



**Indiana's Public Records:**

**The Legal Framework of  
Records and Information Management  
in State Government**

Records Management Division  
Indiana Commission on Public Records

## **PREFACE**

This guide to the legal issues regarding records and information management is designed to explain to state employees what factors may affect the creation, retrieval, storage and destruction of the records in their care. It is important to note that these issues are of concern to all state employees, but are of particular significance to those who make decisions on how records and information is managed.

The publication has been divided into several parts. The first explains why the state has and will continue to invest time and resources into a records management program. The second looks at traditional records management issues and will discuss such topics as public access, confidentiality, privacy and legal admissibility. The last will examine some of the new challenges facing records managers, such as imaging, electronic records and online access to government records.

While some of these issues are fairly straightforward and easily explained, many others leave to state agencies a great deal of latitude for interpretation and application. Still others, especially those relating to electronic records, remain largely unexplored territory; they are on the frontier of records management. Accordingly, this brochure can offer ideas and directions, but may not be able to answer all the questions readers have; this should be used as a guideline for further research and not as the source for definitive interpretations of applicable law.

To get more information, please do not hesitate to contact the Records Management Division of the Indiana Commission on Public Records. As well, be sure to consult your agency legal counsel and the Indiana Attorney General's Office.

# **TABLE OF CONTENTS**

## **PREFACE**

### **1. WHY RECORDS MANAGEMENT**

- 1.1 Introduction
- 1.2 What is a Public Record?
- 1.3 The Indiana Commission on Public Records
- 1.4 Accountability
  - 1.4.1 State Board of Accounts
  - 1.4.2 Federal government
  - 1.4.3 Courts
- 1.5 Management needs
- 1.6 Space management
- 1.7 Historical significance

### **2. TRADITIONAL RECORDS MANAGEMENT TOPICS**

- 2.1 Transfer of records
- 2.2 Public access
- 2.3 Confidentiality
- 2.4 Destruction of records
- 2.5 Legal admissibility
- 2.6 Copyright
- 2.7 Privacy: The Fair Information Practices Act

### **3. NEW RECORDS MANAGEMENT ISSUES**

- 3.1 Electronic records
- 3.2 Creating and preserving electronic records
- 3.3 Public access
- 3.4 Copying costs
- 3.5 E-mail
- 3.6 Imaging
- 3.7 EDI (electronic data interchange)

## **WHY RECORDS MANAGEMENT?**

### **1.1 Introduction**

There are three basic reasons why every agency in Indiana's state government needs an effective records management program: 1) to perform its legal mandates and responsibilities; 2) to store records in the most efficient and cost-effective manner possible; and 3) to assure public access to the documentary history of government. Together, the three ensure that an efficient, democratic form of government will properly function. Public records are at the heart of this.

**The Indiana Code**, in 5-14-3-1, makes that clear when it states:

A fundamental philosophy of the American constitutional form of representative government is that government is the servant of the people and not their master. Accordingly, it is the public policy of the state that all persons are entitled to full and complete information regarding the affairs of government and the official acts of those who represent them as public officials and employees.

As this indicates, the legitimacy of the government and the public's favorable or unfavorable perception of it are integrally linked to the records that state agencies create and preserve. From this perspective, records act as the vital signs of government, indicating to its stakeholders what it does well, what it needs to do better or, as some now demand, what it should not do at all. At a time when voters are clamoring for better and more efficient services and at a time when the government is pressured to re-invent itself, the significance of records is all the more apparent.

### **1.2 What is a Public Record?**

Lest there be any doubt to the importance of records in this context, **IC 5-14-3-2(9)** emphasizes it with this all-inclusive definition:

"Public record" means any writing, paper, report, study, map, photograph, book, card, tape recording, or other material that is created, received, retained, maintained, used or filed by or with a public agency and which is generated on paper, paper substitutes, photographic media, chemically based media, magnetic or machine readable media, electronically stored data, or any other material, regardless of form or characteristics.

With that definition, the General Assembly essentially precludes any state agency or state employee from determining individually what is or is not a record: anything, on any medium and created for any governmental purpose, falls under the rubric of public records law. Note that the term "public," in this context does not have the sense of "open to the public," but, rather, serves to distinguish between "personal," as in an employee's personal papers, and "public," as in records created in the course of state government business and so belonging to the public.

To demonstrate the comprehensive nature of this definition, the representative of the State Board of Accounts on the Oversight Committee on Public Records has stated that SBA auditors even consider post-it notes to have evidentiary value in certain situations. By analogy, this encompasses many items. Accordingly, these and other sections of the Indiana Code pertaining to public records make it clear that agencies have a particular obligation to develop a comprehensive records management program.

### **1.3 The Indiana Commission on Public Records**

The Commission on Public Records Act vests the records management function of state government in the Commission on Public Records (**IC 5-15-5.1**). This act authorizes the Commission:

- To establish a statewide records management program;
- To establish and operate a statewide archival program;
- To prepare, develop, and implement records retention schedules;
- To establish and operate a state records center;
- To operate a central micrographics and imaging laboratory; and
- To establish and operate a conservation laboratory.

Accordingly, the ICPR has a statutory obligation and responsibility to play a fundamental role in the management of state government's records. Its divisions fulfill that obligation by offering services to cover every phase of the life cycle of records. Government employees should not hesitate to contact ICPR staff with their questions and concerns.

### **1.4 Accountability**

The general principle inspiring public records law is accountability. This can take many forms. For example, in defining the mission of an agency, the General Assembly can explicitly mandate that an agency has to treat its records in a certain fashion or take responsibility for specific records. **IC 4-5-1-2** states that:

- (a) The secretary of state shall keep and preserve:
  - (1) the enrolled copy of the constitution of the state.
  - (2) the manuscripts containing the enrolled acts and joint resolutions of the general assembly...

Similarly, **IC 4-33-3-19** instructs the executive director of the Gaming Commission to:

- (1) Keep records of all proceedings of the commission.
- (2) Preserve all papers, books, documents and other records belonging to or held by the commission.

These are examples of statutes entrusting specific records responsibilities to an agency; there are many others like them. Because such statutes are peculiar to an agency, they will not be discussed in detail here. Instead, it is important to note that while some agencies are specifically assigned such missions and are explicitly accountable for them, all agencies create records which serve as the measures to hold them accountable and for which they are legally responsible to maintain.

#### **1.4.1 State Board of Accounts**

The role of the State Board of Accounts is of particular importance in establishing accountability. Within state government, the State Board of Accounts has as its primary responsibility the mandate to track and evaluate the fiscal transactions of state agencies. As stated in **IC 5-11-1-9(d)**, with every examination, the SBA examiners must determine:

- (1) the financial condition and resources of each municipality, office, institution, or entity.
- (2) whether the laws of the state and the requirements of the state board of accounts have been complied with.
- (3) the methods and accuracy of the accounts and reports of the person examined.

To fulfill this responsibility, the State Board of Accounts examiners are authorized in **IC 5-11-1-9(f)** to:

- (1) enter into any state, county, city, township, or other public office in this state, or any agency, or instrumentality, and examine any books, papers, documents, or electronically stored information for the purpose of making an examination.

They are further authorized to issue subpoenas to produce records and to examine witnesses under oath in the course of their duties (**IC 5-11-1-9(g)**). These powers ensure that those dealing with the state's finances are held strictly accountable for their actions; to guarantee that accountability, the SBA examiners are entirely dependent on records.

Once an audit is completed, **IC 5-11-5-8** states that it becomes part of the public records of the office of the state examiner; of the office or the person examined; of the auditing department of the municipality examined and reported upon; and of the legislative services agency. A report is open to public inspection at all reasonable times after it is filed.

#### **1.4.2 Federal government**

Beyond their accountability to state government and to Indiana's citizens, state agencies are often affected as well by federal statutes and rules, especially when they are receiving federal funds.

Examples of how federal oversight is applied can be found in the **Guide to Retention Requirements in the Code of Federal Regulations**, published by the Office of the Federal Register, National Archives and Records Administration.

This describes the retention periods for records of federally funded programs administered by state agencies. Such federal guidelines have a heavy impact on several agencies in Indiana's government, such as, to name only a few, the Department of Environmental Management, the State Department of Health and Family and Social Service Administration.

### **1.4.3 Courts**

When a legal issue is raised and results in a conflict, it very often ends up before a court, which can only make its decisions using evidence. Very often this evidence consists of records.

The **Indiana Rules of Court** have set certain guidelines determining when and how records can be accepted as evidence; these records must have certain bona fides in order to be legally admissible. The topic is discussed in more detail below.

For now, though, it is important to note that an established and approved records management program is necessary for state agencies to use their records in court. Sloppy record keeping or an inexplicable loss of records might well be interpreted to mean that the contents of the submitted records are not reliable.

### **1.5 Management needs**

Accurate and informative records can benefit agency management, as they make both staff and agencies accountable for their performance to the state's administrative hierarchy. While this has always been the case, new approaches to management, such as Total Quality Management or the definitions established by the International Organization of Standards in its ISO 9000 criteria, place an even heavier emphasis on the use of records to determine benchmarks, measure performance and establish goals. In fact, studies have determined that the majority of applicants for such things as the Baldrige Prize or ISO certification fail because of the unreliable nature of their record keeping systems. From this perspective, quality can only be defined and assured through records.

### **1.6 Space management**

When asked, virtually all state employees dealing with records on a regular basis will say that their single biggest problem is space - there simply is not enough of it. As a result, agencies are constantly running out of room to store the documents they create. This leads to a number of problems, particularly a lack of usable space in offices and increasing difficulties in identifying and retrieving records.

A records management program can serve to take inactive records out of valuable office space to a less costly storage site, such as the State Records Center. In addition, a good records management program establishes the relative value of records, creating a set of priorities determining how

records of different importance should be handled. This can involve anything from defining the necessary indexing system to scheduling a destruction date.

## **1.7 Historical Significance**

Certain records created by state agencies are deemed to have a permanent value for the documentary history of the state. The Indiana State Archives is the final repository for all state government records of permanent legal or historical significance. When an agency transfers its records to the State Archives, the title to the records is transferred to the State Archives as well [IC 5-15-5.1-11].

---

## **2. TRADITIONAL RECORDS MANAGEMENT TOPICS**

### **2.1 Transfer of records**

Most state records are routinely transferred from the agency that created them to the state Records Center or the State Archives according to the dictates of retention schedules established by the agency in collaboration with the Commission on Public Records and the Oversight Committee on Public Records [see IC 5-15-5.1-19].

In cases where no retention schedule exists, this section, IC 5-15-5.1-15 (a), applies:

A public official who has the custody of any records, excluding personal records, shall at the expiration of his term, deliver to his successor, or to the commission [i.e., the Commission on Public Records] if there is no successor, all materials defined as records by this chapter.

### **2.2 Public access**

As noted above, the **Indiana Code** makes generous provisions for public access to state government records. The full citation of IC 5-14-3-1, as amended by P.L. 77-1995, makes this clear:

A fundamental philosophy of the American constitutional form of representative government is that government is the servant of the people and not their master. Accordingly, it is the public policy of the state that all persons are entitled to full and complete information regarding the affairs of government and the official acts of those who represent them as public officials and employees. **Providing persons with the information is an essential function of a representative government and an integral part of the routine duties of public officials and employees, whose duty it is to provide the information** [emphasis added]. This chapter shall be liberally construed to implement this policy and place the burden of proof for the nondisclosure of a public record on the public agency that would deny access to the record and not on the person seeking to inspect and copy the record.

Despite the sweeping nature of this assertion, the General Assembly does allow for some routine control over public access. These measures are described in **IC 5-14-3-3**. Basically, while people have a right to inspect and make copies of public records, they must make their requests during regular business hours; they must identify with some "reasonable particularity" the records in question; and they may, at the discretion of the agency, have to make their requests in writing, although they cannot be compelled to state the reason for their request.

**IC 5-14-3-8** also establishes what fees are permissible. No charge can be levied to inspect a record; currently, the price of photocopies cannot exceed \$.10 per page unless an exemption is authorized by statute. It is important to note that this law makes no provision for processing or research fees in the case of paper records. Essentially, agencies may not pass along the costs of identifying, finding or delivering records, no matter what disruption in routine a particular request may represent, unless specifically authorized by law. Electronic records are a special case, though, which will be discussed below.

The law does not set any specific deadline for delivery of a record or records upon request. If, however, a person makes a written request for a record, **IC 5-14-3-9(b)** assumes that an agency has made a denial of disclosure if no response is made within seven days of receiving the request.

### **2.3 Confidentiality**

Not all records are accessible to the public; agencies can deny requests on the basis of confidentiality. There are two general exceptions to the requirement that records be made available to the public.

The first states that certain information is always confidential unless otherwise specified by a state or federal statute, or ordered released by a court. A few of the records included in this category are: records that are declared confidential by state statute, records containing trade secrets, grade transcripts, patient medical records and examination scores obtained as part of a licensure process. **Indiana Code 5-14-3-4(a)** has the complete details.

The second exception states that certain information may be kept confidential at the discretion of an agency. A few of the records in this category are: certain investigative records in law enforcement agencies, work products of an attorney pursuant to state employment or data used in administering a licensing examination. See **IC 5-14-3-4(b)** for further information.

Social security numbers are often mistakenly considered confidential records. This confusion is understandable, as Social Security numbers have become the de facto national identification number and serve as the key to many other records and record databases. Yet there are no federal or state laws that deem Social Security numbers confidential. However, **IC 4-1-8-1** states that:

No individual may be compelled by any state agency, board, commission, department, bureau, or other entity of state government...to provide the individual's Social Security number to the state agency against the individual's will, absent federal requirements to the contrary.

This law does not apply to all state agencies. A few of the exceptions are: Department of State Revenue, State Personnel Department, Auditor of State, Health Professions Bureau, and several programs that administered by the Division of Family Children of Family and Social Services Administration. In these instances, the state can require the disclosure of Social Security numbers. Despite all that is noted above, all records, save those concerning adoptions, automatically lose their confidentiality after 75 years [IC 5-13-3-4(e)]. At that point, no restrictions on access can be instituted. Adoption records, on the other hand, are considered permanently confidential, unless a court determines otherwise.

Inevitably, there will arise some dispute about decisions made as to the confidentiality of records. Accordingly, IC 5-14-3-9(b) affirms that "a person who has been denied the right to inspect or copy a public record by a public agency may file an action in the circuit or superior court of the county in which the denial occurred to compel the public agency to permit the person to inspect and copy the public record." Agencies should note that, in cases of legal action, IC 5-14-3-9(h) allows a court to award reasonable attorney fees and other cost of litigation, if "the plaintiff substantially prevails and the court finds the defendant's violation was knowing or intentional." In other words, there are instances where the state could be liable for the costs of the plaintiff's suit.

## **2.4 Destruction of records**

Because of the importance the General Assembly places on public access to public records, it has also put in place measures to control the loss of documents, in order to assure their continuing availability and to limit the opportunity for careless or wanton destruction. IC 5-14-3-4(f) holds that:

- (1) public records subject to IC 5-15 may be destroyed only in accordance with record retention schedules under IC 5-15; or
- (2) public records not subject to IC 5-15 may be destroyed in the ordinary course of business.

**Indiana Code 5-15**, among other things, establishes the Commission on Public Records, and, at IC 5-15-5.1-5(a)(4), delegates to it the authority to:

Establish a statewide records management program, prescribing the standards and procedures for recordmaking and recordkeeping ...

That includes the authority to develop and implement retention schedules "prescribing how long, where, and in what form a record series shall be kept." [IC 5-15-5.1]

Virtually all state agencies are subject to this, with the notable exceptions determined by statute. Accordingly, for all other agencies, the destruction of records is not licit without the sanction of an official retention schedule. This may have a significant bearing on questions of legal admissibility.

The issue is summarized in IC 5-15-5.1-14:

A public official or agency may not mutilate, destroy, sell, loan, or otherwise dispose of any government record, except under a record retention schedule or

with the written consent of the commission [i.e., Commission on Public Records].

## 2.5 Legal admissibility

Courts in Indiana follow strict, established guidelines on what is or is not legally admissible as evidence in a court of law. As there are certain public records that stand at a high risk of ending up in court, agencies should be careful to evaluate their records management needs with these guidelines in mind.

The basic source of information is the **Indiana Rules of Court**, and specifically, Article VIII of the **Indiana Rules of Evidence**. The principle points to consider are those regarding hearsay and the hearsay exceptions. Hearsay is generally not admissible in court; Rule 801 (C) defines it as: a statement, **other than one made by the declarant while testifying at the trial or hearing**[emphasis added], offered in evidence to prove the truth of the matter asserted

This is important to note, because, with certain exceptions nothing other than personal testimony is recognized as legally admissible evidence [Rule 802].

Rule 803 details the various exceptions, some of which explicitly apply to records. Rule 803(8) allows for the admission of public reports and records as evidence, "unless the source of information or other circumstances indicate a lack of trustworthiness." Otherwise, records, reports, statements, or data compilations in any form, of a public office or agency, setting forth its regularly conducted and regularly recorded activities, or matters observed pursuant to duty imposed by law and as to which there was a duty to report, or factual findings resulting made pursuant to authority granted by law, are admissible in court.

But there are exceptions. Generally, investigative reports or factual findings made by law enforcement agencies, or compiled in situations where an agency is a party to a case, are not exempt from the hearsay rule.

The key terms to note in this definition, though, are "unless the source of information ... indicate a lack of trustworthiness" and "regularly conducted and regularly recorded activities." These caveats suggest that records might be questioned if their authenticity cannot be established through procedural manuals, retention schedules, functional descriptions of an agency's business process or any other a priori documents that define just how records are routinely created, stored and maintained. This is especially true of electronic records, which are just now being introduced into courts; this is discussed more fully below.

## 2.6 Copyright

Copyright is a hotly debated issue now, with the advent of new technologies allowing for easier distribution and access to materials. While it remains to be seen how the debate will be resolved, agencies should remember certain general principles. Basically, while federal agencies are not

allowed to place a copyright on any information or publications they generate, no such restriction is placed on state agencies in Indiana. In fact, the Lottery Commission has explicit legislative authority to own "copyrights, trademarks and service rights." It is theoretically possible, then, for agencies to control the dissemination and distribution of their publications; some agencies, such as the Indiana Historical Bureau, have taken advantage of this to assure that no loss of quality occurs. Copyrighted material, at the moment, is more or less protected for 75 years, although a variety of distinctions may apply. Agencies wishing to explore the use of copyrights for their publications should devote a considerable effort to research the issues involved. They should note, especially, that it would be impossible to copyright and so limit the access to or the use of non-published materials, which clearly fall under the rubric of public records law.

## **2.7 Privacy: The Fair Information Practices Act**

One of the most little known and appreciated statutes governing records is the Fair Information Practices Act, **IC 4-1-6**. This law is designed to ensure that information collected by the state on its citizens, particularly that of a personal nature, remains accurate and is used only for the statutory purposes of the agency which gathers it.

In **IC 4-1-6-1**, "personal information" is generously defined:

"Personal information" means any information that describes, locates, or indexes anything about an individual or that affords a basis for inferring personal characteristics about an individual, including, but not limited to, his education, financial transactions, medical history, criminal or employment records, finger and voice prints, photographs, or his presence, registration, or membership in an organization or activity or admission to an institution.

"Personal," in this instance, is not the same as "confidential." Much of the information which falls under this rubric remains accessible to the public. The intent of the law, though, is to minimize the potential for the abuse of such information, confidential or not, by establishing certain guidelines for the collection, verification and dissemination of these records.

Probably the most important point is made in **IC 4-1-6-2(a)**, which states that agencies shall: collect, maintain, and use only that personal information as is relevant and necessary to accomplish a statutory purpose of the agency.

The intent there is to avoid the needless invasion of privacy. If the collection of certain personal information is demonstrated by a clear, mandated need, then an agency is justified in collecting it. If that need is not clear, then an agency should re-consider its interest in such information.

Even with a justified need, agencies are expected to take a variety of precautions to safeguard personal information. Among others, they should work to:

establish controls for access to personal information [**IC 4-1-6-2(f)**];

maintain lists of persons and organizations with access to personal information that is not a public record [**IC 4-1-6-2(g)**];

maintain a "complete and accurate record" of every access [emphasis added] to personal information that is not a public record [IC 4-1-6-2(h)];

establish rules and procedures to assure compliance with this law and instruct employees on them [IC 4-1-6-2(k)]; and

allow "data subjects" to inspect and copy their records [IC 4-1-6-3] and then to challenge any inaccuracies noted [IC 4-1-6-5].

Further, the law calls for all agencies collecting such information to file an annual report to the governor detailing their responses to the concerns of the statute in some detail [IC 4-1-6-7]. The governor is then required to file an annual report summarizing these to the General Assembly [IC 4-1-6-9].

---

### **3. NEW RECORDS MANAGEMENT ISSUES**

#### **3.1 Electronic records**

Electronic records are in many ways an unknown quantity; because they represent new and untested issues, no one can vouchsafe exactly what the results of the application of new technologies may be, particularly in regards to public records law. People do, however, appreciate their potential: enormous savings in the space used for records storage; faster and simpler access to information; and the widespread distribution of records through networks and other communications systems. But achieving that potential, while ensuring the authenticity and security of records, is no simple problem.

#### **3.2 Creating and preserving electronic records**

At present, the General Assembly has explicitly condoned the use of electronic media for records creation and storage. Various passages in laws defining public records law mention electronic media (e.g., IC 5-14-3-2(9), or IC 36-2-17-17), but Public Law 79-1995, amending IC 5-15-1-1(a), states specifically:

Any officer, office, court, commission, board, institution, department, agent, or employee of the state, county, or any political subdivision being charged with the duty or authorized or required by law to record, preserve, keep, maintain, or file any record, document, plat, paper or instrument-in-writing, may ... for the purpose of recording or copying same, preserving and protecting same, reducing space required for storage or filing for same, or any similar purpose, have or cause to have any or all such records recorded, copied, or reproduced by any photostatic, photographic, micrographic, electronic, or other process which correctly and accurately copies or reproduces, recreates or forms a medium of copying or reproducing the original record, document, plat, paper or instrument-in-writing.

The section goes on to include optical imaging explicitly as one of the available options, but it would seem clear that any electronic format could be adopted as long as it meets the condition of "correctly and accurately" copying the reproducing the original.

The potential problem here is that all electronic media are new and there are very few legal precedents determining what "correctly and accurately" means in practice. It is clear, though, that there is a vast potential for abuse of electronic records, so agencies can assume that any such records they create will be thoroughly scrutinized before they are accepted as authentic. the critical distinction is between the reliability of the technology for records storage and the reliability of the human procedures for records creation or manipulation. The former is proven: electronic media can, in theory, store records safely and accurately. There are some real questions about how long they can do so, without serious problems arising, but the basic principle is set and recognized in law.

The human aspect of the equation is where the most significant questions lie. Maintaining the security and authenticity of electronic records is a major problem, with many aspects. Because data can be so easily altered, agencies should be prepared to demonstrate: the reliability of their equipment, both hardware and software; the integrity of the data entry process, including the means of verification of data; the methods used to prevent the loss of data; and the date and method of creating hard copies of records, such as printouts, especially as those are generally the format electronic records take when presented in court.

Agencies can accomplish some of these tasks and guarantee the authenticity of their records by taking certain technical and procedural steps, such as:

1. building hierarchies of access and rights (such as read only or read and write) into a system, using data compartmentalization and passwords;
2. creating audit trails with date and time stamping automatically to maintain logs identifying who had access to what and when, as well as who entered what and when;
3. building electronic firewalls;
4. using electronic signatures to verify procedures and transactions; and
5. encrypting data being exchanged over networks.

**The Indiana Code** does not explicitly address these issues for public records as a whole, but it does include a section pertaining to hospital records that is of interest. **IC 34-3-15.5-3**, "Authentication of entries; procedure", reads:

- Sec. 3. Entries made in a hospital medical record may be authenticated by showing that (1) the electronic data processing equipment is standard equipment in the hospital;

- (2) the entries were made in the regular course of business at or reasonably near to the happening of the event or order, opinion, or other information recorded;
- (3) the security of the entries from unauthorized access can be demonstrated through the use of audit trails; and
- (4) records of all original entries and subsequent access to the information are maintained.

While these seem straightforward enough, it is important to note that they represent significant investments in planning, training and recordkeeping. To be effective, they must be built into a system at the design phase and then communicated to all system users on a continuing basis. Accordingly, to meet these demands, agencies have to keep records about their records in order to guarantee the latter's authenticity.

### **3.3 Public access**

**The Indiana Code** essentially does not make any distinctions between electronic and other types of records in terms of public access. The basic rule still applies: it is the duty of public officials and employees to provide access to the records they hold [IC 5-14-3-1]. This is emphasized in IC 5-14-3-2, which defines "inspect," as including the right to do the following: In the case of electronically stored data, to manually transcribe and make notes, abstracts, or memoranda or to duplicate the data onto a disk, tape, drum, or any other medium of electronic storage.

Further, IC 5-14-3-2(f) holds that,

A public agency may not enter into or renew a contract or an obligation:

- (1) for the storage or copying of public records; or
- (2) that requires the public to obtain a license or pay copyright royalties for obtaining the right to inspect and copy the records unless otherwise provided by applicable statute;

if the contract, obligation, license, or copyright unreasonably impairs the right of the public to inspect and copy the agency's public records.

This ensures that the traditional method of going to the agency directly to inspect records, in whatever format, cannot be impaired.

Access can, however, be enhanced through the creation of additional methods to inspect and copy public records; and, currently, many agencies are exploring the potential of enhanced access, primarily through the Access Indiana Information Network. The legal framework for such contracts is described in IC 5-14-3-3.5:

- b) A public agency may provide a person with enhanced access to public records if either of the following apply:

- (1) The public agency has entered into a contract with the person under this section;
- (2) The public agency has entered into a contract with a third party under which the public agency provides enhanced access to the person through the third party's computer gateway or otherwise, and all of the following apply:
  - (A) The contract between the public agency and the third party provides for the protection of public records in accordance with subsection (c)(2).
  - (B) The contract between the public agency and the third party provides for the payment of a fee to the public agency in accordance with subsection (c)(1):
    - (i) the third party; or
    - (ii) the person.
  - (C) The third party and the person enter into a contract that provides for
    - (i) enhanced access through the third party's gateway or otherwise; and
    - (ii) the protection of public records in accordance with subsection (c)(2).

Note that subsection (c)(2) prohibits the following: unauthorized access to public records; the alteration of public records; and the disclosure of confidential public records.

In addition, **IC 5-14-3-3(e)**, allows an agency to adopt a rule determining if or how a person receiving electronic records in an electronic format can "use the information for commercial purposes." This might well stem from the same motives inspiring the Fair Information Practices Act, a desire to limit the intrusions on citizens' privacy.

### **3.4 Copying costs**

As noted above, the right to inspect electronic records formally includes the right to receive copies of them, in whatever format they are available. Because meeting such requests may cause a burden to an agency, **PL 77-1995**, amending **IC 5-14-3-6**, allows for the possibility of charging fees for that service:

- (c) a public agency may charge a person who makes a request for disclosable information the agency's direct cost of reprogramming a computer system if:
  - (1) the disclosable information is stored on a computer tape, computer disc, or similar or analogous records system; and
  - (2) the public agency is required to reprogram the computer system to separate the disclosable information from nondisclosable information.

"Direct cost" is strictly limited to only the expense of providing the requested information in the desired format, with no scope for overhead, system maintenance etc. It is defined in PL 77-1995, amending IC 5-14-3-2:

"Direct cost" means one hundred five percent (105%) of the sum of the cost of:

- (1) the initial development of a program, if any;
- (2) the labor required to retrieve electronically stored data; and
- (3) any medium used for electronic output;

for providing a duplicate of electronically stored data ...

### **3.5 E-mail**

Despite its often informal nature and its functional equivalence, say, to a telephone conversation, e-mail is undoubtedly a record within the generous and comprehensive definition provided in the **Indiana Code**. Accordingly, agencies should be prepared to preserve and maintain e-mail messages as per retention schedules, and to make copies available to people who request them. Moreover, agencies should be prepared to make available the context of the messages as well as the content. In this instance, context means the message headers indicating the date and routing of the messages, as well as any responses to them. This principle was established in federal court, in the case *Armstrong v. the Executive Office of the President*; it was reinforced by regulations issued by the National Archives and Records Administration in the 28 August 1995 issue of the **Federal Register**. While these do not specifically apply to state records, they do constitute the most significant precedent available for application.

In the *Armstrong* case, the National Archives, as custodian of the records in question, was forced to go to extreme lengths to meet the demands of the court. The basic problem was that these rules were applied in retrospect, after the creation of the e-mail system and after the creation of the records, which made the records quite difficult to identify, sort and supply.

What this indicates is that legal and recordkeeping principles ought to be considered at the time a system is designed and that they should be communicated to all users of the system, so that routine procedures are in place to assure the lawful disposition of records. Emergency, ex post facto attempts to provide records are not likely to be successful and, as in the *Armstrong* case, could lead to charges of contempt and the possibility of fines.

Some e-mail messages, of course, may be deemed confidential, but, as described above, this has to be established; it cannot be assumed. Indeed, the exact opposite is the real case; agencies should assume their e-mail is public record.

### **3.6 Imaging**

Public Law 79-1995, amending **IC 5-15-1-1(a)**, explicitly allows for the use of an imaging system in the creation and storage of public records:

Any officer, office, court, commission, board, institution, department, agent, or employee of the state may have or cause to have records recorded, copied, or reproduced under this subsection by any optical imaging process that correctly and accurately copies or reproduces, recreates, or forms a medium of copying or reproducing the original record, document, plat, paper, or instrument-in-writing.

However, **IC 5-15-1-1(b)** holds that state agencies may not destroy the original records without the approval of the Commission on Public Records. Accordingly, any agency seeking to employ an imaging system should involve the CPR in the design phase of the system in order to ensure that approval.

The CPR's role is to determine that the proposed system does indeed meet the requirements of public records law and that it will satisfy the various technical standards guaranteeing the authenticity and preservation of electronic records. In the absence of any set legislative guidelines, the principle benchmarks for Indiana are those adopted in Administrative Rule 13, Optical Disk Imaging Standards, in the **Indiana Rules of Court**. These apply directly only to agencies under the aegis of the court system, but they are undoubtedly the standards to which any court will turn if the electronic records produced by an imaging system come into question.

The standards focus on three aspects of a system: documentation, legibility and permanency. The latter two establish certain technical specifications that guarantee the long term viability of records for use. The first is important as it echoes the general concerns voiced about electronic records: that authenticity will be determined largely by the evaluation of the human aspects of the system. In this instance, Rule 13(c) calls for:

(1) **Documentation.** A formal written documentation file shall be created and retained for the life of the information stored on the optical disk based upon an approved records retention schedule documenting the following:

(a) that every stage of the digital imaging process is covered by a written and recorded procedure including:

(i) authority to implement digital imaging technology,

(ii) any weeding policy of documents to determine what documents from any file will be imaged, and

(iii) any contracts with agents of record custodians who will perform the actual optical imaging process;

(b) the imaging process employed to assure accuracy;

- (c) verification of the image on a CRT screen against the original for completeness and legibility;
- (d) definition of the indexing system employed with storage in multiple places on the optical disk for security and integrity;
- (e) the identity of persons who supervised the optical imaging procedures who are capable of giving evidence of these procedures; and
- (f) certification of compliance with this documentation procedure to the Division of State Court Administration.

Instead of the last, state agencies should gain the approval of the CPR and follow the procedures outlined in Chapter 10 of the former Data Processing Oversight Commission's **Blue Book**.

### **3.7 EDI (electronic data interchange)**

The potential applications and benefits of EDI, the interchange of information "on-line" via the Internet or other networks, are as diverse as the functions of state agencies. State governments have employed EDI to quickly and efficiently collect personal property taxes; to solicit bids from contractors and vendors; to provide birth certificates to the public and to register vehicles. The applications of EDI are limitless.

While EDI holds the potential for making government more efficient, less costly, and more accessible, it also carries grave security risks that must be addressed before implementation is contemplated. If sound security measures are not in place, government stands to lose not only the benefits that EDI promises, but also its credibility and the public's confidence. Furthermore, the legal ramifications of not providing adequate security can be serious and costly.

The free and open nature of the Internet and similar networks makes EDI particularly vulnerable to security violations. "Hackers" have found a plethora of techniques to invade and disrupt government programs and databases such as:

1. illegally accessing confidential information on U.S. citizens;
2. intercepting e-mail messages between the state and the outside world;
3. modifying and manipulating state data;
4. stealing passwords;
5. introducing computer viruses on state networks; and
6. embedding "Trojan horses" in programs causing the program to do what the hacker requests it to do.

To minimize security risks and to avoid unnecessary law suits, state administrators should ensure that either their agency or an outside contractor provides the following:

1. a sound security policy;

2. moneys specifically allocated for the continued upkeep of a security system, including funding set aside for unforeseeable security breaches;
3. electronic firewalls;
4. authentication and access controls; and
5. encryption of confidential data exchanged via the Internet.

Meeting these conditions will lessen security problems. Current advances in public-key cryptography promise to solve many of the security problems plaguing EDI today.

Agencies interested in or considering EDI should note that the Office of Technology and the Commission on Public Records will both have some influence in the process.