

## Memo of Meeting

Date: January 17, 2002

Representing Alchemedia Technologies, Inc.:

Daniel Schreiber, Chief Executive Officer  
H.E. Buddy Wilson, Sr. VP, Business Development  
Dave Carlson, Director, Business Development

Representing FDA:

Charles A. Snipes, Compliance Officer, Center For Drug Evaluation and Research  
Dennis M. Dignan, Consumer Safety Officer, Center For Food Safety & Applied Nutrition  
Aydin Orstan, Consumer Safety Officer (detailed to Office of Enforcement from CFSAN)  
James McCormack, Consumer Safety Officer, Office of Enforcement  
Jeff Smith, Project Officer- Regulatory Systems, Center for Biologics Evaluation and Research  
Paul J. Motise, Consumer Safety Officer, Office of Regulatory Affairs

The meeting was held at the request of the Alchemedia representatives, to discuss their electronic records management product (Mirage) in the context of 21 CFR Part 11. At the start of the meeting we explained that FDA does not formally review, approve or disapprove of products or services that enable people to comply with FDA regulations. We advised that the meeting would be an information exchange and that our comments should not be taken as formal FDA positions.

The Alchemedia representatives explained that their four year old company produces an electronic document management program that is intended, among other things, to help the FDA regulated industries meet 21 CFR Part 11 requirements. Most of the firm's customers are regulated by FDA.

The Alchemedia representatives described the problems with electronic records that their software is intended to address: data confidentiality and data currency. They explained that unauthorized information disclosures derive mainly from within an organization; the ease of electronic record duplication and dissemination increases a firm's vulnerability to this problem. Likewise, such dissemination and replication of records within an organization, coupled with the ease of electronic record modification, increases the likelihood that employees

will work with outdated copies of electronic records that are stored on local computers. Records mutate and propagate in poorly controlled environments.

The Alchemedia representatives commented that, according to a study by Price Waterhouse Coopers, the above problems of data confidentiality and currency cost the Fortune 1000 companies about \$15 million per company.

The Alchemedia representatives explained that their software product, Mirage, is a web based client/server application. The program, by working together with server based Livelink document server, enables system administrators to determine who can print, forward, save, or screen capture an electronic record. End users may display the record locally, but further actions can be restricted. The representatives gave us a brief demonstration of how a restricted electronic record could be viewed, but not saved or copied to a Windows clipboard. Unauthorized attempts at record copying, printing, saving or forwarding generate encrypted versions of the record. The record remains encrypted in RAM but decrypted at the video driver level. Attempts to perform a screen capture of protected records results in a display of a pattern of Mirage software logos. Record protection is configurable down to sub-documents, and employs the advanced encryption standard and RSA authentication algorithms. A computer that did not have the client code installed would not be able to view the record from a server that did have the application installed.

The firm's software performs in a like manner with Documentum, and functions on any web based application in the Windows, Solaris and Sun computing environments. The Alchemedia representatives commented that their program does not alter the electronic records themselves nor the records' associated digital signatures. End users see a "Mirage" of the electronic records in native HTML or PDF format, in that they can view, but not "touch" the records. In addition, a record may be rendered unreadable upon a configurable expiration date.

Regarding audit trails of end user privileges, the representatives commented that the next release of their product would include that feature.

During the meeting we discussed the firm's validation efforts. The representatives said they would welcome customer audits of their software development activities. The firm will also provide software test scripts upon request.

We commented that many of the requirements implemented in Mirage which were being attributed to Part 11 were, in fact, necessitated out of long standing predicate rules.

The meeting lasted about two hours.

Attached to this memo are two PDF files of material provided by the firm; a white paper entitled "The Business Case For Deploying Mirage In Pharmaceutical Companies", and flyer entitled "Control is an Illusion, Mirage and Documentum Overview".

cc:  
FDA Attendees  
HFA-224  
Part 11 Guidance Dockets

Doc ID AlchemediaMemoOfMeeting011702.doc  
P. Motise 01/28/02



at Docuat Docu

# The Business Case For Deploying Mirage in Pharmaceutical Companies



December 2001

# The Business Case For Deploying Mirage in Pharmaceutical Companies

---

This document is intended to facilitate an assessment of the benefits of integrating Mirage into existing or planned document management systems in the Pharmaceutical Industry.

## Overview

The pharmaceutical, biologics, blood products, and medical devices industries (collectively, the Pharmaceutical Industry) face increasing regulatory agency requirements for rigorous document management and tracking. The advent of widespread distribution and use of electronic documents has made compliance with these requirements much more difficult. One daunting challenge is the assurance of correct version use in an environment where unauthorized or “rogue” copies of documents are commonplace. Exacerbating this problem is the presence of 21 CFR Part 11, which requires audit trails and authorizations, neither of which exist for rogue documents.

The cost of rogue documents is real and substantive, but fortunately, there are mechanisms to prevent them. One such solution is Alchemedia’s Mirage™ Enterprise, a system that serves encrypted copies of documents to distributed workstations. Client software on each workstation decrypts the documents for use only by authorized users, while simultaneously disabling local print functions for unauthorized printers. This combination of encryption and local print management serves to prevent rogue documents and assures correct version use by restricting use to on-line, current versions. The benefits

of a Mirage system include the strong, demonstrable protection of document and data confidentiality, the reduced cost of compliance, reduced product, data, and time loss due to incorrect version use, and the reduced risk of regulatory citation.

## The Need for Stringent Document Management

The Pharmaceutical Industry faces the challenge of complying with ever more stringent regulatory requirements for rigorous information management. In particular, Standard Operating Procedures (SOPs), protocols, and specifications must be meticulously tracked and controlled.

The USA’s FDA, the UK’s MCA, the EU’s EMEA, Japan’s MHLW and other regulatory agencies (collectively, “the Agencies”) require organizations to provide extensive documentation, as well as evidence that “only the right people are using only the right documents.”

In more formal document management terms, this means that while providing extensive documentation, the Pharmaceutical Industry must also ensure two other things in their clinical, laboratory, and manufacturing operations (collectively, “operations”), namely:

- **Currency:** That people use only approved and current versions of documents.
- **Confidentiality:** That only approved users have access to confidential documents.

It is this need to ensure both currency and confidentiality while also providing extensive documentation that creates a very real problem for these companies.

## Ensuring Documentation Currency

In a regulated environment, the Agencies generally operate under the axiom that “If it isn’t written down, it never happened, and if it is written down, it did happen.”

### If It Isn’t Written Down, It Never Happened

The Agencies routinely presume that a lack of rigorous documentation concerning an activity is equivalent to the activity itself not having been performed. Accordingly, it can and does happen that regulatory actions are based not on actual physically adulterated products but upon presumptively adulterated products—the presumption being made due to a lack of rigorous documentation.

In response to this enforcement policy, pharmaceutical companies have developed intricate and pervasive systems for distributing officially issued copies of SOPs, specifications, and standards, etc., to all areas of their operations.

### If It Is Written Down, It Did Happen

However, it is also important to note, that the Agencies also generally presume that local documentation reflects what occurs (or has occurred) locally. This means that if local copies of procedures or specifications differ from the officially approved, centrally issued copies, inspectors presume that the local documentation is applicable. Accordingly, when local and central documents do differ, it is almost certain to result in an observation of non-compliance with applicable regulations.

Therefore, not only do companies have to ensure that everything that happens is documented, they also have to ensure that everyone is using officially approved, centrally issued copies of that documentation.

In order to ensure that only correct and current documents and versions of documents are distributed (or in document management parlance, “issued”), and that superseded or incorrect ones are removed from service, organizations have typically relied on classic, centralized document issuance systems that include:

- Document distribution lists and schedules
- Pre-positioned official document binders or files
- Controlled paper stock for “official copies”

- Procedures to “copy mark” copies of official documents
- Expiration dating of documents to prompt reissuance
- Document existence and currency audits

However, these practices are very labor intensive, and are encumbered with the associated high costs and high error rates of any such intricate and dispersed manual process.

## Electronic Systems Reduce the Burden of Extensive Documentation...

Acting to mitigate these costs and errors, some organizations have deployed systems to automate the issuance of documents. These systems, which require that the original documents be created using network-attached computers, fall into two basic types:

- **Electronic Document Filing System (EDFS):** This is a system where documents are created on-line but are manually routed, reviewed, signed and filed, etc. In this type of system, physical copies of documents are printed and then signed on paper, while electronic copies are retained on the computer network and are made available for limited or widespread use. Generally, if a company requires on-line access to approved, active documents, locked copies of these documents are placed in a secure, shared file area, known as a vault. They can then be accessed for read-only use by authorized users.
- **Electronic Document Management System (EDMS):** Similarly to EDFS, an EDMS generally manages a vault of approved, active documents. However, in a substantial improvement upon an EDFS, an EDMS includes mechanisms that both enforce access restrictions at a highly granular level and log access to the documents.

An EDMS also manages and tracks all of the document creation, editing, routing, approval, and issuance processes. Most EDMSs do this using a check out/check in scheme, where copies of documents are “checked out” (or forwarded) to editors, and then “checked in” (or received) from editors as later revisions that include modifications.

## ...While Increasing The Collateral Risk

Bearing in mind the axiom, “If it is written down, it did happen,” both EDFS and EDMS introduce a substan-

tial risk to the challenge of ensuring document currency and confidentiality. This is because both types of system require a user to transfer copies of documents to local workstations, whether for editing or viewing. This in and of itself increases the risk of creating uncontrolled or “rogue” copies of a document.

A rogue document is created when a controlled document, in any of its various file formats<sup>1</sup>, is transferred to a local workstation. Once on a local workstation, it is outside the direct control of the EDFS or EDMS. The local user can then retain a working copy of the file, or can locally print it. Both the electronic and paper copies are known as rogue documents.

There are several types of rogue documents, as follows:

- Expired documents, which are documents that are out-of-date or that have been superseded by more current documents or versions
- Mutant documents, which are documents that have been edited by unauthorized editors or have not been centrally tracked
- Bootleg documents, which are confidential documents that have been disclosed to unauthorized individuals or organizations

All three types of rogue documents produce substantial costs in time, labor, money and regulatory risk.

### Expired Documents

Almost universally, the Agencies require “periodic review” of procedures, standards, and records associated with the operations. Most organizations accommodate this requirement by placing expiration dates on documents to trigger their review and re-issue. Centralized EDFS and EDMS operators re-issue documents as required and distribute the revised documents, or notices of the revisions, to authorized users.

The existence of rogue documents disrupts this system. When authorized users maintain personal paper copies of documents, they tend to rely on their copies and overlook the broadcast of updated revisions. In order to counter this tendency, pharmaceutical organizations

1. Copies for editing are usually in the form of native files. Copies for viewing only are in either native, HTML or PDF format. It is important to note that HTML and PDF formats are not an adequate defense against electronic rogue documents. An HTML document can be saved and printed as easily as any other format, and even a PDF that has been protected using Adobe Acrobat's Standard Security can be forwarded to anyone, or screen captured at will.

spend substantial amounts of time and labor maintaining and auditing local binders of paper documents.

Some companies depend upon an EDMS and attempt to limit local paper copies. However, in an EDMS environment electronic copies of documents are often left on local computers as the residue of the check out/check in procedure. In addition, most systems actually permit the creation of local unauthorized electronic copies via the “Save As” function. Thus it is very difficult to prevent the creation of rogue copies of documents.

Organizations are left with the choice of relying on procedural controls and the good intentions and attentiveness of end users. Experience has shown both to be insufficient.

### Mutant Documents

Mutant documents occur much less frequently than expired documents, but their effect is much more profound.

For example, see the following incident:

“We encountered one situation at a major pharmaceutical manufacturer that merits review. It seems that for one of their diagnostic products, a critical manufacturing step required considerable skill on the part of the operator to accommodate raw material variability. The lead operator (we'll call her ‘Alice,’ which is not her real name) had worked out a system to get the process to perform, but was severely admonished by her supervisor ‘not to cause trouble’ by submitting ‘\*%&^@#%! change request paperwork’ that made life miserable for said supervisor. Wanting to be consistent, Alice copied the published, unworkable procedure, marked it up with the workable process steps, and kept it handy for producing the product. She did not submit the marked-up procedure to QA for edit, review, and approval by the Change Board.

“This system worked well for more than one year, until Alice left for a two-week dream vacation in Hawaii, and Bob (again, we use a fictitious name) had to substitute for her and produce several lots of the ‘difficult’ product. Bob meticulously followed the published procedure (not Alice's mutant markup) and produced several non-performing lots of diagnostic reagent, which had to be scrapped and written off as a loss. Upon Alice's return, the problem was quickly resolved.

“Besides losing over \$100k of production, the company also exposed itself to a substantial regulatory risk, when its non-conforming material investigation was required to formally document that actually following the pub-

lished procedure caused the product failure. By implication, the corrective action that the company was required to perform also established that all of the previous lots were manufactured using improper documents, and that the SOP system was uncontrolled.”<sup>1</sup>

### Bootleg Documents

The least visible but most costly rogue documents are bootlegs. In simple language, they are simply stolen intellectual property. Organizational costs associated with bootleg documents include:

- Civil and criminal liability for unauthorized disclosure or personally identifiable information, including medical records and personnel records
- Loss of corporate prestige and position due to breaches of privacy
- Competitive disadvantage due to loss of proprietary sales and marketing information
- Loss of patent protection as a result of disclosure
- Success of outright industrial espionage and loss of product pipeline

With per-incident losses measuring in the tens of millions of dollars<sup>2</sup> and with 90% of information leaks originating with bootleg copies<sup>3</sup>, companies need to eliminate bootleg copies.

## 21 CFR Part 11 and Rogue Documents

In August of 1997, the FDA’s 21 CFR Part 11<sup>4</sup> “Electronic Records; Electronic Signatures” (Part 11) changed the entire landscape of document management.

With Part 11, the FDA requires the Pharmaceutical Industry to institute controls over electronic documents that are no less stringent or reliable than those in existence for paper documents<sup>5</sup>. In addition to these controls, for the first time the FDA establishes in a regulation a requirement for validation of a second-tier system that does not have direct product or patient con-

tact<sup>6</sup>. Throughout § 11.10, which describes controls for closed systems, the FDA establishes a plurality of requirements, including that of an unalterable audit trail of all actions that “create, modify, or delete electronic records.”<sup>7</sup>

Since rogue documents are by nature outside the control of an EDFS or an EDMS, it is not possible to generate an audit trail of actions that create, modify, or delete them, and therefore rogue documents are by their very nature not compliant with Part 11.

In essence, through Part 11, the FDA has outlawed rogue documents, and companies are required to institute controls to prevent them from being created and used. Companies can expect to be cited for non-compliance if any expired, mutant, or bootleg documents are found during an inspection.

### How Using An EDFS or EDMS Amplifies Part 11 Risks

Even the most robust EDMS does not stop users from copying read-only documents. Copying can be done in many different ways. This can take the form of clicking the mouse in a word processor; cutting and pasting in a browser window (indeed, all browsers even allow a simple Save command, removing the need to cut and paste); or using screen capture or print screen features. These methods all create rogue copies of documents.

Many companies attempt to control this problem with procedures that prohibit local retention of document copies. However, real world experience teaches that people do not adhere rigidly to such document management policies. And when even a seemingly “minor” deviation from established document management procedure creates a rogue document that is difficult or impossible to distinguish from the official original, the

---

1. B. Meserve and T. Quinn, Co-Instructors, “Implementing EDMS for Pharmaceutical Manufacturing,” PDA Training and Research Institute, 2000

2. PricewaterhouseCoopers/ASIS—Trends In Proprietary Information Loss 2000

3. FBI/CSI Computer Crime and Security Survey 2001

4. [http://www.21cfr11.com/library/government/21cfrpart11\\_final\\_rule.pdf](http://www.21cfr11.com/library/government/21cfrpart11_final_rule.pdf)

---

5. The FDA’s emphasis on document integrity in its Part 11 compliance guide underscores its concern that data integrity and product quality depend upon effective electronic record-keeping procedures. “FDA will consider Part 11 deviations to be more significant if...the deviations make it difficult for the agency to audit or interpret data, or if the deviations undermine the integrity of the data or the electronic system.” Compliance Policy Guide Section 160.850, Enforcement Policy: 21 CFR Part 11; Electronic Records; Electronic Signatures (CPG 7153.17). [http://www.fda.gov/ora/compliance\\_ref/cpg/cpggen/cpg160-850.htm](http://www.fda.gov/ora/compliance_ref/cpg/cpggen/cpg160-850.htm).

6. 21 CFR § 11.10 (a) “Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.”

7. 21 CFR § 11.10 (e)

hope that “rogues won’t happen” is at best naïve, and at worst, negligent.

This risk is amplified by other sections of the regulation. Part 11 requires strict controls over electronic document processes and it requires audit trails of processing steps that are searchable during inspections and regulatory actions. In order to be compliant with Part 11, both manual EDFS transactions and automated EDMS transactions must produce audit trail entries whenever documents are checked out of the vault. These audit trail records provide a readily accessible roadmap for the search for rogue documents. Armed with a list of checked out documents sorted by user or workstation, it is a straightforward task for an auditor or inspector to locate rogue copies of official documents on local workstations.

This risk is not conjecture. The FDA has already explicitly cited companies for Part 11 violations where records may be easily altered in a way that is “difficult to detect,”<sup>1</sup> where edit authorization rights “were available to unauthorized users,”<sup>2</sup> and where controls were inadequate to assure that “changes in records are instituted only by authorized personnel.”<sup>3</sup>

The risk of significant regulatory action is immediate and credible; all the more so as Agency personnel are becoming steadily more skilled at inspecting automated systems.

## Mirage Eliminates Rogue Documents

Fortunately, rogue documents, along with their associated costs, are not inevitable. While allowing users to access documents in the normal manner, Alchemedia’s Mirage Enterprise software effectively stops the unauthorized creation of electronic copies. It also controls and audits who is allowed to print what documents, how many times, with what watermark, and on which printer.

Mirage software integrates smoothly with an existing EDMS and extends its roles-based-rules. Moreover, Mirage allows a company to control and audit not only

what happens in its EDMS, but also on the thousands of personal computers that have access to that system.

With Mirage, companies need no longer worry about rogue documents circulating on personal computers throughout the organization—or beyond. By providing control over documents that are in use, Mirage helps ensure that only the right people use only the right documents.

### What Is Mirage?

Mirage ensures data confidentiality by protecting proprietary information from theft and misuse and ensures data currency by preventing out-of-date information from being circulated. Mirage does this by:

- Preventing the unauthorized copying, e-mailing and screen capturing of documents
- Enabling secure printing of a protected document or preventing printing altogether
- Preventing unauthorized document duplication
- Rendering documents unreadable when a pre-defined expiry date has passed

The Mirage system consists of two components which integrate seamlessly with your network:

#### The Mirage Server

The Mirage Server intercepts the browser’s requests for documents, retrieves the documents and encrypts them before sending them to the browser.

The Mirage Server offers a flexible and scalable architecture, which is especially useful for load balancing configurations and for environments with multiple servers across the enterprise.

#### The Mirage Client

The Mirage Client enables a protected document to be decrypted and then securely displays it in the browser, preventing the end user from unauthorized copying, saving, printing, e-mailing and screen capturing the protected document.

The Mirage Client component is installed inconspicuously onto any number of workstations using standard desktop-deployment tools, where it runs at the operating system level. By decrypting information at the last possible opportunity, Mirage delivers a higher level of

---

1. Linweld, Inc., File KAI #99-023
2. Schein Pharmaceutical, Inc., File 00-NWJ-22
3. Integrity Pharmaceutical Corporation, File 2000-DT-27

security compared with systems that encapsulate information and require a proprietary viewer.



To ensure documents are securely encrypted, Mirage uses keys which are company specific. This means that an encrypted document in Company A cannot be read at Company B, even if Mirage is installed in both places.

Mirage’s modular architecture, standards-based protocols and rich API suite allow it to be easily integrated into most collaborative applications—such as corporate portals, supply chain management, document management and B2B exchanges. This straightforward technological integration is supported by Alchemedia’s rich partner program, which includes CoVia, Documentum, Hummingbird, Netegrity, Open Text, Oracle, SPSS MR and Sybase.

## Case Studies

The following examples represent typical problems that can manifest as the result of rogue documents. The situations have been modified to conceal company and individual identities.

### Expired and Mutant Documents

**Problem 1:** The Acme medical device company received complaints about a hip replacement device with a higher than expected fracture rate. The manufacturing process was modified in November 1998 to reduce the expected fracture rate. Additional complaints for the same problem were received in mid-1999.

The complaint investigation uncovered the following facts:

- In January of 1999 Bane, a sub-contract manufacturer facility, began manufacturing these devices.
- The suspected device manufacturing lots were traced to the Bane plant.
- The Bane plant was originally qualified in August 1998 using the old SOP, i.e., it did not have the modified manufacturing process.

The QA investigation of Bane’s processes and documentation uncovered a procedural deficiency in the distribution of SOPs. Although modifications to the SOP were distributed to Bane’s Document Control group via encrypted e-mail and posted on their internal intranet and an internal e-mail was distributed to inform manufacturing of the change, manufacturing continued to follow the old “paper” SOP.

**Problem 2:** The example given in “Mutant Documents”, where Alice created an unofficial SOP, illustrates the substantial costs that can be incurred as a result of mutant documents. In the situation that is described there, the company had an EDMS, but the rogue document was a paper copy and therefore outside the EDMS’s control.

**Cause 1 and 2:** Problems 1 and 2 have the same root cause, which is an open loop in the document revision system. Changes can be broadcast, but there is no mechanism to ensure that changed documents are fully deployed.



The effects of expired and mutant documents in a regulated manufacturing situation are very similar. Both types of rogue documents can be avoided.

**Solution 1 and 2:** One way of preventing either expired or mutant SOPs is to provide only on-screen access to SOPs. If people can only access documents via the workstations, this would eliminate the “paper reference” (a.k.a. rogue) copies. The challenge here is ensuring that the electronic copy is truly the only copy of the SOP that is used.

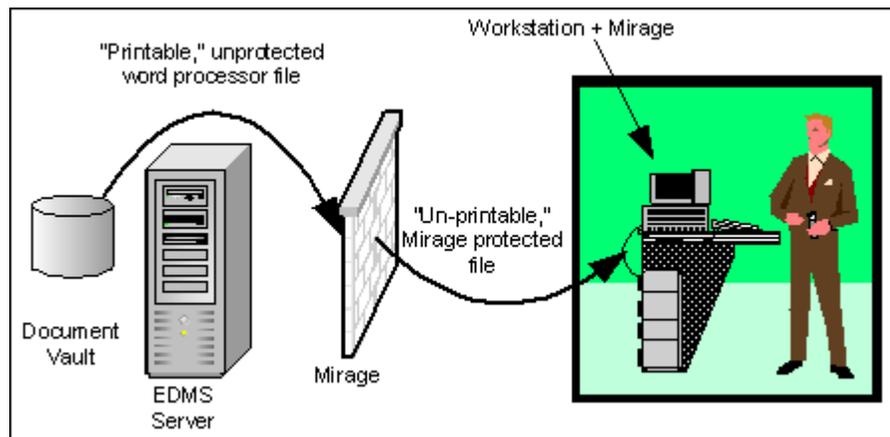


Figure 1: Typical Mirage Deployment in Regulated Manufacturing

In such a situation, you can use Mirage to ensure that only electronic copies of SOPs are used. As shown in Figure 1, Mirage can ensure that all documents that are delivered to the workstations in the manufacturing areas are protected against copying and printing, as well as screen capturing.

## Bootleg Documents

**Problem 3:** Crocorp is a contract research organization that is conducting a very large, international clinical study<sup>1</sup>. Al, one of the data management directors, has been working closely with Beth, the clinical research director, to improve clinician compliance with the patient recruitment SOP. The statistics group has noted some trends, possibly even bias, with some recruitment.

Al has had several meetings with Beth to correct the situation, and they have reviewed several of the reports that data management/statistics has issued.

In response to the problem, Beth has designed a training program that includes a PowerPoint presentation. Beth will personally “take it on the road” and deliver to the clinical sites participating in the study. She has 21 sites to train.

Virtually all of the sites request copies of the presentation, so that they can train staff who could not make it for Beth’s visit, and Beth happily obliges.

Unfortunately, in her haste, Beth sometimes copies her entire “Recruitment Retraining” folder (instead of just the “Recruitment Retraining” presentation file) to a disk for the clinical site. Even more unfortunately, this folder contains many of the query results and reports from Al and Beth’s analysis of the recruitment problem.

Because of this situation some clinicians become aware of their own or of other clinicians’ recruitment compliance performance. Some unguarded comments at an industry conference lead to some very terse telephone calls to Crocorp’s chief medical officer.

One clinical site is actually a large university hospital. At this site, one of the research quality assurance associates learns of the existence of the files, obtains a copy of them, and performs her own analysis. She quickly realizes that by sorting the data by patient number, recruitment date, and recruitment site, and then comparing this to the hospital’s records, she can easily associate patient names with patient numbers. Concerned about this possible lack of blinding, she e-mails Crocorp’s Vice President of Quality Assurance.

**Cause 3:** The root cause of this problem is the security deficiency in Crocorp’s system that permits unauthorized access to confidential data.

**Solution 3:** Mirage can be used to prevent unauthorized access to confidential data. Files that are protected by Mirage are sent to the browser in an encrypted format,

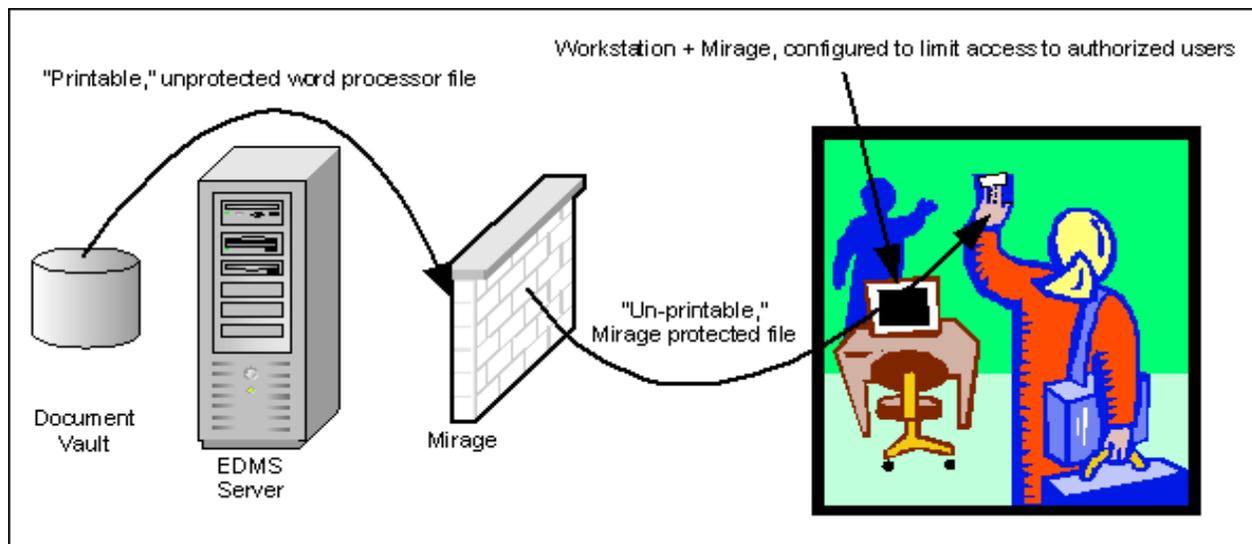


Figure 2: Typical Mirage Deployment To Ensure Document Confidentiality

and can only be read after decryption. Unauthorized users simply do not have the correct keys to decrypt the data. Furthermore, even authorized access to protected files can be restricted to expire after a certain time period, after which time the file is no longer decrypted in the browser.

In the problem described at Crocorp, putting such a solution in place (i.e., using Mirage to protect files on the EDMS) would have resulted in unauthorized users being unable to read the confidential data that Beth mistakenly gave them.

## Why Use Mirage?

Pharmaceutical companies are continuously challenged to find ways to reduce risk. The direct benefit of using Mirage is the reduction of risk caused by rogue documents in several key areas:

- **Productivity:** By using Mirage, companies can significantly increase the compliance of the multiple locations with document version assurance policies. Mirage provides the technology to assure that only

current versions are used for current operations. This reduces the risk of productivity loss due to re-work or rejection resulting from staff using expired or mutant procedures and specifications. Mirage automates the task of version assurance, which when done manually is tedious, expensive, and error-prone.

- **Confidentiality:** Mirage encrypts documents and assures that only authorized people can access them. This provides companies with the benefit of protection against loss due to unauthorized disclosure of confidential, personal information. Mirage also protects the market position of companies by preventing competitors from accessing confidential procedures, specifications, and data.
- **Prestige:** Pharmaceutical companies rely on the public's trust in order to do business. A large part of this trust can be lost as a result of product recalls, unauthorized disclosures, and regulatory actions. Mirage's capabilities to protect productivity and assure confidentiality provide the benefit of protecting a company's prestige and position of trust.



© 2001 Alchemedia Ltd. All rights reserved. Alchemedia, Mirage, Secure Display, "Security is an Illusion" and all logos are trademarks of Alchemedia Ltd. All other product names are trademarks or registered trademarks of their respective owners.

Patent No. 6298446

Alchemedia Technologies, Inc.  
215 West College St., Grapevine, TX 76051  
Tel: 817-442-8552  
Fax: 817-442-8542 or 415-864-3746  
[www.alchemedia.com](http://www.alchemedia.com)  
[info@alchemedia.com](mailto:info@alchemedia.com)  
(P/N A1129)

### **The Problem:** *Control is an Illusion™*

Documentum drives content management through e-businesses with an open, flexible, Internet-scale platform that enables users to create, deliver, publish, and personalize content in all formats across all e-business applications. Existing Documentum WebPublishing users are utilizing Documentum's versioning, workflows, lifecycles, and publishing configurations to automate the process of publishing documents on their Web sites. Documentum protects content through a combination of user- and role-based security, as well as extended permissions that control how content is accessed and modified. Documentum 4i supports LDAP, along with SSL, digital certificates, and electronic signatures for approving and routing content and meeting regulatory requirements. However, once that content is accessed, it inevitably reproduces, evolves and travels without a trace, resulting in unauthorized copies, which populate your organization and beyond. The propensity of digital documents to replicate and travel, therefore, carries severe implications for Data Confidentiality and Data Currency.

### **Data Confidentiality:**

According to the FBI, 90% of information leaks occur due to authorized insiders. The damage they cause is the single costliest security problem facing enterprises today, resulting in 10 times more damage than system penetration by hackers, 18 times more than viruses and 36 times more damage than Denial of Service attacks

### **Data Currency:**

In many industries, documents need to be carefully controlled – either to meet regulatory compliance requirements (e.g., 21 CFR Part 11) or in order to ensure quality standards and best business practices. Many companies have suffered fines, closures, product-recalls and lawsuits as a direct result of someone relying on outdated copies stored on their local computer (e.g. Standard Operating Procedures, Material Safety Data Sheets or Maintenance Procedures and Records). In addition, all businesses need to be able to control – and at times retrieve or destroy – key documents. Celebrated lawsuits have hinged on digital records that were impervious to deletion – having replicated beyond their owner's control or knowledge. The resultant losses are often staggering.

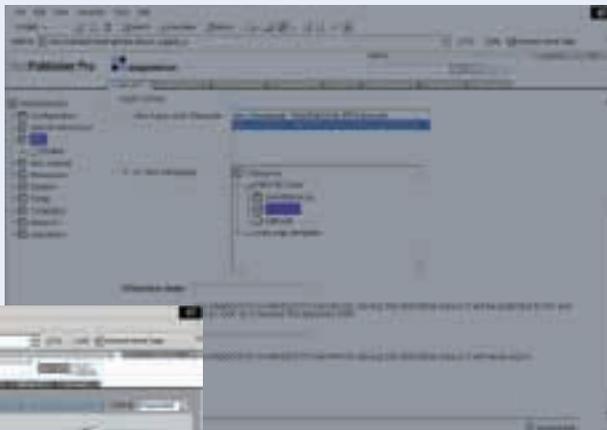
Documentum securely manages and stores your data in the Docbase repository – Mirage™ Enterprise 3.0 continues that control even while documents are in use. Mirage integrates with Documentum at the Web server, protecting content identified through the Documentum cabinet/folder properties and Web publishing configurations.

Using Alchemedia's patented Secure Display™ technology, industry-standard encryption (AES) and RSA authentication algorithms, Mirage makes documents behave like a mirage! They can be seen, but not touched. Easily deployed and invisible to end-users, Mirage was rated 9/10 by ZDNet and has been used by leading enterprises to protect over half a billion documents. By combining the power of Documentum and Mirage, you control your data's confidentiality and currency – whether in storage, in transit, or in use.



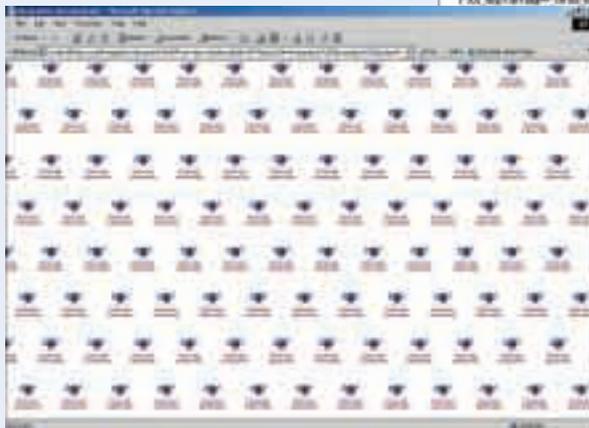
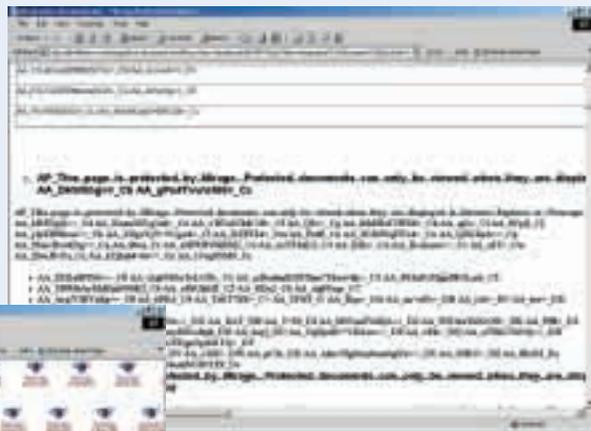
Mirage is integrated with Documentum using the Documentum SDK to extend the robust functionality of Documentum

Documents are imported to the "Protect" subfolder where users can select the Mirage-protected document.



Documentum's Role-Based-Rules determine how the user can access the document. Authorized users can read the document, but unable to compromise its confidentiality or compliance in any way

Any unauthorized attempts to capture documents protected with Mirage – whether via Copy, Print, Save or Forward – results in an encrypted version of the document



Protected documents are also impervious to screen capture attempts. Whether using the Print Screen button or one of hundreds of screen capture applications, only the Mirage logo is captured!



**Alchemedia Technologies, Inc.**

215 West College St. • Grapevine, TX 76051

(800) 561-8295 • sales@alchemedia.com • www.alchemedia.com