DATA SHEET

Intapp Walls

Top 10 reasons firms use Intapp Walls and Activity Tracker

In the face of growing requirements — from clients, regulators, and the court — law firms are increasingly revisiting their approaches to managing client confidentiality, information security, and regulatory compliance.

More than ever before, law firms require a comprehensive plan for protecting client information, safeguarding firm reputation, and maintaining a modern standard of care for compliance and responsibility. Intapp Walls is the product that firms overwhelmingly select to manage their confidentiality and security needs.

Intapp Walls is the most widely adopted ethical wall and information security management product for law firms. More than 230 organizations, ranging in size from 35 to 5,000 lawyers — including 19 of the 20 largest firms in the world — rely on Intapp to automate and centralize information security and confidentiality management.

Leading firms use Intapp Walls to address a variety of concerns. Here are the top 10:

Client and regulatory requirements

1. Client security audits and requirements

Ever-increasing threats to data security, as well as growing client demands, have pressured firms to restrict access to key information. Clients, particularly those in the financial services industry, impose outside counsel guidelines requiring firms to implement information barriers to protect confidentiality. Firms cite Intapp Walls as the industry standard for responding to RFPs, security questionnaires, and audits, assuring top clients that their information will be protected from unauthorized disclosure and fostering the trust required for a successful and ongoing client/firm relationship.

2. Data-protection laws and regulations

Regulations such as the U.S. Health Insurance Portability and Accountability Act (HIPAA) mandate that firms restrict access to and monitor usage of protected data classes. Firms of all sizes — ranging from large global networks to smaller regional enterprises — use Intapp Walls to ensure HIPPA compliance. Intapp Walls enables firms to control and track access to sensitive electronic information, and also provides visibility into lawyer and staff engagement with data, even across a firm's multiple systems and cloud collaboration tools.

3. Government data privacy and security laws

Regulatory requirements covering personally identifiable information — including the European Union's Data Protection Directive and U.S. state data privacy laws — create specific security requirements for certain types of information. Firms use Intapp Walls to enforce document-level or matter-level security in accordance with central firm policies. Intapp Walls' granular security capabilities enable firms to maintain open access to less-sensitive information within a particular matter or workspace in order to maintain collaboration and knowledge management, restricting access to only the most sensitive documents.

Ethics and professional responsibility

4. Automated ethical wall management

Today's firms cannot compete effectively or address professional rules adequately 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

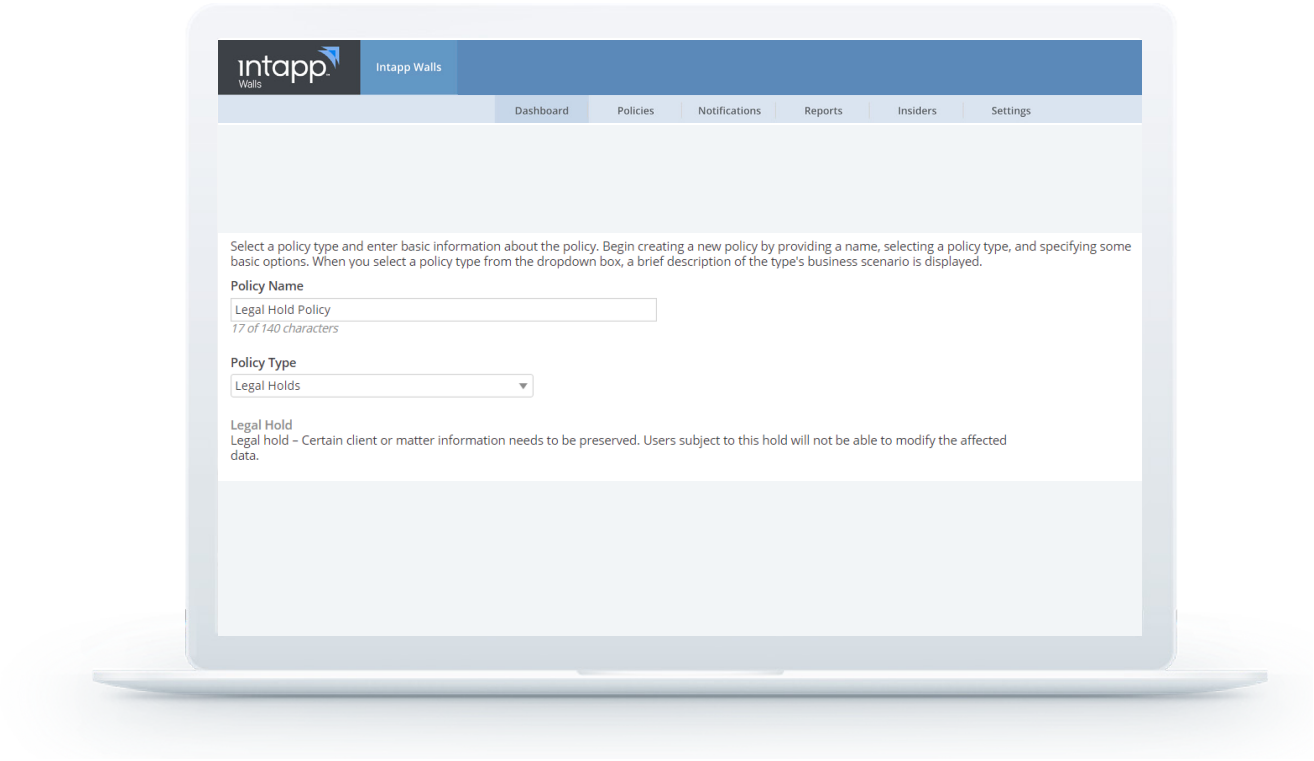
Lateral transfers are attractive to firms precisely because they bring valuable strategic experience and client relationships. But this mobility often creates business conflicts. Intapp Walls includes specific policies to manage ethical screens necessitated by lateral hires. The system also offers transparent activity monitoring to identify suspicious behavior that may signal impending departures.

6. Legal holds management

Firms of all sizes need to centralize processes that manage internal litigation holds. Intapp Walls provides firms with a simple, central means to manage key tasks, including placing holds on document- and records-management systems, notifing and collecting acknowledgments from affected custodians, synchronizing with systems to update custodians, and maintaining an audit log of legal hold policies.

7. Malpractice insurance standard of care

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



Firm security initiatives and priorities

8. Intelligent monitoring and data loss prevention

At a recent Gartner Security & Risk Management Summit, presenters emphasized the need for detection and analysis tools to track potential security threats from employees. Firms must implement tools to alert management of suspicious activities that may signal an internal security breach, impending lateral departure, or unintentional policy violation, such as sending sensitive information to a personal email address.

9. Layered security controls

With cultures designed to foster collaboration, knowledge, and productivity, firms have traditionally provided internal users with open-by-default access to client and firm information. More recently, a growing number of firms lock down sensitive information — for example, by implementing rule-based access controls to segment their DMS, then applying members-only restrictions for particular practice groups, industry sectors, or office locations for additional protection.

Only Intapp Walls lets firms implement these sophisticated, overlapping controls without compromising business and productivity.

10. Certification framework requirements

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