WHITE PAPER

HIPAA Compliance and Third-Party Records Partners: Today's Security Landscape and Auditing Best Practices

Using SOC 2 Type II Audit Reports and Checklists to Validate Compliance and Identify the Most Security-Conscious Records Partners

ontellus

In today's information economy, companies across every industry are faced with the imperative to secure information assets, creating an enterprise risk management strategy that establishes comprehensive information governance. With cyber security threats on the rise, insurance claims departments, in-house counsel, and law firms quickly become a focus area for company data privacy and security leaders. These departments and their third-party partners frequently exchange documents containing personally identifiable information (PII), opening the door to costly data breaches, non-compliance fines, regulatory penalties, as well as civil litigation. But the collection and review of personal health information in medical records are core functions of legal professionals and insurance adjusters working to evaluate claims and build case strategy. So, how should professionals respond?

This white paper explores the impact that HIPAA has on third-party records companies, best practices for auditing and evaluating partners, and how Ontellus is leading the industry in records security and innovation.

Healthcare organizations are the MOST TARGETED SECTOR with new sophisticated cyber-attacks emerging.

Healthcare Records: Targets and Threats

The sensitive nature of PII has made healthcare records a primary target for hackers and legal protections alike, particularly with the introduction of electronic medical records and health information systems. Ripe for medical identity theft, these documents contain private account numbers and financial data. Studies from Experian and the Ponemon Institute show that "while more organizations have put data protections and breach response plans into place, a level of complacency has set in that is preventing response readiness. Many are lagging in practicing and updating their response plans as well as keeping up with new types of attacks." As such, Experian predicted that in 2017 "healthcare organizations will be the most targeted sector with new sophisticated cyber-attacks emerging."[1]

Further emphasizing the importance of secure data exchange with third-party partners, Experian anticipates that "mega breaches will move on from focusing on healthcare insurers to focusing on other aspects of healthcare, including hospital networks."[1] Furthermore, as insurance companies, law firms, and records companies actively share healthcare records, new vulnerabilities are rising out of the increasingly mobile and remote workplace environment. More mobile applications, more cloud-based services, and more connected mobile devices combined with the number of different entities and their various, distributed networks that access protected information, are also increasing risks.[2]

Likewise, the routine nature of email as a primary means of sharing information also continues to pose a threat. Regulatory compliance rules as part of the Health Insurance Portability and Accountability Act (HIPAA) do not expressly prohibit email as a channel for sharing information, meaning that encrypted email applications and strict email policies can make the difference between protected and unprotected information.

[1] https://www.experian.com/assets/data-breach/white-papers/2017-experian-data-breach-industry-forecast.pdf

[2] https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf

How HIPAA Impacts Records Partners

HIPAA was America's response to the growing the need to protect health information, and HIPAA compliance rules protect the privacy and security of certain health information. Effective March 2013, HIPAA also regulates subcontractors and third-party service organizations (including records providers, copy services, and court reporting companies) that are hired to obtain, process, or store protected health information (PHI) for covered entities and business associates. Under the new rule, insurance carriers and law firms can be found liable for a breach of PHI due to a record partner's negligence. Risks include significant data breach costs, non-compliance penalties, unfavorable media exposure, and investigations conducted by federal and state authorities.

Thus, it is imperative that carriers and law firms perform thorough due diligence when selecting records partners. Under HIPAA, any provider that stores, transmits, or protects medical records must be compliant and have documented policies and procedures, including:

- Administrative Safeguards: Administrative actions, policies, and procedures that manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information
- Technical Safeguards: Technology elements, policies, and procedures that protect and control access to electronic PHI
- Physical Safeguards: Physical measures, policies, and procedures that protect a covered entity's or business associate's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion

DATA BREACHES: NOT IF BUT WHEN

No healthcare organization, claims department, nor law firm (regardless of size) is immune from a data breach, and studies show that it's not a matter of if but when. A Ponemon Institute study revealed that between 2014-2016, **nearly 90% of healthcare organizations surveyed had a data breach**, and nearly half (45%) had more than five data breaches in the same time period.[2] While the majority of these breaches were small, containing fewer than 500 records, the frequency and prevalence of breaches acts as a call to action.

Auditing Records Partners using the SOC 2 Type II Report

Given the HIPAA federal requirements, insurance carriers and law firms must evaluate their records partners to ensure their information management systems are compliant with HIPAA security and privacy rules. Audits are the most effective methodology for partner assessment, and auditing standards further simplify this task. Rather than conduct the audit themselves, most carriers and law firms require their records partners to undergo a standardized audit using an independent auditing firm. Audits generate reports that provide "reasonable assurances" about a record partner's data security controls and information governance.

Readers Tip: Records companies may state they are HIPAA compliant but often do not have the documentation and evidence to validate compliance. Auditing records partners is the ideal way to ensure records in your extended network are protected.

The American Institute of Certified Public Accountants (AICPA) is the authoritative guide on auditing standards. This entity created a standard for reporting on controls at third-party service organizations such as records partners. Audits including SSAE 16 (Statement on Standards for Attestation Engagements No. 16) and Attestations Standards Section 101 (AT-101) are international auditing standards that can be used to effectively validate HIPAA compliance.

The SSAE-16 and AT-101 audits include the creation of Service Organization Control (SOC) reports. There are several different types of SOC reports (SOC 1, SOC 2, SOC 3, as well as Type I and Type II) each with unique determinations. However, for the purposes of evaluating records partners and HIPAA compliance, SOC 2 reports are the most relevant report and thus will be the focus herein.

A Service Organization Control (SOC) 2 report is one of THE MOST EFFECTIVE ways a records partner can communicate information about its information security controls

SOC 2 Report Types and What They Evaluate

There are several types of SOC reports with varying areas of focus and degrees of depth, so it is important to note that SOC 2 reports are best for verifying HIPAA-compliant records partners. As the most stringent test, the SOC 2 Type II report is the gold standard for verifying HIPAA-compliant records partners.

SOC 2 Report: Designed for Service Organizations that Manage Client Information

A SOC 2 report is for service organizations that hold, store, or process their clients' information. The SOC 2 report was designed to allow service organizations to communicate information about their system description in accordance with a core set of principles and criteria called the Trust Services Principles and Criteria. This standard framework is highly respected in the records industry and was designed to address the risk and opportunities associated with information technology and records storage.

The specific SOC 2 evaluation criteria are:

- Security: The system is protected against unauthorized access, use, or modification
- Availability: The system is available for operation and use as committed or agreed
- Processing Integrity: System processing is complete, valid, accurate, timely, and authorized
- Confidentiality: Information designated as confidential is protected as committed or agreed
- Privacy: The system's collection, use, retention, disclosure, and disposal of personal information are in conformity with the commitments in the service organization's privacy notice and with criteria in the Generally Accepted Privacy Principles (GAPP)

The SOC 2 Type II report is THE GOLD STANDARD

The Difference Between Type I and Type II Audits

SOC 2 Type I: Point-in-Time Test

A Type I report is intended to cover the service organization's system description at a specific point in time (e.g. June 30, 2012)

SOC 2 Type II: Six-Month Audit Period Testing Operating Effectiveness

A Type II report not only includes the service organization's system description, but also includes detailed testing of the service organization's controls over a minimum six-month period (e.g. January 1, 20xx to June 30, 20xx)

In both a Type I and II report, the service auditor will express an opinion and report on the service organization as to:

1. The Fair Presentation of the System: Whether the service organization's description of its system fairly presents the service organization's system that was designed and implemented as of a specific date or the specified time period

2. The Design to Achieve Control Objectives: Whether the controls related to the control objectives stated in management's description of the service organization's system were suitably designed to achieve those control objectives - also as of a specified date or the specified time period

ONLY in a Type II report will the service auditor express an opinion and report on the service organization as to:

3. The Effective Operation throughout the Time Period: Whether the controls related to the control objectives stated in management's description of the service organization's system operated effectively throughout the specified period to achieve those control objectives

To summarize, the SOC 2 Type II report is the most stringent test for two reasons. First, it expands the evaluation to cover a six-month period, taking a deeper look into how effectively security controls perform over time. Second, it requires auditors to extend their evaluation beyond the intent of the system design (policies and procedure design), assessing how the system actually performed and operated throughout the six months. This demonstration test examines the policies in action, truly analyzing system functionality to prove that controls in place are effective in creating a secure environment.

Records partners are EQUALLY RESPONSIBLE for the safety and security of records and should be open in forthright in providing their information governance policies and practices for identifying HIPAA-compliant records partners, YET FEW partners have certifications.

Verifying Compliance with SOC 2 Type II Reports

A Voluntary Act. While HIPAA compliance is required, providing a SOC 2 Type II report is voluntary for records partners.

“It’s important to point out that records partners are not necessarily required by law to undergo an audit that produces a SOC 2 report—much less a Type II report. HIPAA requires third-party partners to comply, but it doesn’t obligate these companies to invest in any type of standard audit to prove their compliance," explained Melanie Pita, Executive Vice President - Product Development, Ontellus. "There aren't many records partners out there that have SOC 2 Type II reports, so it's becoming a key differentiator in the records retrieval market."

Easy to Understand. The SOC 2 report is a pass/fail test, meaning that the security controls either pass or fail in demonstrating effectiveness. With a pass/fail situation, the audit is clear—carriers and law firms don't have to read through auditor reports to interpret their partner's security levels.

"When a records company can show a SOC 2 Type II audit report—the client inquiry is met. The client should have full and complete confidence that they are partnering with company that takes HIPAA seriously and has proven that their systems comply," added Pita.

No Formal Certification Commission Exists Today. There is no formal list or verified database of SOC 2 Type II audited companies, which means it can be difficult if carriers and law firms want to verify that the audit report was indeed provided to the records company in question. Upon audit completion, the auditor issues a report to the records partner. This is the only official documentation, and records partners should be willing to provide potential clients with a copy upon request.

BUYER BEWARE

SSAE-16 and AT-101 standard audits may or may not include the Type II report. Therefore, one cannot assume that these certifications include a Type II audit report. Likewise, ISO 2700 and other ISO standards may not necessarily cover all HIPAA requirements. When in doubt, ask specifically for a SOC 2 report.

Comparing HIPAA and SOC 2

People ask the question: "What is the difference between HIPAA and SOC 2 Type II?"

HIPAA is a federally mandated compliance regulation with no specific required type of audit or compliance report. Although people tend to speak of SOC 2 as though it is a federally mandated regulation, it is not. Simply put, SOC 2 is one type of report that is the outcome of standard auditing processes (SSAE-16 and AT 101) which are commonly used to demonstrate HIPAA compliance.

While HIPAA's rules focus primarily on privacy and security (administrative, technical, and physical safeguards), SOC 2 Type II evaluations widen HIPAA's evaluation scope to also include:

- **Availability:** The system is available for operation and use as committed or agreed
- **Processing Integrity:** System processing is complete, valid, accurate, timely, and authorized
- **Confidentiality:** Information designated as confidential is protected as committed or agreed

"Another advantage of the SOC 2 Type II audit is that it typically signifies that the records partner has policies and procedures in place to address data breaches and the associated liabilities. This puts the teeth in the compliance approach, making it stronger and developed in coordination with the legal department," said Pita.

A Matrix: HIPAA vs. SOC 2

The matrix below provides a side-by-side comparison of the criteria required as part of the HIPAA regulation and SOC 2 Type II audit. Records partners, such as Ontellus, should meet all criteria.

Criteria	SOC 2 Type 2	HIPAA	Ontellus
Management Directives	✓		✓
Information Security Polices	✓	✓	✓
Human Resource Initiatives	✓	✓	✓
Personnel (Internal and External Roles)	✓		✓
Contractual, Legal, Administrative and Technical System Documentation	✓	✓	✓
Security Awareness and Personally Identifiable Information (PII)	✓	✓	✓
Employee Skillsets and User Awareness	✓		✓
Security Response and Reporting	✓	✓	✓
Communication of System Changes to Relevant Users	✓		✓
Risk Analysis and Management	✓	✓	✓
Monitoring of Controls	✓	✓	✓
Data Back-Up Plan		✓	✓
Access Rights Standard and Protocols	✓	✓	✓
General Access Rights Provisions	✓	✓	✓
Unique User Identification	✓	✓	✓
Disaster Recovery Plan		✓	✓
Role Based Access Controls and Two-Factor Authentication	✓	✓	✓
Physical Access and Monitoring	✓	✓	✓
Emergency Mode Operation Plan		✓	✓
Network Access	✓	✓	✓
Disposal / Media Re-Use		✓	✓
Data Transmission and Encryption	✓	✓	✓
Emergency Access Procedures		✓	✓
Anti-virus Mechanism	✓	✓	✓
Logging and Monitoring, System Backups, Ticketing System	✓	✓	✓
Breaches and Incidents	✓	✓	✓
Confidentiality	✓	✓	✓
Sanction Policy	✓	✓	✓

Best Practices for Evaluating Partners

While HIPAA is a primary concern, choosing the right partner can help insurance companies and law firms avoid the embarrassment, costs, and substantial financial penalties associated with any type of data breach. Beyond the SOC 2 Type II audit report there are a variety of other criteria that can help in the selection.

A Checklist: Identifying Security-Conscious Partners

✓	Information Governance Matching: As a general rule of thumb, records partners should have information governance practices that at least match those of the client and preferably reach above and beyond, helping you become a records security leader.
	Compliance Reports: Records partners that make compliance a top priority report on performance as it relates to security and information governance. The most advanced partners will offer compliance reporting on a client-by-client account basis, giving you a report specific to the records orders and documents managed within your client account.
	Accountability Reports: Records partners should be able to provide a tracked history of activity associated with each record or records order, including who accessed each record and how records were distributed. These reports are often key pieces of evidence in data breach investigations and requested by plaintiff counsel or as part of claims inquiries.
	Physical Security: The office or area where records are processed should be secure and secluded from regular business. The most security-conscious records partners forbid cell phones on the production floor and take extra precaution to shred hard copies.
	Vulnerability Testing: Annual penetration tests are a best practice and should reveal areas for improvement, updates, or changes to security policies. Don't be afraid to ask partners how they are advancing and improving data security processes. Security is not static checkbox but an evolving journey.
	Employee Training and Background Checks: As a key part of compliance and data security, employee training should include initial training and testing on the policies/procedures, as well as frequent reminders. Internal employee-driven data breaches are common—you don't want just anyone accessing healthcare records.
	Records Partners Should Audit their Other Records Providers: Many records partners outsource parts of their work to other records providers or have back-end integrated systems connected to external records repositories, which all add risk. Look for a partner who audits their extended network of providers. These companies are your providers, too.
	Data Breach Insurance: Insurance is available to cover the cost of a data breach and can be a sign of a responsible records partner. Reports show that the cost of a data breach can be crippling and even fatal for companies, so the cost is always justified. The risk is too great.
	Compliance Free of Cost: Records partners should never pass the cost of compliance or audits onto the client. The burden of compliance falls squarely on the records company. Any lack of responsibility and accountability is likely a red flag.

The Ontellus Approach to Compliance

Ontellus has implemented physical, technical, and administrative safeguards in order to comply with HIPAA regulations. The following Ontellus systems and procedures have been audited and satisfy the HIPAA requirements.

Physical Safeguards

- Contingency Operations: As part of Ontellus disposal and media re-use policies and procedures, electronic media containing protected health information is scrubbed of electronic protected health information prior to re-use.
- Facility Security Plan: Ontellus facilities nationwide utilize multiple levels of building and network security to protect against unauthorized physical access, tampering and theft.
- Access Control and Validation Procedures: Ontellus assigns a level of role-based access for each of its employees to control an employee's individual access to physical areas within company facilities and network access to select software programs.
- Maintenance Records: Ontellus documents any repairs and modifications to the physical component of any and all of its facilities which are related to security, including hardware, walls, doors and locks.
- Workstation Use: Ontellus has implemented policies and procedures governing proper function(s), method(s) and physical attributes of all workstations that are capable of accessing electronic protected health information.
- Workstation Security: Ontellus implements physical safeguards on workstations that access sensitive information and, on a periodic basis, verifies the presence of and proper configuration of such safeguards.
- Disposal: Ontellus has policies and procedures in place to remove electronic protected health information, and to log any movement and/or destruction of hardware or electronic media on which it is stored.
- Media Re-Use: Ontellus has procedures in place to remove sensitive information from equipment before it is re-assigned or reused in a different area.
- Accountability: Ontellus assigns an individual or individuals to track the movement of company hardware and electronic media and maintain a log of said movement.
- Data Back-Up and Storage: Ontellus regularly tests its procedures for data back-up and storage to prepare for any event necessitating the creation of a retrievable, exact copy of electronic protected health information.

Under the HIPAA's newest rules, insurance carriers and law firms can be FOUND LIABLE for a breach of PHI due to a record partner's negligence

Technical Safeguards

- Unique User Identification: Ontellus requires unique USER ID's and Passwords to gain access to company applications and resources.
- Emergency Access Procedures: Ontellus conducts testing of access to necessary electronic protected health information in various emergency situations on a periodic basis and as needed in accordance with drastic technological and non-technical changes within the company.
- Automatic Logoff: Ontellus implements electronic procedures to temporarily suspend electronic sessions after a predetermine time of inactivity.
- Encryption and Decryption: Ontellus possesses and implements mechanisms to encrypt and decrypt sensitive information retrieved, stored, transmitted, and received.
- Mechanism to Authenticate ePHI (electronic protected health information): Ontellus has electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
- Integrity Controls: Ontellus has security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.
- Encryption: Ontellus has implemented a mechanism to encrypt electronic protected health information whenever deemed appropriate to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

Administrative Safeguards

- Risk Analysis: Ontellus conducts an annual risk assessment throughout the organization identifying potential risks and vulnerabilities regarding sensitive information held.
- Risk Management: Ontellus has a Risk Management plan to address and resolve any possible risks and vulnerabilities uncovered during the Risk Analysis.
- Sanction Policy: Ontellus has in place appropriate sanctions in place to address workforce violations regarding security policies and procedures.
- Information System Activity Review: Ontellus test procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
- Assigned Security Responsibility: Ontellus has identified individuals as security officials responsible for the development and implementation of policies and procedures required under HIPAA.

New data security VULNERABILITIES ARE RISING out of the increasingly mobile and remote workplace environment[2]

- Security Response and Reporting: Ontellus has an established Security Incident Response policy that lays out the framework for a thorough investigation and reporting of any possible security incident.
- Data Back-Up Plan: Ontellus has in place comprehensive data backup policies, procedures, and supporting processes for ensuring all environments are backed up in a timely, accurate, and complete manner. Furthermore, any incident relating to backups, such as backup failures, are corrected immediately for ensuring the integrity of the data.
- Disaster Recovery Plan: Ontellus has comprehensive Business Continuity and Disaster Recovery Planning (BCDRP) policies and procedures in place. Additionally, the documentation has been developed in accordance with industry-leading benchmarks, standards, frameworks, associations, and best practices.
- Emergency Mode Operation Plan: Ontellus has comprehensive Business Continuity and Disaster Recovery Planning (BCDRP) policies and procedures in place. Additionally, the documentation has been developed in accordance with industry-leading benchmarks, standards, frameworks, associations, and best practices.
- Testing and Revision Procedures: Ontellus has established periodic testing for contingency plans. Any revision to those plans are documented and distributed to the applicable parties.
- Authorization/Supervision: Ontellus has procedures in place controlling and supervising workforce member's access to sensitive information. Workforce access to sensitive information is restricted to those individuals who have been trained on the security requirements need to access such information.
- Workforce Clearance Procedures: Ontellus workforce member's access to sensitive information is restricted to minimum necessary to complete their job function. Procedures are established to determine which workforce members can access certain sensitive information.
- Termination Procedures: Ontellus maintains procedures on terminating access to workforce members when employment with the organization has ended or the individual no longer requires access for the job function.
- Security Reminders: Ontellus provides security awareness training to all employees upon hiring and annually. Additionally, the organization will provide periodic security reminders regarding the protection of sensitive information.
- Protection from Malicious Software: Ontellus has in place anti-virus software and configured its systems to provide updates against new malicious software.

MEGA BREACHES will move from focusing on healthcare insurers to focusing on other aspects of healthcare, including HOSPITAL NETWORKS[1]

COMPLACENCY HAS SET IN

While more organizations have put data protections and breach response plans into place, a level of **complacency has set in** that is preventing response readiness. Many are lagging in practicing and updating their response plans as well as keeping up with new types of attacks.[1]

- Log-In Monitoring: Ontellus maintains procedures for tracking and reporting users log-in to and reporting any incidents that need further investigation.
- Password Management: Ontellus maintains procedures and rules establishing the creation of passwords, requirements for changing password and the restriction of sharing password among users.
- Access Authorization: Ontellus requires users to have specified access including User ID's and Passwords in order to be granted access to sensitive information.
- Access Establishment and Modification: Ontellus has policies and procedures in place controlling the rights of users in accessing sensitive information based on program, workstation and user rights.
- Application and Data Criticality Analysis: During review of contingency planning, Ontellus identifies specific applications and prioritizes those in supporting data.
- Written Contract or Other Arrangement: Ontellus enters into written contracts with other business associates to ensure that required satisfactory assurances are met.

Beyond Compliance: How Ontellus Drives Innovation

A Security Culture: Training Starts with the Legal Department

Ontellus has comprehensive employee training programs that include HIPAA compliance and data security training, and it all starts with the Legal Department. The Ontellus in-house legal team serves as the company's compliance experts. They are key stakeholders in the creation and evolution of the training program. All employees attend this training, are tested on the material, and must pass or re-take the class until a passing grade is achieved. The training itself and employee certifications are updated annually. Additionally, employees receive security reminders in the form of quarterly communiques and monthly meetings with managers.

"Information security has become the fabric of who we are as a company," said Newton Ross, CEO, Ontellus. "It's part of our DNA and culture."

Client-Based Compliance Reports that Follow Through

Ontellus distributes compliance reports to clients on a regular basis and on any schedule the client prefers. The Ontellus key account team reviews these reports during client stewardship meetings, working to further align with clients on security practices and procedures. Furthermore, these reports are segmented by client

Ontellus compliance reports are SEGMENTED BY CLIENT ACCOUNT, so each report accurately reflects the security practices performed on the specific records within each client account.

account so that the information represents a compliance report specific to the records orders and documents managed as part of each specific client account.

"While our reports may appear ordinary or an assumed process for any records partnership, two things are very different when compared to other records companies," explained Pita. "First, we actually present reports. Many records companies say they provide reports but don't actually deliver or distribute them to their clients. Our delivery demonstrates our commitment to accountability and visibility. Second, the reports aren't canned data or a general overview across all accounts. They accurately reflect the security practices on the records handled within your account. This is of extreme value to our clients and a true differentiator for Ontellus."

Executive Leadership Behind the Incident Response & HIPAA Compliance Team

Ontellus maintains an Incident Response Team comprised of executives and leaders from IT and the Legal Departments. Additionally, Ontellus maintains a HIPAA compliance team, supported by executives. Every incident is:

- Thoroughly investigated to evaluate a data breach
- Documented
- Shared with the HIPAA compliance team
- Labeled as either a data breach or security incident

The company data breach response policy is then put into action as needed.

"Few record partners have identified response teams and compliance teams to take responsibility for investigating security incidents and even fewer have incident response teams that include executives and cross-departmental leaders from IT and Legal. This is another area where Ontellus really goes above and beyond. We're leading the industry," explained Ross.

"Few record partners have identified response teams and compliance teams to take responsibility for investigating security incidents and even fewer have incident response teams that include executives and cross-departmental leaders from IT and Legal. This is another area where Ontellus really goes above and beyond. We're leading the industry."

-Newton Ross,
CEO, Ontellus

Delivering Real Value: Customized Reports Built on Client KPIs

While basic records providers will simply deliver records, true records partners like Ontellus work diligently to extend the value of their service. Ontellus key account teams help carriers and law firms reduce retrieval costs, boost security, and evaluate their existing records process in order to further automate ordering processes and gain efficiency and productivity savings.

Initial alignment meetings and ongoing client stewardship meetings give carriers and law firms a chance to customize their Ontellus records-related reports around the key performance indicators (KPIs) that matter most to their business. This tight collaboration delivers data that supports the client's strategic objectives—whether it's taking a deep-dive on security, tightening up order workflows, increasing performance, or training and advocating for more technology adoption and utilization. Ontellus supports requests for custom and ad-hoc reporting too, giving clients useful insight and a records expert to develop and execute actions plans.

Driving Records Innovation: Not Just Keeping Up but Staying Ahead

“At Ontellus, our approach to compliance is not just to keep up with the regulations but to stay ahead of them. With this strategy, we’re proactively ready when the laws change,” explained Ross.

The Ontellus legal support team and IT executives are constantly monitoring the latest trends in security technologies and information governance to expand the company’s vision and stay on the cutting-edge. Plus, Ontellus maintains strategic partnerships with key players in the artificial intelligence space, so the company can incorporate sophisticated data analytics to advance client insight.

“For many of our clients, Ontellus acts a thought leader in security, guiding them in ensuring data and records are passed in the most secure manner,” added Ross. “Our team brings experience in designing secure records sharing systems, and we’re happy to share that knowledge with our partners.”

Conclusion: Audit Your Partners

As holders of valuable information assets, healthcare organizations and their partners are marked as key targets for hackers seeking to leverage new security vulnerabilities from today’s increasingly mobile and remote workplace. As such, insurance carriers and law firms working with healthcare records must move quickly to ensure their systems and partners are HIPAA compliant and exercising the most stringent practices in data security. Most importantly, carriers and law firms need to audit all third-party partners, asking for a SOC 2 Type II report. Records partners should have the client’s best interest at heart and always be thinking about information security. Do you know how secure your records are when they sit outside your organization?

About Ontellus

Ontellus empowers insurance carriers, self-insured corporations and law firms to reduce costs, make informed decisions and accelerate claims resolution. As the nation’s largest, privately-held records retrieval provider, Ontellus leverages decades of experience and cutting-edge technology to deliver impacting products and client-centric services within industry-leading turnaround times.