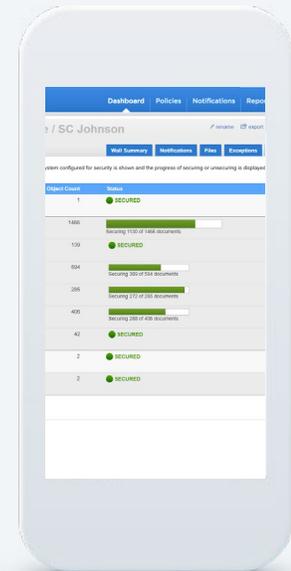# Intapp Walls

## Top 10 Reasons Firms Use Intapp Walls and Activity Tracker

In the past few years, law firms have been compelled to revisit their approach to managing client confidentiality, information security and compliance to address information risks emerging in today's mobile and digital age. Central to law firm information security and compliance programs are the tools firms use to manage access controls and confidentiality across the organization. Firms require the best protections available to safeguard client confidences, guard (and even improve) firm reputation and meet today's standard of care for professional responsibility and compliance.

And the product firms overwhelmingly select to manage confidentiality and security is Intapp Walls. Intapp Walls is the most adopted ethical wall and information security management product for law firms. Over 230 organizations, ranging in size from 35 to 5000 lawyers, including 19 of the 20 largest firms in the world, rely on Intapp solutions to automate and centralize information security and confidentiality management.

Firms use Intapp Walls to address a variety of security and compliance requirements. Here are the top 10 use cases.

## Client and Regulatory Requirements

### 1. Client Information Security Audits and Requirements

Ever increasing threats to data security as well as client demands have put pressure on firms to restrict access to information. Clients – particularly in the financial services industry – are imposing outside counsel guidelines requiring firms to implement information barriers to protect confidentiality. Firms cite Intapp Walls as an industry standard in RFPs, security questionnaires and audits, to assure top clients that information will be protected from unauthorized disclosure and foster the trust required for a successful ongoing client-firm relationship.

### 2. Data Protection and Data Privacy Laws and Regulations

Regulations such as the US Health Insurance Portability and Accountability Act (HIPAA) mandate that firms restrict access to and monitor usage of personally identifiable information (or protected health information (PHI) in the case of HIPAA). Firms ranging from large global firms to smaller regional firms use Intapp Walls for HIPAA compliance. Intapp Walls enables firms to control and track access to sensitive electronic information, and also provides visibility into lawyer and staff engagement with PHI on multiple firm systems and cloud collaboration tools.

### 3. International, National and State Data Privacy and Security Laws

Regulatory requirements on personally identifiable information, like the EU Data Protection Directive or any state Data Privacy Laws create specific security requirements for information that meets defined criteria. Firms use Intapp Walls to enforce document-level or matter-level security on personal information in accordance with central firm policies. These more granular security capabilities enable firms to maintain open access to less sensitive information within a particular matter or workspace for collaboration and knowledge management, restricting access to only the most sensitive documents.

## Ethics and Professional Responsibility

### 4. Automated Ethical Wall Management

With lateral mobility and merger activity continuing, today firms cannot compete and address professional rules effectively without automating management of ethical screens triggered by new clients, lateral hires, contract lawyers or mergers. Intapp Walls is the only product on the market that manages ethical walls, with native integrations to secure 25+ systems.

### 5. Lateral Hires and Departures

Lateral transfers are attractive to firms precisely because they bring with them past experience and client relationships of value to the firm's business interests and strategy. But this very success often creates business conflicts. Intapp Walls includes specific policies to manage ethical screens necessitated by lateral hires. And, conversely, it also offers transparent activity monitoring to identify suspicious behavior that may signal impending departures.

### 6. Legal Holds Management

Centralizing processes to manage internal litigation holds is crucial to firms of any size. The Legal Holds feature provides firms with a simple, central means to manage holds on document and records management systems, notify and collect acknowledgements from affected custodians, synchronize with systems to update custodians, and maintain an audit log of legal hold policies.

### 7. Malpractice Insurance Standard of Care

Top malpractice underwriters and brokers have partnered with Intapp to help firms understand and manage the ever-increasing risks of cyber exposure. The insurance industry recognizes Intapp Walls as the standard of care for confidentiality, rewarding firms who invest in the product.

## Firm Security Initiatives and Priorities

### 8. Intelligent Monitoring and Data Loss Prevention

A panel on insider threats at the 2016 Gartner Security & Risk Management Summit emphasized the need for detection and analysis tools to track potential security threats from employees. Firms must have a tool to alert management of suspicious activity that may signal a security breach, lateral departure, or unintentional policy violation, like sending sensitive information to a personal email address.

### 9. Moving Away from the Open-By-Default Paradigm

With a culture designed to foster sharing, knowledge and productivity, firms have traditionally provided internal users with "open-by-default" access to client and firm information. But more recently, a growing number of firms are locking down sensitive information – for example, by applying rule-based access controls to segment their DMS, and layering members-only restrictions for particular practice groups, industry sectors or office locations for additional protection. Only Intapp Walls enables firms to implement these sophisticated, overlapping controls without compromising business and productivity.

### 10. ISO 27001/27002

To improve their ability to quickly and comprehensively respond to client information security questionnaires and audits, firms are increasingly pursuing certification or alignment with stand-ardized and accepted security and risk management frameworks like ISO 27001. Firms employ Intapp Walls to address the access control policies ISO requires on information repositories.