security to the highest bar to cover all
4) AWS has an annual SOC-1, SOC-2 and SOC-3 audit by Ernst & Young
5) Medidata supplements AWS security with 24x7 SIEM monitoring of our clients and encryption

- Virtualization Security: Industry Best Practice

1) While data is being processed, different instances running on the same physical machine are isolated from each other via the Xen hypervisor.
2) The AWS firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance's neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts.
3) The physical RAM is separated using similar mechanisms.
4) DDoS protection
5) MITM (Man in the Middle) attack protection
6) IP Spoofing prohibited at host OS level
7) Packet Sniffing Promiscuous mode is ineffective at hypervisor level
8) Configuration Management employed for changes



Used with AWS permission

Figure 5. AWS Virtualization

Storage Device Decommissioning

When a hard drive reaches the end of its useful life, Medidata procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. Medidata uses the industry standard techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. Until a device

can be decommissioned using these procedures, the device is physically stored in a locked secure environment in the server room.

Configuration Management

Emergency, non-routine and other configuration changes to existing Medidata infrastructure are authorized, logged, tested, approved and documented in accordance with industry norms for similar systems. Medidata communicates with our customers via telephone or email prior to a software update or infrastructure repair in order to minimize any impact on the customer and their use of the services. Medidata applies a systematic approach to managing change so that changes to customer services are thoroughly reviewed, tested, approved and well communicated.

Security Patches and Incident Response

Information Security alerts are escalated from our Security Operations Center (SOC) or Global Network Operations Center (GNOC) System to the ISP Staff and then to the Corporate Information Security Officer (CISO) and senior management. Our incident response policy details the circumstances that would trigger a customer alert and how our customers are to be informed. The policy also references the response for controlling the lifecycle of a security incident. The plan describes the stages and actions associated with those stages, from identification, preparation and containment to restoration, notification and post-mortem of an event and or incident. Under reasonable timeframe following a detection, Medidata will confirm and perform impact analysis of the security incident and inform Medidata clients through communication channels established in the Services Agreement. All issues are tracked in an online, database-driven issue management system. Senior level management ensures information security is part of Medidata's culture.

In general, security issues that have a high threat of exploitation, in combination with a vulnerability type rated critical by our internal Nessus scanning tool or authoritative external sources, will be addressed with countermeasures within 30 days. Permanent fixes will usually be implemented within 90 days. However, no patches are applied until we coordinate with our network of partners to ensure full testing and agreement. Recent worldwide issues like Heartbleed and Shellshock are examples of a high threat and critical vulnerability that were remediated within hours.

Database Security

All data is backed up on a regular basis. Full backups are performed at least weekly, with incremental backups performed daily. Critical clinical study data is backed up every 15 minutes. The backed-up data is transferred to tape in an encrypted format and stored at an off-site location provided by Iron Mountain. Rave clinical data is also fully duplicated electronically each day to our disaster recovery backup facility.

Client information in our Rave Database is segregated through the use of virtualization. Each client is virtualized and runs on a separate database. The other elements of our platform execute within the Amazon Web Service in a

Figure 6 Virtual Databases

multitenancy environment where multiple customers share the same application, running on the same operating system, on the same hardware, with the same data-storage mechanism. The distinction between customers is achieved during our application design, thus customers do not share or see each other's data.

Business Continuity and Disaster Recovery

Business Continuity (BCP) and Disaster Recovery (DRP)

Business Continuity and Disaster Recovery Planning are viewed as a dual approach for the entire business. As such, the activities involve business management from all functional and business areas, including administrative, human resources, IT support functions, and DRP for customer products. The BCP Team is responsible for overseeing the development of the internal business program, while our Service Delivery department oversees the client disaster recovery planning. Both departments ensure that senior management invests sufficient resources into planning, monitoring and maintaining the plans.

Medidata's Disaster Recovery/Business Continuity Plan defines plans, procedures and guidelines for the company in the event of disaster. Specifically, the plan establishes procedures for recovering business operations, internal data, systems and critical internal functions to maintain Medidata in the face of unexpected events.

The plan has the following primary objectives:

- To identify, assess, and prioritize Medidata vulnerabilities to emergencies or disasters and the resources available to prevent or mitigate, respond to, and recover from them.
- To outline short-, medium- and long-range measures to improve Medidata's capability to respond to and recover from an emergency.
- To provide for the efficient utilization of all available resources during an emergency.
- To ensure the continuity of operations of Medidata in times of emergency or disaster situations.

Medidata performs traditional backup as well as site-to-site electronic replication of data to protect client data in the event of a disaster. There is a dedicated disaster recovery site distant from the production data centers. BCP/DR testing is performed annually.

Plan Components

The Plan is comprised of a number of elements; all working in concert to assure that Medidata meets all known industry and regulatory requirements.

Business Continuity Plan (BCP)

- Crisis management
- Business center relocation
- Alternate workplace options
- Comprehensive contracts with service providers

Pandemic Response Plan (PRP)

- Education
- Preventative actions to contain pandemic
- Responsibility, Governance
- Policies & Procedures

Disaster Recovery (DR)

- Annual exercises
- Documented recovery procedures
- Comprehensive contracts with service providers

Disaster Recovery (DR)

Medidata has a disaster recovery plan in place, which covers: alert lists, team responsibilities, recovery and notification procedures, resumption plans, installation tasks, work area checklists and preparedness procedures. Medidata's support, product and account management teams would notify all customers of unscheduled downtime via email initially, via phone if the situation escalates. In conjunction with the senior management team, the service delivery team designs and maintains the plan.

In the event of a disaster limited to the data center, work would continue at one of the Medidata disaster recovery sites. All production, DR and testing facilities are fully supported on redundant power feeds and Uninterruptible Power Supplies (UPS). These will provide full power until diesel generators are brought online (typically within 12 seconds).

Policies

POL-IS-001 Information Security

This policy addresses how our systems should be configured to provide the confidentiality needed to meet various global privacy regulations. Legislation such as EU 95/46, PIPA, FISMA, and others place legal requirements on Medidata to protect personal privacy and ensure the confidentiality and security of clients' information.

POL-CORP-006 Corporate Incident Management Policy

The policy directs the creation and maintenance of plans to enable Medidata to continue its mission and commitments by preventing and minimizing the impact of discontinuity incidents. As a result of this policy, Medidata created a corporate incident management plan that details our critical corporate systems, restore actions and restore timelines. This plan obsoleted the Business Continuity Plan on April 29, 2016 and is managed by our facilities team.

POL-ISP-004 Organizational Security Policy

This policy details the Medidata organization for the protection of information both internally and externally. For example, an internal control would allocate information security responsibilities, whereas an external control would address security in third-party service agreements. Organizational Security ensures business continuity and minimizes business damage by preventing and minimizing the impact of security incidents.

POL-IS-005 Physical and Environmental Security Policy

The purpose of this policy is to provide guidance that limits access to every office, server room and other Medidata work area containing sensitive information. We use a variety of controls to satisfy the requirement to physically restrict access to those people with a business need. This policy also reinforces our requirement for environmental controls that are resilient and flexible to enable uninterrupted service to our customers.

POL-IS-006 Asset Classification & Control Policy

The purpose of this policy is to detail the essential requirements for asset classification and control. These measures are needed to help protect Medidata information from disclosure, unavailability or corruption following an error by staff or compromise by an outsider.

POL-IS-007 Information Security & Privacy Policy Regarding Staff Members

The purpose of this policy, created in concert with our HR department, provides guidance on Information Security standards applicable to the Medidata staff. We ensure that our staff understand and acknowledge acceptable use of the data we manage.

POL-ISP-008 Network and Computer Operations Security Policy

The purpose of this policy is to identify the elements of a good network operations security policy, explain the need for network information security and specify the various categories of network and operations information security. This document establishes an overarching network operations security policy for Medidata.

POL-ISP-009 Access Control Security Policy

The purpose of the Access Control Security Policy is to define a set of computer connection rules, designed to minimize the exposure to Medidata computer systems from destruction, theft and loss of data (e.g. confidentiality and privacy), disruption to business operations, and damage to Medidata's image which may be caused by unauthorized use of its electronic resources.

The Access Control Security Policy defines the roles of servers, Internet servers and client computers when connected to Medidata's network and defines permissible communications flows between them.

POL-IS-010 System Development and Maintenance Security Policy

Medidata holds large amounts of information. It has a variety of statutory, contractual, regulatory and internal obligations to process this information in a way that assures its confidentiality, quality and availability at all times. Security can be compromised by vulnerabilities or inadequacies in the design and maintenance of these systems. Information systems in this policy include infrastructure, commercial off-the-shelf packages, external systems, operating systems, business applications and user developed systems, in any format (e.g., paper or electronic).

Basic security requirements should be identified, justified and built into information systems from their conception and design, through creation and maintenance. This can be achieved by sound risk assessment and mitigation at every stage.

POL-ISP-011 Responding to Security Incidents and Malfunctions

The purpose of this policy is to provide general guidelines for how to handle a data breach before an intrusion has occurred. Medidata is committed to establishing standard guidelines for responding to a computer security incident involving Medidata's systems. Attacks are many and varied; they change constantly; and responding to them can involve a varied assortment of legal and technical issues. This policy is intended to provide an outline of the issues involved and the practical guidelines to prevent attacks and mitigate damages. Medidata conducts an annual data breach exercise to evaluate the effectiveness of our plans.

POL-ISP-013 Compliance Security Policy

The purpose of this policy is to be compliant with the regulatory regimes in which Medidata operates, while encouraging innovation. Medidata's aim is to ensure that effective arrangements are in place to enable us to comply with our regulatory and international law obligations with regard to Information Security and Data Privacy. We work closely with legal and regulatory experts within Medidata as well as outside subject matter experts.

POL-ISP-014 Mobile Device Security Policy

This policy addresses the requirements for Medidata staff to use a secure agent, OKTA, on any mobile device like a smart phone or tablet device. This agent segregates Medidata corporate information and encrypts it on the device. The agent also permits Medidata to delete that data remotely.

Patient Cloud Security

As medical devices become more interconnected and interoperable, they can improve the care patients receive and create efficiencies in the clinical trial system. While designing our systems, Medidata carefully considers possible cyber security risks that might connect to medical devices, and we develop plans to manage system controls or software updates. Our guidance in this area originates in NIST SP 800-53 and NIST 800-82. These same NIST publications were the basis of the FDA recommendations.

The approach to securing the Patient Cloud software differs from the rest of the Clinical Cloud software since part of it is its executing on a mobile device. The Medidata security team has taken the following steps to assure Patient Cloud's safety:

- Reviewed the design of the application and ensured that all communication to/from the device is encrypted. Due to the strength of the encryption we obtained an evaluation and approval from the US Government to export the encryption built into our software.
- We had the product penetration tested by a third party, Coalfire Labs, to identify any security weaknesses. None were found in the iOS version and one was found and corrected in the Android version.
- The operational architecture was reviewed during several design meetings to make sure all information was being protected from device to storage in our data centers. The data center security for all of our products is covered in this white paper.

Medidata Imaging Security and Privacy Controls

In April of 2016, Medidata acquired Intelemage®, the medical image management and workflow provider. The policies and procedures outlined in this White Paper generally apply to Medidata's current management of Intelemage, now known as "Medidata Imaging". The Medidata Imaging products (e.g., InteleGrid®), however, are not physically integrated with Medidata's other offerings. The following additional information is specific to the Medidata Imaging products.

Security controls.

Medidata's Imaging offerings operate two data centers, one in Cincinnati, Ohio and another in Phoenix, Arizona. Phoenix is the primary Tier 4 data center, which is an i/o data center colocation provider. Both data centers have annual Service Organization Control (SOC1) audits focused on controls for physical security and environmental maintenance. Further information concerning audits is available in our Regulatory and Audit Policies.

(Starting in 2017, these data centers will also include ISO 27001:2013 and FISMA certifications. Medidata Houston and New York currently have these certifications, so expanding the scope to include Medidata Imaging is a straightforward and logical extension to our certification strategy.)

The Medidata Imaging security controls strategy is based on a number of well-established security models, including ISO 27001:2013, NIST 800-53 and CoBIT. The specific areas of controls include:

1. Incident management
2. Change control
3. Encryption (in transit, and at rest)
4. Identity and access management
5. Vulnerability assessment and remediation
6. Configuration management
7. Software and hardware lifecycle
8. Physical security
9. Security training and education

10. Disaster recovery and business continuity.

Additionally, Medidata Imaging's information security management system (ISMS) is reviewed annually as part of Medidata's commitment to continuous improvement.

PHI and HIPAA Applicability

NOTE: The following information about electronic protected health information ("PHI") as defined under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is provided for informational purposes to Medidata Imaging Customers, and is not legal advice.

PHI is defined as a set of eighteen identifiers that, if present, allow for the identification of a specific individual's health information. Pursuant to HIPAA and related regulations, PHI must be protected under certain circumstances, including the requirement for entities handling PHI to execute Business Associate Agreements ("BAAs").

With regard to Medidata Imaging, HIPAA is not applicable where:

1. PHI is not collected (does not reach Medidata Imaging servers);
2. PHI is collected under a patient authorization (e.g., as part of the Informed Consent in a clinical trial); or
3. PHI is collected for purposes of patient treatment (the patient treatment exception)

In further detail regarding whether PHI is collected (#1 above), Medidata Imaging's offerings may be configured to avoid the collection of PHI in the first instance. The offerings provide an "applet" for installation on customer systems; the applet can then be configured to perform PHI redaction (e.g., of DICOM header information) prior to the secure transfer of any data to Medidata Imaging. The result is that the data is no longer PHI when it is securely transferred to Medidata Imaging's servers.

In addition, certain image types do not contain PHI, regardless of their DICOM header information; such images would not be subject to HIPAA requirements.

Healthcare sites and other entities who contract with sponsors or contract research organization (CROS) (an Medidata Imaging Customer") should direct any further questions regarding Medidata Imaging security or privacy controls to the Medidata Imaging Customer.

Medidata Regulated Content Management (RCM)

Medidata acquired CHITA, now known as Medidata RCM, in February 2017. RCM provides users with the ability to create, store, view, edit and jointly work on both regulated and non-regulated content in a single application. The security control strategy for RCM is based on ISO 27001:2013 and as such the policies and procedures outlined in this White Paper also apply to Medidata's management of RCM.

Medidata RCM currently processes in two Equinix co-location data centers, one in San Jose, CA and the other is Ashburn, VA. Infrastructure support services at these data centers are provided by Synoptek. Equinix data centers have annual Service Organization Control (SOC-1 and SOC-2) audits and are ISO 27001 certified.

Medidata is planning to relocate RCM processing to its data center in Houston, Texas by the 3rd quarter of 2017.

Frequently Asked Questions

1. Is the Amazon Web Service as safe and secure as a traditional data center?

Security in the cloud is similar to security in Medidata's organic data centers. From the client perspective there are no physical servers or storage devices; both use software-based security tools to monitor and protect the flow of information into and out of the computing resource.

How is it the same?

- The security tools and techniques Medidata uses in our data center are used in the cloud.
- The same operating system (OS) and Medidata applications are used and updated with the latest security patches, backups of your data, anti-virus, intrusion detection and security incident and event monitoring (SIEM) tools.
- Medidata sets up subnets in order to separate environments that should remain isolated from one another—for example, we separate our development and test environment from your production environment—and then configures network Access Control Lists (ACLs) to control how traffic is routed between them.
- We have multiple users—like developers, testers and administrators—and provide them with their own unique credentials for accessing AWS resources. We even require them to use multifactor authentication.
- We use network monitoring and security management tools from SumoLogic to collect and analyze logs and network traffic information from our resources.
- Medidata performs vulnerability scanning on our systems.
- We are also on the verge of establishing a Virtual Private Cloud (VPC) from our data center to our cloud resources to add an additional layer of transmission protection. In the VPC our clients will be operating in a private subnet, not the traditional public subnet.

How is it different?

- Our administrators/developers manage AWS resources remotely instead of locally.
- We use software-based security mechanisms instead of hardware-based solutions.
- Instead of racking and stacking, our IT support folks will be launching and configuring.
- Authentication using digital signatures and crypto keys is required for every Medidata application running in AWS.
- Instead of just a firewall protecting all of your resources, every virtual server also contains a security groups that act like a secondary firewall.
- The software is hardened through a baseline image of our virtual server (EC2 instance). We create an Amazon Machine Image (AMI), which is a template that includes our OS, libraries, applications, configurations, etc. We can then save that baseline image and have it automatically loaded on every new instance launched.
- Operating in a SaaS model versus an onsite data center is physically different. But AWS data centers must meet Medidata's specific security requirements and possess certifications like SOC2, ISO 27001 and Safe Harbor.

Security Advantages of the Cloud

- **Instant visibility into our inventory**
  The first step in securing assets is to know what they are. With tools like AWS Config and resource tagging, we can always see exactly what cloud assets we're using at any moment.

- **Additional security tools**
  AWS provides Medidata with a list of security tools specifically designed to monitor and configure the AWS virtual space that we use.

- **Significant DDoS protection**
  AWS's size and scale makes them more capable and DDoS resilient. The AWS infrastructure is equipped to handle extremely large amounts of traffic; and when we use AWS services like ELB, Auto Scaling, CloudWatch and CloudFront, Medidata can architect a highly available system that can help weather DDoS attacks.

- **Security economies of scale**
  Medidata and its customers reap the same security benefits as the largest corporations when we're in the AWS cloud. In addition to Medidata's dedicated security team, AWS also has a large, dedicated security team and a variety of systems and tools that continuously monitor and protect the underlying cloud infrastructure.

- **Continuous hardware replacement and upgrade**
  AWS is always improving their infrastructure. They replace end-of-life hardware with the latest processors that not only improve performance and speed, but also include the latest secure platform technology, like the Intel AES-NI encryption instruction set, which significantly speeds up the execution of the AES algorithm that Medidata uses.

2. Why does Medidata use FTPS instead of SFTP?

The two industry standard protocols available for Secure FTP transfers are SFTP (FTP over SSH) and FTPS (FTP over SSL). Both SFTP and FTPS offer a high level of protection since they implement strong algorithms such as AES and Triple DES to encrypt any data transferred. Both options also support a wide variety of functionality with a broad command set for transferring and working with files. So the most notable differences between SFTP and FTPS is how connections are authenticated and managed.

With SFTP a connection can be authenticated using just a user ID and password to connect to the SFTP server. SSH keys can also be used to authenticate SFTP connections in addition to, or instead of, passwords. With key-based authentication, a user would need to generate a SSH private key and public key beforehand. When you connect to the SFTP server, your software would transmit your public key to the server for authentication. If the keys match, along with any user/password supplied, then the authentication will succeed.

With FTPS a connection is authenticated using a user ID, password and certificate(s). Like SFTP, the users and passwords for FTPS connections will also be encrypted. When connecting, your FTPS client will first check if the server's certificate is trusted. The certificate is considered trusted if either the certificate was signed off by a known certificate authority (CA), like VeriSign, or if the certificate was self-signed (by your partner) and you have a copy of their public certificate in your trusted key store.

In summary, SFTP and FTPS are both very secure with strong authentication options. However, since FTPS is much safer to port through our firewall, it fits our overall security architecture, and we are seeing an increasing percentage of clients adopting FTPS, FTPS was the clear winner for our secure FTP needs.

3. *What third-party products are used for processing?*

Product:	**Google Analytics**
Category:	Site Usage Tooling
Medidata Use:	Tracking website usage. It provides information on user location, language they are requesting, some performance information, what is done on our site, length of connection, etc. Google Analytics encrypts its data at rest and stores this data in its own secure data centers.

Product:	**SocketLabs**
Category:	Email as a service
Medidata Use:	User data that we send to SocketLabs includes: a) study and study group names; b) the contents of the custom email property of a study and study group. This is user configurable but it is typically just instructions on signing up and more information about the pharmaceutical company and the study; c) email addresses of all of our users; (d) the names of users who are administrators; (e) activation codes for all user accounts. All of the data that we send to SocketLabs is also put into emails, so it is data that can be handled by servers anywhere in the world, no matter which email provider is used. Innocuous data includes: the Medidata logo, and boilerplate language about being invited to a study and changing your email address.

Product:	**Newrelic**
Category:	Application performance management
Medidata Use:	Medidata uses Newrelic to gather performance metrics on our deployed applications, both in production and non-production environments. These metrics include transaction response time, web traffic throughput and Apdex score. These metrics are broken down by deployed instance and are available both for live traffic and historical data. We also capture slow transactions with Newrelic and detailed information on these slow transactions stored in the Newrelic system, including a comprehensive list of the calls (both web service and database) made during the slow request. In order to collect these data from our servers, we install Newrelic collector daemons on our servers. Newrelic hosts our data in its own secure data centers. Also, data sent to Newrelic in secured in flight with TLS.

Product:	**SumoLogic**
Category:	Log aggregation and analytics
Medidata Use:	Most of Medidata's suite of applications send their application, web server and app server logs to SumoLogic on a periodic basis (generally new log lines are sent to SumoLogic every few seconds). We employ SumoLogic's collectors on our servers to buffer and send logs to SumoLogic. We ensure that sensitive information, such as user passwords, third-party credentials, is not written to our logs, either on server or in SumoLogic. SumoLogic sends our historical log files to AWS's Simple Storage Service (s3) on our behalf so we can undertake analysis of this historical data with, e.g., map-reduce tools if need be. SumoLogic also has a UI and API for log analysis, alerting and custom dashboarding.

4. *Which pieces of the platform are Single Instance Multi-tenant (SIMT) and which are Multi Instance Single-tenant (MIST)?*

Product	SIMT	Datastore	Location
Balance	Yes	mySQL	AWS
Cloud Admin	Yes	MySQL	AWS
Coder	Yes	SQL Server	AWS
CSA	Yes	PostgreSQL	AWS
CTMS	No	mySQL	AWS
Grants Manager	Yes	SQLServer	AWS
Imaging	Yes	MySQL	Medidata Data Center
iMedidata (including authMedidata)	Yes	mySQL and PostgreSQL	AWS
Insights	Yes	SQLServer	Medidata Data Center
MCC Platform services (mAudit, etc.)	Yes	AWS s3	AWS
Patient Cloud	Yes	mySQL	AWS
Payments	No	mySQL	AWS
Rave (incl. Rave Web Services, SAS on Demand, ODM Adaptor, File Transfer, JReview etc.)	No	SQLServer	Medidata Data Center
Rave Ad-Hoc Reporting (BO4)	Yes	SQL Server	Medidata Data Center
RaveX	Yes	SQL Server	Medidata Data Center
RCM	Yes	mySQL	Equinix
Safety Gateway	Yes	SQLServer	Medidata Data Center
SQM	Yes	SQLServer	Medidata Data Center
TSDV	No	SQLServer	AWS