# Why Secure File Transfer Matters in the Legal Field

## The Legal Ecosystem and Community

Lawyers are busy enough managing client needs and all the data surrounding the legal process. In today's legal world, the exchange of files is paramount for collaborative thinking and resolution. Often lawyers are required to communicate with numerous parties at one time.  For each conversation and data transfer point to be successful, trust and security must be paramount.

The legal community is varied and diverse and the management systems reflect that. Sometimes it is hard to know what is protected and what is not. To be effective, cyber protection in the legal community today focuses on three main areas: personal data, asset protection and workflow according to court needs.

Much has been written about personal data protection and GDPR; but if you can protect the files in transit, you mitigate risk. That takes a major cost risk out of the equation and burdens the sender or receiver to protect their own data. Using secure file transfer like an armored truck is an effective way to manage risk.

## Protecting legal data in-transit

Successful data sharing focuses on a permission-based transfer. In order to create transparent and secure communication, each party must believe in the other – beyond audit of regulation or compliance. The transfer of legal data therefore must center on managing and protecting data for both the individual attorney and his/her firm. From a liability point of view, legal data management must protect all data transferred between the parties – the lawyer, the firm, and all the clients.

One method of protecting the attorney and the firm is to improve control.  In instance, control becomes more than securing passwords and relies on file transfer security as the key to dramatically decreasing security risk.

When people send files filled with data, they must trust a few things – for example.

» Can I trust the person I am transacting with?

» Are the files fully protected from departure to acceptance?

» How do I know someone received the files?

So often emails are sent with precious information and for legal transactions, small companies or lawyers don't always have the resources to manage the data.

## Secure File Transfer – The Best First Step

Put aside cyber security hype. The most pervasive threat comes from humans and data-in-transit. When employees and partners share information and data, they create a daily interchange for thriving business. Today, this must be secure to ensure trust.

The best first step is to protect the files so securely that it takes away the most vulnerable weak link of data-in-transit. If done easily and automatically, then the path to greater security is assured. Secure file transfer, when done right, dramatically lowers the risk of data breach.

## Protecting the Peer to Peer Relationship

The value of a trusted relationship – whether in a private conversation, a critical moment of need, or protecting assets cannot be underestimated. We develop relationships and communicate in a unique way; secure data is very much like that too.  When we transfer data, it must be as safe as precious cargo. If we establish a peer to peer relationship, with a toolset that guarantees secure file transfer, we can substantially protect files and data. Imagine a cyber approach where you can increase protection in five minutes - one where you establish a trusted peer relationship and pull files from a trusted place for both parties. Like an armored truck.

Safety4Data is a data encryption and transfer application which relies upon a secured, peer-to-peer virtual network that allows users to confidently exchange data with anyone in their network.

## Layers of Security
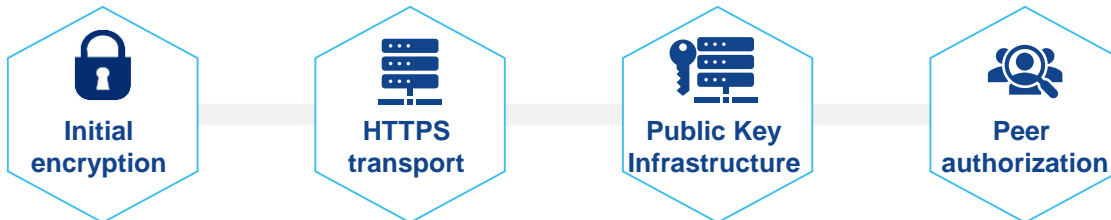
Every file is secure from the moment of release to the moment of acceptance.

## A Bit More about Security

Safety4Data works by assigning a pair of PKI keys – one public and one private. Only the user who owns the keys has the private key, but the user's public key can be given to anyone. When using PKI, the user secures not only the server authentication, but also the Safety4Data user authentication. In addition, users can encrypt/decrypt files using PKI.

During transfer, data is sent via Safety4Data's highly secure, encrypted HTTPS tunnel. The server is then authenticated by a server certificate, verifying the user is communicating with the legitimate Safety4Data application, not an unreliable server.

Files are encrypted and stored on Safety4Data servers until the recipient downloads them, at which time the files on the server is permanently deleted. Encryption certificates are acquired via "Certificate Authorities" and managed to optimize security.  Each of these steps occur automatically within the Safety4Data platform.

Data security is created by using the Azure cloud server environment – technology which delivers a superior level of confidentiality, integrity and stored data availability. This is completely managed by the Safety4Data service within the client peer-to-peer realm.

## The Safety4 Data Elements

### The Service

» Web administration local service is automatically installed in the background for PKI distribution and the files send/download process and the encryption/decryption process.

» Local service setup is done through the web administration and options are available in the notification tray.

» PKI trust is achieved with providers' certificates or optionally with the user's own certificates.

### The Administration

» The local administrator creates a virtual user network with either simple (all users can communicate only with local admin) or full (every user can communicate with all users).

» You can also create communication groups.

### File size

» As small as 200 MB

» File size can increase to over 1 GB or more if required

### User Flexibility

» Users work in their own OS with upload/download folders for drag-and-drop ease

» Optional file sending with a context menu (right-click mouse operation) is available

» Optional direct files upload/download to/from web administration (for one-time communication with client) to provide more comfort for users.

### Logging, Audit, Notification

» Every file transfer is registered into the communication log to provide overview for users. An error log is provided if there are errors during the file encryption of transfer.

» A list of downloaded files (simple Download manager) is included in the communications log and includes the name of file, information about sender and option to open a folder where the file is placed.

» Notification of email and system tray about upload/download file is fully configurable..

## The Safety4Data Hosted Service

To use Safety4Data, you subscribe on a ser basis and install a light footprint client to ensure secure file transfer. Safety4Data is a set of software and tools on a hosted application, built on a client-server architecture to enable the creation of virtual secured networks.

Administration is an easy-to-use dashboard that manages files, users and subscriber settings for high file security.
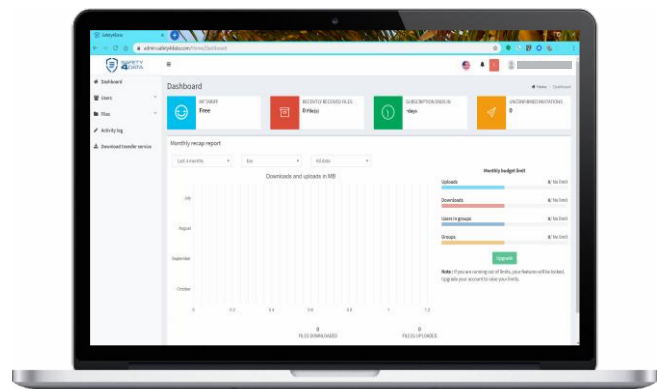
## Services and Support

**Safety4SERVICES** represents the program, where file security experts can be engaged for projects and enterprise installations if needed. In addition, the Safety4Data team can create connections to existing data sources, API's and cloud-based systems. The hosted Safety4Data solution is fully supported with software and client upgrades.

We offer personal Cyber Security Consulting services for small to mid-size businesses. We work directly with your business to fill the gaps and find affordable solutions to keeping your information secure and money saved. We understand that cyber security may not be a top priority, however, it is of the utmost importance to prepare, protect and be proactive, as opposed to assume you are safe, then be reactive to a breach that could be easily prevented.

**Safety4CARE** is Safety4Data's software upgrade program that provides notification of software features and upgrades for the hosted solution.

## Get Safety4Data

Start with the trial
download HERE

Contact us at
sales@it-cns.com