The Evolution of a Proactive Data Management Plan
Assessing, Protecting, and Recovering Sensitive Information (PII/PHI)
The Evolution of a Proactive Data Management Plan

Identifying Threats to Data Integrity and Accessibility
  Is the Data Really There?
  How Safe Is the Data?

Mitigating the Risk
  Proactive Data Mapping
  Data Recovery Planning
  Creating a Security Aware Culture
  What to Do When a Data Disaster Strikes or Data Loss Occurs
  Formalizing Data Disposal

A Real-Life Example – Fire in the Research Lab

Conclusion

About Kroll Ontrack
The Evolution of a Proactive Data Management Plan

Assessing, Protecting and Recovering Sensitive Information (PII/PHI)

The convergence of legislation and regulatory measures such as the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the accelerated adoption of Electronic Health Records (EHR) is driving the need for hospitals to examine and strengthen their data management processes and systems. Hospitals are increasingly challenged as they define plans to implement, comply, and mitigate the risks involved with the secure collection, storage, and exchange of so much sensitive data. The volume of electronic data will continue to grow exponentially while requiring the ability to retain and access that data regardless of its storage location. As a result, the need for an information management plan to incorporate proactive data recovery and data protection planning has never been greater.

The benefits of electronic health data are tangible and include improvements to patient safety, quality of care, and clinical and administrative efficiency. However, the required complexity of the corresponding data landscape – managing data centers, storage space, servers, clinical applications, computers, and millions of patient records – will not go away. Additionally, as interoperability among Health Information Exchanges (HIEs), business associates, vendors, and payors continues to grow, there will be new areas of risk at all levels. It is critical to manage that risk and rely on cross-functional teams within the hospital to evolve in their planning as new technology or systems become available. Although technology continually improves and humans endeavor to manage it flawlessly, it is not an infallible process. Data loss is a risk that is frequently ignored and yet, experience proves it is not a question of if it will happen, but when and to what extent.

This white paper will discuss best practices for managing sensitive information and offer tips for assessing areas of risk, closing security gaps, and preparing your organization’s data recovery and breach response plans.
Identifying Threats to Data Integrity and Accessibility

Ensuring data integrity and accessibility means understanding where the threats reside within people, processes, and systems. It is common to think the greatest threat is an unforeseen external intrusion such as a hacker or virus. However, recent studies show the greatest threat resides within the organization itself in terms of negligence by staff or third parties, human error, and theft.

Is the Data Really There?

Hospitals routinely back up and store information, thinking their processes are strong and the data is sound. However, a variety of issues can hinder data retrieval, some of which are never discovered until the hospital is in a reactive crisis mode and scrambling for alternatives. The table below highlights some of the most common threats to data accessibility.

<table>
<thead>
<tr>
<th>Threats to Data Accessibility</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Software Failure</td>
<td>Backup software is set up correctly and the process is kicked off, but the backup data itself is never verified.</td>
</tr>
<tr>
<td>Storage Media Failures</td>
<td>A tape drive fails, tapes are corrupt or inaccessible, or the information written to tape cannot be read (logical errors in the data). There is a significant difference between data from the last backup versus data from the point of failure.</td>
</tr>
<tr>
<td>Aging Systems and Obsolescence</td>
<td>Issues arise when maintaining legacy data or converting old static systems to another format or newer technology. Auditors may also request submission of old data records – such as, in the case of one organization, the submission of 17,000 sets of entries from the 1980s. The tapes were available, but the software and drives required to read the data were no longer serviceable.</td>
</tr>
<tr>
<td>Human Error</td>
<td>Errors such as accidentally reinitializing a tape or forgetting to enable the append option before starting a backup are common.</td>
</tr>
<tr>
<td>Malicious Intent</td>
<td>A disgruntled employee views, damages, or deletes critical data. Consider the case of a former City of San Francisco lead network administrator who reset the passwords to the city’s computer network, locking out other system administrators, and then withheld the new passwords during a workplace dispute. Data was not damaged and systems operated normally, but administrative control of the network was lost for 12 days. The city was forced to spend hundreds of thousands of dollars to fully recover from the incident.</td>
</tr>
</tbody>
</table>
### How Safe Is the Data?

The rising occurrence of medical identity theft and the need to comply with new laws and regulations has increased awareness of patient data security. However, data breaches continue to increase. The 2010 HIMSS Analytics Report: Security of Patient Data commissioned by Kroll’s Fraud Solutions, found:

- The number of healthcare facilities that reported a breach in security that required notification increased 6 percentage points (13% in the 2008 report, compared with 19% in 2010).

- Hospitals appear to be focusing on how to handle a breach after it has taken place, rather than focusing on risk assessments.

- Nearly two-thirds of respondents indicated that the source of the breach was unauthorized access to information by someone employed by the organization at the time of the breach. This was most closely followed by the wrongful access of paper-based patient information.

- Respondents were much less likely to report that patient data at their organization was maliciously compromised in other ways. Eleven percent of respondents noted that data was compromised when a laptop, handheld device, or computer hard drive was lost or stolen.

At the time of this writing (December 2010), Privacy Rights Clearinghouse listed 162 breaches of about 2.8 million records in 2010 alone. At an average of $144-$204 in indirect costs (fines and penalties because of missed regulatory deadlines or mandates) and $60 in direct costs (mailing expense, call center services) per compromised record, the financial impact could conservatively be estimated at $588 million.
Mitigating the Risk

Whether it is e-mail, collaborative SharePoint content, patient information, or financial transactions, the data is vital to continue business operations and provide quality care. So how can hospitals reduce the risks surrounding the massive amount of information being produced each day? Current data maps, evolving information management planning, and an organizational culture focused on security can go a long way to improving the protection of sensitive data.

Proactive Data Mapping

Having a data map before an event occurs and continuing to maintain it is helpful for risk assessment, business continuity, incident response, and early case assessment when litigation occurs. The data map addresses important information including:

- Where does all data reside? What is it called? Where is it stored?
- Is it encrypted? Who has the encryption keys?
- How long is it retained? Where is it backed up?
- Who are the internal IT, business, and application experts?

When an incident occurs, the map provides a common starting point for determining a resolution and getting the right people involved immediately. It is a living document and must be maintained as the needs of the organization change. The map must be updated if systems are added or retired, departmental responsibilities shift, or a merger or acquisition occurs.

Data Recovery Planning

As part of your information management plan, include proactive data recovery and data protection elements and then test your planning:

- Thoroughly vet a professional data recovery provider ahead of time and do your due diligence. Sourcing a professional data recovery vendor in the middle of a crisis (e.g., server outage) is not the time to begin.
- Plan for remote data recovery with your provider. If hardware is still functioning during the failure, a skilled data recovery expert can recover data right on your server, desktop, or laptop through a secure Internet connection. By eliminating the need to dismantle and ship hardware in for service, data is recovered more quickly and the security of the data is maintained because it never leaves the premises.
- Hospitals already conduct drills to test and measure other types of emergency response performance. Use mock data loss drills to verify that people know the plan and can respond accordingly in a variety of “what if” data disaster or loss scenarios. Just like other drills, the initial results may be rough, but they provide a baseline and will improve over time as deficiencies are discovered and process improvements are identified.
Creating a Security Aware Culture

With the latest HITECH modifications to HIPAA requirements, due diligence regarding data security is needed more than ever when initiating or renewing business associate relationships. While it is important to consider third-party relationships, the results of both the 2008 and 2010 HIMSS Analytics Report: Security of Patient Data, commissioned by Kroll’s Fraud Solutions, found that employees are most commonly committing security breaches. This underscores the continued importance of background screening, sound hiring practices, and ongoing training initiatives.

On the technology front, it may be tempting to add even more layers of IT policies to restrict and monitor employee access to data. However, there comes a point when a checklist mentality is no longer successful and only results in making the workday more difficult and less efficient. Rather than adding more security policies, consider ways to make security practices and employee awareness part of the culture of organizational excellence. For example, consider holding an annual security meeting with employees and a security summit with partners and vendors. Remind attendees of your security practices, threat awareness, the importance of good passwords, and simple tasks such as locking your computer before stepping away.

Formalizing Data Disposal

Keeping data longer than necessary bloats IT budgets unnecessarily and increases e-discovery risks and costs when an investigation, litigation, merger or acquisition occurs. Many organizations have clear document retention policies that specify how long important data, such as financial or customer records, needs to be kept. However, many of those same organizations do not have clear policies for handling data that no longer needs to be retained or for disposing of old PCs, hard drives, servers, and other data storage devices. Simply deleting files or reformattting a hard drive or other storage device before recycling it does not protect those files from being recovered. Physically destroying the drive using a power drill, hammer, or other tools certainly reduces the possibility of data recovery, but knowledgeable data recovery engineers can give you many examples of data recovered from drives that were crushed, impaled, cracked, and seemingly dead.

When organizations neglect to erase data before discarding, selling, or giving away hard drives or servers, a major security breach is revealed that could have been avoided. Enterprise-level data erasure software permanently destroys data using standards widely recognized by government agencies, including the American and British militaries. If you choose to do the data erasure internally, an experienced data recovery vendor can conduct an appropriate and rigorous investigation of your deleted drives, provide a detailed report confirming the data deletion, and alert you to any retrievable data on the media.
A Real-Life Example – Fire in the Research Lab

A Kroll Ontrack client, a university hospital, needed to recover research data after a fire broke out in one of its research labs. Although the server room was also located on the same floor, the fire was contained strictly to the lab area. Working with a disaster recovery cleanup team and the hospital staff, Kroll Ontrack put a process in place to determine whether the hard drives were still functioning. The failed drives were sent to Kroll Ontrack's cleanroom for recovery. More than 75 hard drives totaling 10 terabytes of data were successfully recovered, saving hundreds of hours of research effort and a $1.5 million dollar grant.

Conclusion

Data disasters and data loss can happen at any time. Whether it is mechanical failure, human error, a power outage, or some other unforeseen event, it is the organizational response that determines how successful a data recovery will be. As part of protecting valued assets, resolving regulatory risk, and reducing costs, hospitals need to proactively build data recovery response measures into their disaster recovery and information management plans and procedures.

Successful recovery plans incorporate:

- Selecting a professional and highly secure data recovery vendor
- Maintaining current data maps
- Generating employee activities and data loss drills to ensure prompt organizational response
- Formalizing data disposal

Organizational excellence demands it.

About Kroll Ontrack

Kroll Ontrack provides technology-driven consulting services and software to help legal, corporate, and government entities as well as consumers manage, recover, search, analyze, produce, and present data efficiently and cost-effectively. In addition to its award-winning suite of software, Kroll Ontrack provides data recovery, paper and electronic discovery, document review, computer forensics, secure information services, ESI and jury consulting, and trial presentation services. Kroll Ontrack is the technology services division of Kroll Inc., the global risk consulting company. Kroll is a subsidiary of Altegrity, an industry-leading provider of information solutions. For more information about Kroll Ontrack and its offerings, please visit www.krollontrack.com.