



# Security Whitepaper

# Security and Data Redundancy

## At MyCase, Security is Our Top Priority.

Here at MyCase, we understand how important it is to keep our customer's data secure. Dealing with privileged case information isn't a responsibility that we take lightly. **Everything we do is built with security in mind.** It's the fundamental base that we always use as the starting point for any task.

We understand that our customers may be nervous about moving their data to the cloud. It's a new and exciting field, but with that brings a fear of the unknown. Can you really trust an Internet company to protect your data? How secure is cloud-based storage? What's being done to protect your data?

In this whitepaper, we provide an overview of how we address the security and redundancy of your data. It's our goal to put your mind at ease. Yes, you can trust us with your data. Yes, we're as concerned about security as you are. And yes, we're on top of it - the field is always evolving, and you can be confident that we'll be evolving with it, protecting you every step of the way.

### A Brief Overview of Our Security Policies

Physical Security	State of the Art Encryption	Data Redundancy
MyCase runs on Amazon EC2 cloud servers.	All sensitive information is encrypted by MyCase before it's written to disk.	Data is backed up using Amazon S3 storage, providing 99.999999999% durability.
Amazon facilities are nondescript locations protected by military grade perimeters.	We use 128-bit SSL encryption for data transmission and 256-bit AES encryption when storing data.	We perform hourly backups of the entire MyCase database.
Physical access is strictly controlled by two factor authentication and 24 hour security escorts.	Unique keys are generated for every individual document, providing an additional layer of security	Data integrity is validated on every individual update.

## Amazon's Cloud Computing Platform

MyCase is built on top of Amazon's EC2 cloud computing platform (yes, the same Amazon that you use when shopping online). They've got over a decade of experience on running online servers and data centers, so you know you can trust them to be at the leading edge of online service technology.

Amazon has strict procedures in place to protect the physical security of their servers, as well as protecting the integrity of the data they store. By building on their platform, **we gain the benefit of all of their experience and knowledge.** We're not just running on a server in some kid's basement - this is the best of the best when it comes to hosting your cloud-based service.

Amazon has received a number of certifications for their servers. In addition, HIPAA compliant websites have been built on top of the Amazon cloud platform (you know if a website can pass through all of the health care regulations, there isn't much else that it couldn't handle!) Compare that to other companies that host their own servers - how reliable are their facilities? Is their data protected? Or think of trying to run your own local IT department - would you even know where to begin on building a secure storage solution? That's why we defer to the experts here.

You can read more about Amazon's cloud security in their own whitepaper, available online at:

[http://s3.amazonaws.com/aws\\_blog/AWS\\_Security\\_Whitepaper\\_2008\\_09.pdf](http://s3.amazonaws.com/aws_blog/AWS_Security_Whitepaper_2008_09.pdf)

## Experience Counts

The CTO of MyCase has a background in securing data and servers for the US Department of Defense. He understands the importance of securing data, and has the knowledge to prevent unauthorized access and monitor compliance. With over 10 years of experience in developing commercial websites, he's worked through the evolution of the Internet from the dot-com days and has worked first hand with numerous online services.

It's this experience that gives us the confidence that we've built a secure online platform that you can trust. **We're experts in our own right** - top performers in our respective industry. This isn't the first time we've been down this road, and we've seen and learned a lot along the way. We're constantly monitoring the latest security threats, and evolving and adapting our service to address any concerns.

## State of the Art Encryption

MyCase uses two forms of encryption to protect your data. When you connect to our servers, your data is encrypted before transmission using 128-bit SSL connections. **This is the same type of secure connection you use when doing online banking**, investments, health care portals, etc. Encrypting your transmission ensures that nobody can intercept your data along the way, and verifies that you're connected to our servers and not some impostor.

After we receive your data, we use 256-bit AES encryption to encrypt your data before storing it to disk. This is the same level of encryption authorized for storage of top secret military information. Anything sensitive is encrypted before storage - client names and addresses, messages, appointment details, etc. In the highly unlikely case that someone did manage to steal a physical disk drive from an Amazon facility, all they would get from that disk is a bunch of jumbled garbage data.

In addition, we generate a unique key for every single case document that you upload to MyCase. When you delete a document from MyCase, we delete that unique key as well. Even though Amazon may store a redundant copy of that

document on their servers (which may stick around for a few days after you've deleted it), without that unique encryption key, the data is useless. There's no way for an outsider (or us) to recover that deleted document.

## Activity Streams and Audit Logs

All the activity in MyCase is logged in your activity stream. You see this information on your dashboard whenever you login to your account. By monitoring your firm's activity stream, you can notice suspicious activity and take steps to prevent it. Is there a client you no longer trust? Suspend his or her MyCase account immediately and they'll no longer be able to login to the website.

We also monitor every single unique page access on our server. We store the IP address, date/time, and URL of each request. These audit logs are there for your protection in the unfortunate event that you suspect your account has been compromised. We can review the audit logs and let you know the extent of what was accessed, allowing you to take preventative steps immediately.

## Server Access and Monitoring

Our servers are running the open source Linux operating system. Security patches are installed as soon as they become available, ensuring that we're always up to date with the latest fixes. Our servers are protected with a firewall so only the necessary information can pass through. Shell access to our servers is restricted by IP address, so remote access to the server is impossible unless you're physically present at the MyCase office.

We monitor our server logs on a daily basis, allowing us to quickly resolve any issues. We also run a 24-hour monitoring service that checks the health of the server and alerts us immediately to any changes to files or problems with the website. Add nightly virus scans on top of that, and **you can rest assured that your data is safe and our servers are locked down appropriately.**

## What You Can Do to Protect Your Data

No matter how many steps we take to secure your data, **the most common cause of data loss is based on the human element.** It's important that you take steps to secure your own account. Use a strong password (we'll tell you how strong your password is when you change it). Don't use the same password for MyCase that you use for other websites. Don't give your MyCase password to anyone else. Change it frequently. Make sure that other people can't access your e-mail - otherwise they could reset your MyCase password and gain access to your account.

At any time, if you feel like your account may have been compromised, just contact us immediately. We can freeze access to your firm, locking out all users immediately until we can make sure that everything is safe.

## Some Final Words...

We know it seems like a lot to think about, and we know that security is always our customers' top concern. But rest assured that we're working on it. We're always thinking about it and constantly evolving to address new security threats. Compare that to using e-mail to communicate with your client - an unencrypted, insecure platform. Anyone can read your e-mail along the way. There's no auditing and no security controls. Or think about running your own IT department and your own servers... can you really put together a team with more online experience than Amazon?

**We're always here to help.** By working with us and keeping security at the forefront of your mind, we can make sure that your MyCase experience is protected and secure.