AN ATTORNEY'S GUIDE

Law Firm Security and Data Redundancy

mycase

Table of Contents

i At MyCase, Security is Our Top Priority 2

1 What is Cloud Computing? 3

2 A Brief Overview of MyCase’s Security Measures 4

Amazon’s Cloud Computing Platform 4
Data Redundancy & Disaster Recovery 5
Experience Counts 5
State of the Art Encryption 5

3 Protection in MyCase 6

Authentication & Passwords 6
User & Case Permissions 6
Document Trash Bin 7
Secure Client Portal 7
Two-Factor Authentication 7

4 What You Can Do to Protect Your Data 9

At MyCase, Security is Our Top Priority

Here at MyCase, we understand that you have an ethical obligation to maintain confidentiality. That's why keeping our customers' data secure is our top priority. Protecting privileged case information for thousands of attorneys (and their clients) is a responsibility that we take very seriously.

We recognize that some attorneys may be nervous about moving their data into the cloud. You undoubtedly have a lot of questions about the steps we take to ensure that your law firm's data is safe and secure at all times:

- Is my data secure at rest and in transit?
- Where does the data reside? Is it encrypted? Is it backed up?
- Is my data secure from phishing attacks or hacks?
- How can I keep client information confidential using permissions?
- How can I prevent accidental or malicious data loss?
- Are my client communications secure?

In this whitepaper, we will answer all of those questions and provide an overview of how we ensure the security of your law firm's data, in part by providing redundant data storage and backup. Our goal is to put your mind at ease by sharing our security procedures, which are relied upon by thousands of attorneys like yourself who trust MyCase to help them manage their law firms.

1 What is Cloud Computing?

Cloud computing may be a new concept to you, but rest assured, even if you're unfamiliar with what cloud computing is, you're likely already using it in your law practice. The concept of cloud computing is simple: when you store documents online, whether in MyCase as web-based email attachments, or via a stand-alone online storage solution, you're storing them "in the cloud." In other words, your law firm's digital data lives in the cloud when it's being stored on servers owned and maintained by a third party rather than your law firm.

So, if you've ever used Westlaw, Google Drive, or Dropbox, you've used cloud computing. Your online bank account and every bill you pay online are also managed in the cloud. If you've ever used any of these online tools, you're probably already well aware of the many benefits gained by using cloud computing.

For starters, costly solutions like in-house IT departments, expensive servers, and up-front infrastructure costs are avoided when you leverage cloud computing. Another benefit of cloud computing is the convenience and mobility it offers attorneys and legal professionals. The ability to access your law firm's case files 24/7, from any location, using any Internet-enabled device is an incredible convenience. But there's more to cloud computing than simply IT savings and mobility; the security it provides your law firm is likewise immeasurable.

2 A Brief Overview of MyCase's Security Measures

Amazon's Cloud Computing Platform

MyCase runs on Amazon Web Services' EC2 cloud computing platform. We chose Amazon's EC2 cloud servers because Amazon has well over a decade of experience managing cloud servers across 16 different geographical regions across the United States for some of the largest, world renowned companies in business today. Because of the breadth of Amazon's experience providing cloud computing services, you know you can trust them to be at the leading edge of online service technology.

Amazon has strict procedures in place, which protect the physical security of their servers and safeguard the integrity of their data. Amazon's data centers and network architecture are built to meet the requirements of the most security-sensitive organizations.

Learn more about Amazon's cloud infrastructure and security at http://aws.amazon.com/security/.

In addition to Amazon's security standards, our network traffic is isolated from other AWS customers via Virtual Private Cloud (VPC) dedicated to MyCase customers only. We communicate with our database using a secure connection and aggressively protect access to our servers with firewalls.

Data Redundancy & Disaster Recovery

Even with all the security measures that AWS has in place, MyCase understands that the thought of losing important case information is beyond scary. For that reason, we store data in AWS in multiple regions and backup the database to various different locations. **In other words, we store and backup any document that is uploaded to MyCase forever, even if it is deleted.**

Experience Counts

When it comes to protecting data for your law firm, experience counts. Our in-house security team performs internal security audits on a regular basis to ensure our system is secure and your information is protected. We run static analysis tools on our code regularly, and we automatically scan lists of known vulnerabilities (CVEs) for references to the software on which we depend.

MyCase was founded by an attorney and designed from the ground up with the unique security needs of attorneys in mind. Our 10+ years of experience in SaaS serving the legal industry ensure that we've built a secure online platform for lawyers that you can trust. We're constantly monitoring the latest security threats, and evolving and adapting our service to address any issues that may arise.

State of the Art Encryption

When you connect to our servers, your data is encrypted at rest and during transmission using 256-bit SSL connection. If the user's internet browser does not support full 256-bit encryption, the connection degrades to 128-bit, but by default your data is protected with the highest, state-of-the-art encryption available. Our cipher suites also support Perfect Forward Secrecy (PFS) which prevents backward decryption of stored data should keys be compromised in the future.

This is the same type of secure connection you use when accessing online banking, investments, healthcare portals, etc. Encrypting your transmission ensures that nobody can intercept your data along the way, and verifies it is truly you who is connected to our servers and not an impostor.

For added peace of mind, view our real-time SSL Labs test times and grade:
https://www.ssllabs.com/ssltest/analyze.html?d=www.mycase.com&hideResults=on

3 Protection in MyCase

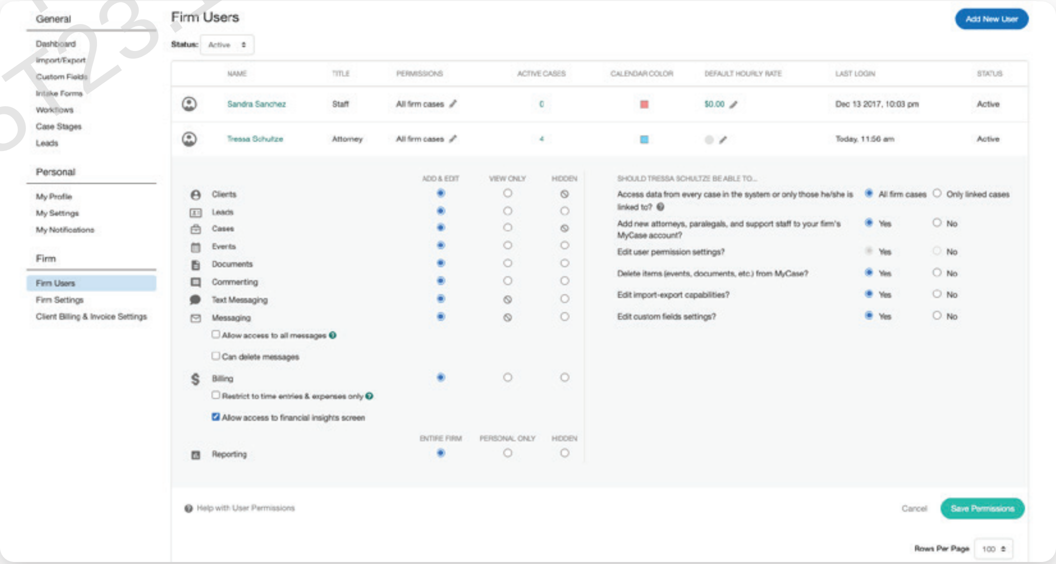
In addition to the security steps Amazon and MyCase take on the server side, there are also a number of features built into MyCase that will help keep your firm's data protected.

Authentication & Passwords

MyCase will automatically log users out during times of inactivity or when the account has been accessed on another device. In addition, MyCase stores passwords using the latest top security recommendation. We add per-user random information (salts) to passwords, before hashing them with bcrypt — an algorithm designed to be resistant to brute-force attacks. In fact, MyCase only allows a certain type of password (referred to as a "salted, bcrypted password"), which helps resist brute-force attacks and provides an additional layer of protection.

User & Case Permissions

As a MyCase customer, sophisticated permission settings and access controls in the software help your firm protect client information and keep it confidential. Permission settings allow you to customize and control what each user can view or make changes to within MyCase. Specifically, access can be granted or withheld for each section of MyCase (e.g., documents, reporting, etc) as well as on a per case basis. In addition, you are able to control who can and cannot delete data from MyCase.



Firm Users

Status: Active

NAME	TITLE	PERMISSIONS	ACTIVE CASES	CALENDAR COLOR	DEFAULT HOURLY RATE	LAST LOGIN	STATUS
Sandra Sanchez	Staff	All firm cases	0	🟥	$0.00	Dec 13 2017, 10:03 pm	Active
Tressa Schultze	Attorney	All firm cases	4	🟦		Today, 11:56 am	Active

	ADD & EDIT	VIEW ONLY	HIDDEN
Clients	●	○	⦸
Leads	●	○	○
Cases	●	○	⦸
Events	●	○	○
Documents	●	○	○
Commenting	●	○	○
Text Messaging	●	⦸	○
Messaging	●	⦸	○
□ Allow access to all messages			
□ Can delete messages			
Billing	●	○	○
□ Restrict to time entries & expenses only			
☑ Allow access to financial insights screen			
	ENTIRE FIRM	PERSONAL ONLY	HIDDEN
Reporting	●	○	○

SHOULD TRESSA SCHULTZE BE ABLE TO...		
Access data from every case in the system or only those he/she is linked to?	● All firm cases	○ Only linked cases
Add new attorneys, paralegals, and support staff to your firm's MyCase account?	● Yes	○ No
Edit user permission settings?	○ Yes	○ No
Delete items (events, documents, etc.) from MyCase?	● Yes	○ No
Edit import-export capabilities?	● Yes	○ No
Edit custom fields settings?	● Yes	○ No

Rows Per Page 100

Document Trash Bin

Accidental or malicious document deletion is a potential risk at any law firm. For an extra layer of protection against this threat, the **Document Trash Bin** in MyCase enables users with apt permissions to move documents to the Trash Bin, after which your firm can easily recover and restore said documents **from** the **Document Trash Bin**, if need be.

Secure Client Portal

As a MyCase user, you have the option of granting your clients (or other associated parties) access to a secure **Client Portal**. Therein you can communicate and share important case details with your contact(s) in a manner much more secure than traditional email.

To keep your sensitive data under lock and key, parties with access are **only** able to see the appointments, documents, and invoices you've explicitly shared with them. Furthermore, this access can be changed or revoked at any time.

Beyond its functions as a communication tool, the MyCase **Client Portal** offers your clients peace of mind in knowing their case information and documents are protected and only accessible using their unique login credentials or by parties managing their case(s).

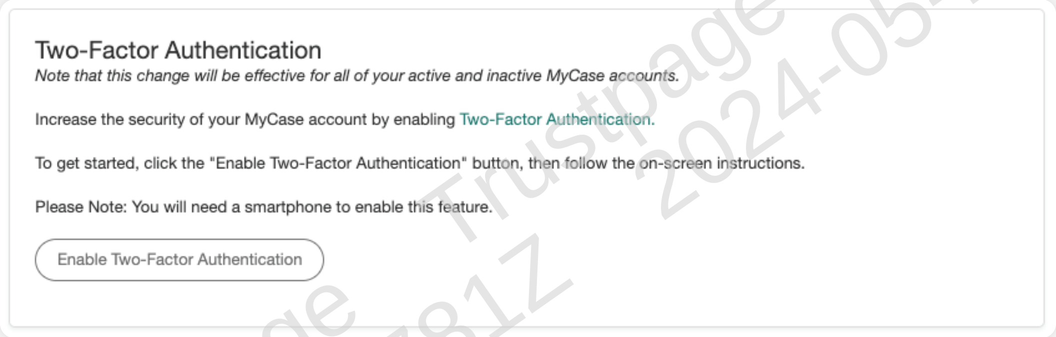
Two-Factor Authentication

MyCase offers Two-Factor Authentication via Google Authenticator, giving you an additional level of law firm security in the cloud. Two-Factor Authentication (or 2FA) is a security feature that makes it extremely difficult for unauthorized users to access your account. In the event that your username and password are compromised, 2FA would still prevent someone from gaining access to your confidential data. Here's how it works:

- **Without 2FA:** Logging into a web-based software system that does not implement 2FA is a simple, one-step process. All the user has to do is enter the correct username and password, at which point the entire database of sensitive client information is made available.

- **With 2FA:** Logging into a 2FA system requires an additional login step. After users enter their correct login credentials, they are not immediately logged into the system. Instead, they are redirected to a second login screen which prompts them to enter a temporary verification code. This verification code is a Time-Based One-Time Password with a 10-byte secret key generated by a CSPRNG — a cryptographic pseudorandom number generator.

Upon setting up a 2FA in MyCase for the first time, you'll need to go navigate to **Settings** > **My Profile** > **Two-Factor Authentication** whereupon you must follow three simple steps, starting with downloading Google Authenticator on your iPhone or Android (see images below).



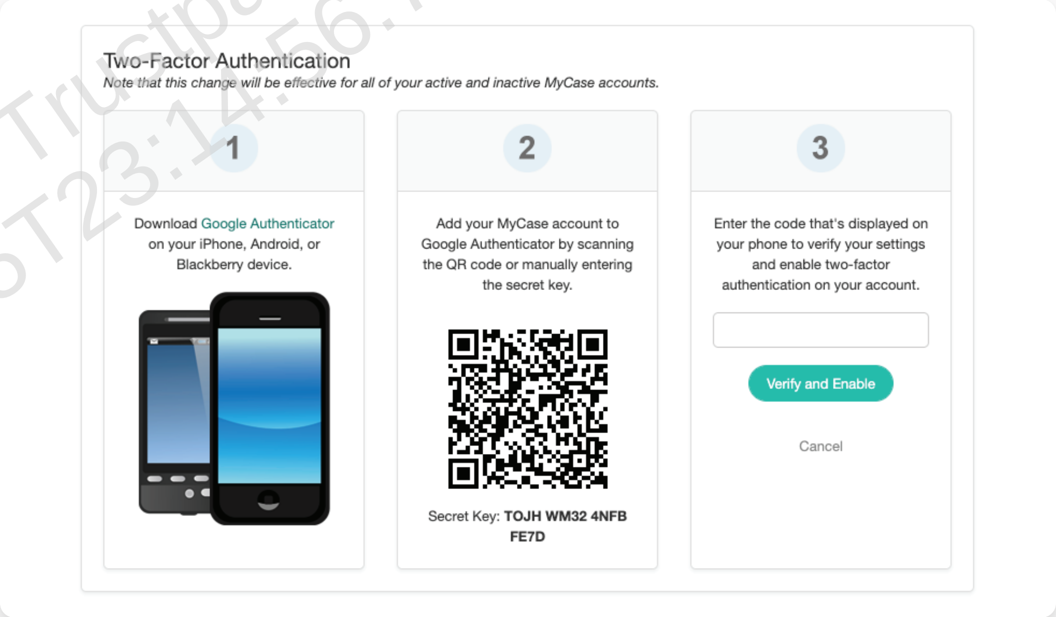
Two-Factor Authentication

Note that this change will be effective for all of your active and inactive MyCase accounts.

Increase the security of your MyCase account by enabling Two-Factor Authentication.

To get started, click the "Enable Two-Factor Authentication" button, then follow the on-screen instructions.

Please Note: You will need a smartphone to enable this feature.



Two-Factor Authentication

Note that this change will be effective for all of your active and inactive MyCase accounts.

1 Download Google Authenticator on your iPhone, Android, or Blackberry device.

2 Add your MyCase account to Google Authenticator by scanning the QR code or manually entering the secret key.

Secret Key: **TOJH WM32 4NFB FE7D**

3 Enter the code that's displayed on your phone to verify your settings and enable two-factor authentication on your account.

4

What You Can Do to Protect Your Data

We hope this guide has addressed any concerns you may have had about data security and cloud computing. The fact remains, however, that regardless of the security measures companies can take to secure your data (whether it's Amazon or even your local Internet Service Provider), the most common cause of data loss is human error.

That's why it's important that you take steps to secure your account (in addition to setting up 2FA):

- Use a strong password (MyCase will even tell you how strong your password is).
- Don't use the same password for MyCase that you use for other software.
- Use at least 10 characters and include a special character, number, and one or more capital letters.
- Don't give your MyCase password to anyone else, and change it often.
- Make sure that no one else has access to your email inbox — otherwise they could reset your MyCase password and gain access to your account.

Should you ever feel that your account has been compromised, contact us right away! We can freeze access to your firm's account instantly, locking out all users until we can ensure that everything is secure. If you still have reservations, see what your peers have to say about how MyCase's security provides peace of mind and is helping to transform their law practice:

> "**The client secure access** was a major reason we switched to MyCase."

- Alan Dobson, DC Metro Immigration Law, PLLC

> "The Client Portal is great for sharing documents and **more secure than email.**"

- Jennifer Antonini, Law Offices of Jennifer Antonini, Ltd.

> "I have peace of mind with MyCase's **highly encrypted security.**"

- Janaan Hashim Esq., Amal Law Group

We understand how important security is to your law firm. That's why multiple security features are built into MyCase. Our goal is to ensure that MyCase is reliable and that your law firm data is protected and secure; that way you aren't distracted by IT concerns and can focus on doing what you do best: practicing law.

Try MyCase Free

Start My Free Trial

*no credit card required

About MyCase

MyCase is a complete, cloud-based law practice management solution, providing the tools you need to collaborate and manage your law firm from anywhere. With MyCase, all of your critical case details — documents, contacts, calendars, messages, tasks, invoices, and more — are easily accessible in a single, organized location.

Learn more at www.MyCase.com

mycase

Give us a call, or email us today
800-571-8062 | sales@mycase.com