



THE INFORMATION CHALLENGE FOR EL CENTRO

It categorized the potentially sensitive data into logical and relevant classification categories and provided a detailed mapping of scan findings (full paths to folders and files) within each category. The output made it very easy for the El Centro IT team and El Centro management to review and verify the scan results.

The Information Challenge

In 2014, El Centro implemented a comprehensive project to provide encryption capability for hard drives, email, and any files and folders that contain sensitive PHI information.

As part of this encryption implementation, the project team made a concerted effort to identify and encrypt sensitive files and folders on El Centro's networked file storage systems. This effort took several months, and when the encryption process ended, there were still nagging doubts about data that may have been missed.

El Centro needed some reasonable way to improve the assurance and confidence in their security protection and compliance status.

The Solution In late 2014, El Centro contacted DocAuthority to scan the stored data as a way to identify and classify any potentially sensitive data in a thorough and cost effective manner.

The entire set up and scan process went very smoothly, with no measurable impact on clinic operations or response times, and the scan output results were impressive. DocAuthority produced a concise summary of all scanned areas, indicating what was found and flagged as sensitive.

There were several items of special note:

- The classification output categories included not only El Centro's requested PHI and PII reviews, but additional potentially sensitive business operations, audit, security and governance-related content.
- Scan results flagged files that, at first glance, looked like false positives (such as files named template or form); however, on close review, these files actually did have field data entries that contained sensitive or personal information. (These most likely would have been missed on manual reviews for potentially sensitive contents.)
- Scan findings were easily grouped into regulatory and compliance items vs. business or operational risk decision items.
- The format and specific content of scan results helped IT expedite remediation efforts and this greatly improved confidence in El Centro's compliance posture.



About Us

Organizations protect the sensitive documents they are aware of, but out-of-sight documents are left unprotected and may fall into the hands of insiders and hackers. DocAuthority solves this by automatically discovering and accurately identifying unprotected sensitive documents, thus enabling a broad yet business-friendly security policy.

Email

hello@docauthority.com

Americas

+1 844 362-2884

3340 Peachtree Road NE,
Atlanta,
GA 30326

International

+ 44 333 050 3241

Hamilton House,
Mabledon Place,
London
WC1H 9BB

Israel

+972 54 744 4803

Ha-Tidhar St 15, Ra'anana,
4365713
Israel

Using DocAuthority has allowed El Centro to make well-informed decisions about exactly what to protect and how within their logical model of desired security, compliance and risk management. Within a very short period, DocAuthority enabled IT to apply encryption where needed, archive or eliminate unnecessary files, and complete their overall encryption project implementation.

The explosion of data is a huge problem for organizations. Now with GDPR-like regulations coming into place, company data is now also a massive compliance risk. DocAuthority enables you to turn these compliance requirements into business opportunities and use them to dramatically improve all aspects of unstructured data usage, management and governance. DocAuthority's revolutionary and patented AI engine quickly and efficiently identifies and creates an inventory of all of your business data with the precision of 99.99%. With ease, you can now accurately identify both data's risk and its value and automate its ongoing classification, protection and retention while improving accessibility and quality.

