

# Redaction

## Defined:

**Meeting Information  
Disclosure Requests with  
Secure Content Delivery**

*An IGC White Paper*



## Accessibility of Electronic Content

Today's technology has made it easier than ever to share and access data. Email, high speed internet, blogging and other social networks and neutral formats like PDF make it easy to share content anywhere, anytime. Even when you would rather not.

With greater convenience comes increased risk of misuse of data. How can you protect sensitive content when so many people need to have access to the information? Sensitive content includes:

- intellectual property
- personal information (e.g., social security numbers)
- account numbers
- financial data
- confidential data

## Risks of Content Security Breach

The risks of unintentional disclosure of sensitive content can be severe and costly. Some of the key risk discussed here are:

- identity theft
- non-compliance
- loss of competitive advantage
- compromised security / loss of intellectual property
- embarrassing press
- litigation

### ***Identity Theft***

Protecting sensitive information is critical in helping to prevent Identity Theft. According to the February 2007 Federal Trade Commission (FTC) Report on Consumer Fraud and Identity Theft Complaints, 2006 was the seventh year in a row in which Identity Theft was the number one complaint received by the department. Of the total 674,354 complaints received in 2006, 36% were due to Identity Theft (246,035 complaints).

The FTC estimates that nearly nine million people have their identities stolen each year. This number equates to substantial losses in time and money both for businesses and individuals:

- Loss to businesses: \$52.6 billion
- Loss to individual victims: \$5 billion
- Hours victims spent resolving their problems: 297 million<sup>2</sup>

### ***Non-Compliance***

Corporate accounting scandals and high profile law suits have resulted in new government regulations on how much information must be publicly available, and more specifically, available online. Such regulations include:

- Freedom of Information Act (FOIA)
- Openness in Government Act of 2005
- Privacy Act
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley Act of 2002 for Financial and Accounting Disclosure Information
- Gramm-Leach-Bliley Act of 1999 for Financial Services Modernization
- Federal Information Security Management Act of 2002 (FISMA)

Posting sensitive information in public arenas, such as the Internet, without redaction, exposes the document owner to customer distrust and potential litigation from customers affected by malicious use of their personal information.

### ***Loss of Competitive Advantage***

There are a number of examples illustrating the danger of exposing internal strategies and campaigns. Case in point: confidential competitive strategies designed by Whole Foods to take market share from low-cost leader Wal-Mart were revealed in a PDF document the Federal Trade Commission's (FTC) legal organization filed with the court electronically. In the document, words intended to be inaccessible were just electronically shaded black rather than truly redacted -- a common mistake. The suppressed words in versions downloaded from court servers were copied into Notepad and with the blocked text fully visible.

Had Whole Foods provided the necessary documents to the FTC with sensitive content already properly redacted, this may have been avoided.

### ***Compromised Security / Loss of Intellectual Property***

A Lockheed Martin employee lost a USB thumbdrive at a gas station containing data on the F-35 fighter, including diagrams of the jet's fuselage, engine, wiring, firing system and propulsion system. While it appears no one intercepted the

thumbdrive, which was found at the gas station by a trucker and turned in, this illustrates just how vulnerable content is, even in the hands of responsible, well-intentioned employees.

### ***Embarrassing Press***

There have been numerous examples of insurance and mortgage companies having to publicly admit to having servers stolen containing the privacy information of thousands of customers. In June 2006 the American Insurance Group (AIG) reported that a server containing the social security numbers and medical records of 930,000 customers was stolen. In these cases, the press coverage can scare away potential customers, on top of the damage caused by the actual breach. Such press can shake the faith of stockholders and customers and demand expensive and time-consuming investigations into what went wrong.

### ***Litigation***

In October of 2004, database giant ChoicePoint had a server stolen containing the detailed personal information of over 145,000 Americans. After a Senate Judiciary Committee investigation, the company settled with the Federal Trade Commission for \$10 million in civil penalties and \$5 million for consumer redress. At least one victim was seeking a class action lawsuit.

In the healthcare field, a disgruntled employee of Kaiser Permanente posted information on her blog noting that Kaiser Permanente included private patient information on systems diagrams posted on the Web, resulting in fines by the California Department of Managed Health Care for exposing the confidential health information.

## **How to Protect Sensitive Information**

Protecting electronic content is challenging and can involve a combination of physical security of servers, network security, document management with user rights and strongly enforced policies. But many content security breaches are outside of these systems. Intercepted thumbdrives or disks (on the way to contractors, for example), stolen laptops and inappropriate content on public websites are alarmingly common. How can these be avoided?

### ***Proprietary vs. Open Formats***

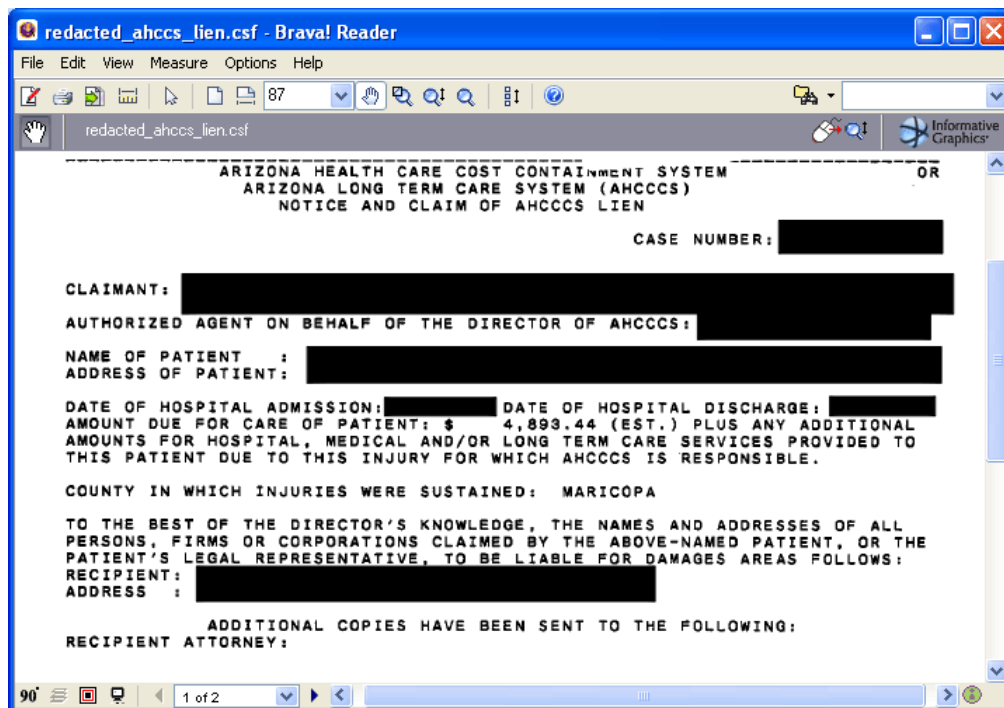
Open formats, like TIFF and PDF, make it easy to share data. There are many applications that can create and view these files and they are ideal for many uses; however, because they are publicly shared formats, there are also many software programs that can edit these files. There are even applications that can open password-protected files.

Proprietary formats are not shared with third party software companies. Only the originating company can create products that create or view these formats. Proprietary formats are better-suited for short-term, secure content sharing. A proprietary format that is encrypted and has security options (like password protection, an expiration date, and feature restrictions) is more secure than an open format.

## Redaction

Electronic redaction identifies and blocks or removes sensitive content from documents. Electronic redaction can be manual or automatic. Manual programs are best for handling a small number of documents while automatic programs work best for large batches and as part of a workflow.

Best practices for redaction generally include creating a copy of the document in a neutral format (e.g., PDF, TIFF, JPG) while the original remains secure and complete. Utilizing a neutral format copy for redaction ensures no metadata (hidden text including revision history and document information) is retained and that the original document is not altered. Ideally, the redaction completely removes, rather than just covers, the sensitive content. This way it cannot be hacked or compromised in any way.



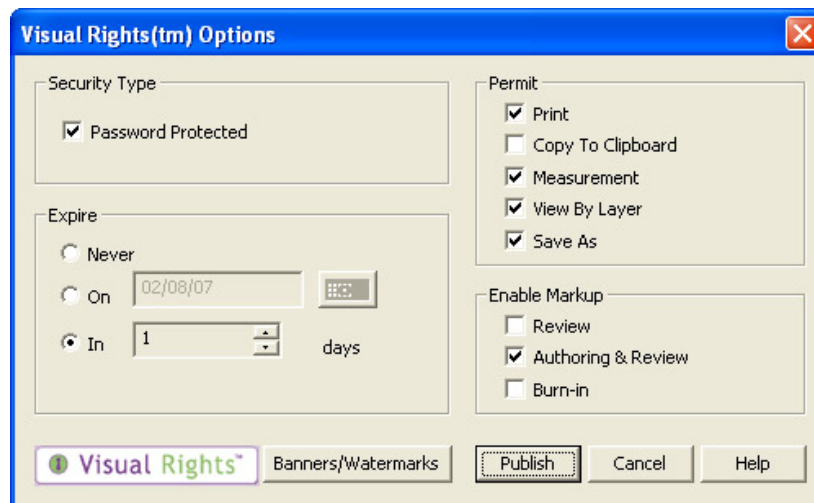
Example of electronic redaction

## Informative Graphics' Content Security Solutions

### Content Sealed Format

Content Sealed Format (CSF) is an encrypted, compressed format that incorporates our Visual Rights® technology. CSF is a proprietary format which can only be created or viewed by our software. There are no third party editors for this format.

When creating CSF files, users can choose to password protect or expire the file, allow or disallow many features like markup and printing, and add a watermark or banners to display copyright or other information. Because only our viewers support this format, there is no way to circumvent these settings.



### Redact-It

IGC offers products for simple desktop redaction, a plug-in for scanning or image capture software and a server-based product for automated, batch redaction. Redactions are always performed on a rendition of the source file, so the original is left untouched and secure. Users can save redacted files as TIFF, PDF or CSF.

Our redaction technology completely removes sensitive content and no metadata or document properties are transferred to the redacted file.

**About the Author**

Gary Heath is CEO of Informative Graphics, a leading developer of commercial software products for content visualization, secure publishing and collaboration. Founded in 1990, Informative Graphics products are deployed by thousands of corporations worldwide.



For more information, please contact:

**Informative Graphics Corp.**

4835 E. Cactus Rd

Scottsdale, AZ 85254

Phone: 800.398.7005 (intl +1.602.971.6061)

URL: [www.infograph.com](http://www.infograph.com)

eMail: [sales@infograph.com](mailto:sales@infograph.com)