by Raymond C. Ellis, Jr.

A matter of record: What and how long must hotel records be maintained?

Record keeping for hoteliers has always been a challenge. What should be recorded? What is mandated? What is optional? Is there a preferred format? Is it in free-form or is it a standardized printed form? What are the rules for the retention of records? Should the form and information be computerized? Fortunately, there are some excellent sources of information about record retention.

Employment-related records

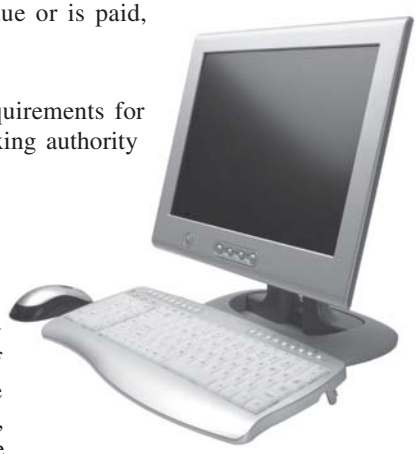
Essentially, employers are required to maintain employment-related records anywhere between one year to five years after they are applicable, depending on the concern at hand and the type of record. One source of information about retaining employment-related records is available from the Society for Human Resource Management Information Center (www.shrm.org). Here, a white paper titled "Federal Record Retention Requirements for Employers" can be downloaded. A table, derived from the white paper, listing the federal record retention requirements is enclosed in this issue of *The Rooms Chronicle®* as an insert. (Note: Under the OSHA entry, the authors fail to note an unusual requirement. If an employee has an injury or work-related illness that will require, at least, an annual medical check-up, records must be retained for 30 years, even though the employee may no longer be employed.)

Tax-related records

For federal tax records, the length of time a business should keep a document depends on the action, expense, or event the document records. Generally, one must keep your records that support an item of income or deductions on a tax return until the period of limitations for that return runs out. The period of limitations is the period of time in which one can amend their personal or business tax return to claim a credit or refund, or that the IRS can assess additional tax. The information below contains the periods of limitations that apply to income tax returns. Unless otherwise stated, the years refer to the period after the return was filed. Returns filed before the due date are treated as filed on the due date.

1. You owe additional tax and situations (2), (3), and (4), below, do not apply to you; keep records for 3 years.
2. You do not report income that you should report, and it is more than 25% of the gross income shown on your return; keep records for 6 years.
3. You file a fraudulent return; keep records indefinitely.
4. You do not file a return; keep records indefinitely.
5. You file a claim for credit or refund after you file your return; keep records for 3 years from the date you filed your original return or 2 years from the date you paid the tax, whichever is later.

6. You file a claim for a loss from worthless securities or bad debt deduction; keep records for 7 years.
7. Keep all employment tax records for at least 4 years after the date that the tax becomes due or is paid, whichever is later.



Be aware however that various states, counties, and municipalities have differing retention requirements for their tax related records. These requirements can be ascertained by contacting the applicable taxing authority for the jurisdiction in question.

Statute of Limitations by state

Each state has a Statute of Limitations that will specify how long records such as these must be maintained by businesses. Unfortunately, the Statute of Limitations is not uniform across all fifty states, nor is it consistent for varying types of documents within each state. The Statute of Limitations is intended to limit the timeframe during which a civil legal claim (i.e., lawsuit) may be filed against an individual, organization, or business for issues such as breach of a contract, delinquency of debt, liability for personal injury, or liability for property damage. Generally, the clock starts ticking once the contract is mutually entered into by all parties or the date the injury or property damage occurs. Please see the enclosed table to determine the minimum number of years your hotel's records must be maintained before disposal.

Computerized records

Even if your hotel has never been served a subpoena for "electronically stored information," it is time to review the company's protocol for retention of electronic records. In the rapidly changing programs and capabilities in the cyber world, there is a developing system known as "computer forensics." The expert technician in this skill is able to reproduce every email or computerized file any employee has ever created, sent, received, or deleted. The only way to truly delete any electronic record is by destroying the computer's hard drive or server where the file is stored. This of course assumes that no other copies of the email or record have been placed on any other hard drive or server. Remember, unlike paper-based records, once a written record is saved or transmitted electronically, it becomes a permanent record that can be discovered or recovered later.

Risk management records

One of the greatest adverse risks to hotels as it pertains to recordkeeping is associated with the completion of incident reports. Typically, when a guest or employee is injured, or someone suffers a personal property-loss or damage, an insurance claim may materialize, and/or an investigation is warranted, a manager or security officer will be called upon to write up an incident report. An incident report is a form that is filled out in order to record details of an unusual event that occurs at a lodging property, be it an injury/death, theft, loss or damage of personal property, or unexplainable event. The purpose of the incident report is to document the exact details of the occurrence while they are fresh in the minds of those who witnessed the event or found evidence of the event after the fact. This information is often useful in the future when dealing with liability issues stemming from the incident. However, to prevent exposing the hotel and Management to potentially greater liability than is warranted, it is essential that all incident reports be completed in an unbiased and matter-of-fact process that is free of speculation, implication of liability, or admitting fault.

Writing an incident report that even potentially suggests liability on the part of the hotel could result in an "adverse inference" by the court during a civil lawsuit where the case could settle for the plaintiff without trial. To prevent this situation, hotels should train their managers and security personnel in the following incident report protocols:

- All guest and employee incidents must be fully investigated by a manager or security officer. With the wide variety of hand-held electronic devices; pictures of the accident scene and entry of witness statements and facts of the case involving the "alleged" victim may be readily obtained. Pictures should show conditions of the area (such as for slip and fall incidents). In a "slip, trip or fall incident," be sure to picture the footwear – "flip-flops," sandals, clogs, high-heel shoes (note 4 inch or other height of heel, worn heels or soles, etc.).
- Train staff to enter "facts," only on the report. There should never be any assumptions.
- Do not "editorialize." Include date, time, weather conditions, structural or floor, step or other surface status (when applicable), contact info of witnesses and their statements.
- Minimize the amount of email exchanges on any given event. Phone or interpersonal discussion of questionable incidents is advisable. Just remember, anything committed to email can be recovered, unless your hotel has a policy of destroying the hard drive on a regular schedule integrated with retention protocol. If such a practice is formally adopted, be sure it is stated in a printed and published copy of your Standard Operating Procedures. This will avoid problems in court with the charge by the plaintiff that the hotel deliberately destroyed evidence. Yes, the hotel may deliberately destroy information, but as a regular standard business practice and not as a matter

of convenience to avoid pending legal liability. Of course, an incident that is obviously going to head for court should be reviewed with legal counsel before destroying such data.

- Special care should be taken that an email is not "ghosted" in your system. This is the retention of an email message by a staff member that has failed to clear the message from his or her saved messages. That will provide the plaintiff with the email when serving the company with a subpoena for "electronically stored information."

An expensive lesson learned

The potential for a major record liability problem occurred even back before personal computers were commonly used in the workplace; but this example reminds hotel managers to ensure that all unneeded information is deleted. Years ago the Sheraton Corporation (in pre-Starwood days) built the Hotel DuPont Plaza in San Juan, Puerto Rico. When they sold the property, they failed to remove some boxes of records from a basement storage area. The property did not have a fire sprinkler system. On the afternoon of December 31, 1986 an arson fire resulted in the death of 97 persons and injuries to over 140 individuals. The fire was started by three disgruntled employees of the hotel that were in the middle of a labor dispute. After investigations and on-site work by official organizations, the property was opened to plaintiff's attorneys. During their investigation, they discovered the old Sheraton records. This data included communications between senior Management and the architect. The architect originally envisioned two towers while senior Management prevailed on just one tower. Experts proved in court there would have been less loss of life if there had been two towers. Resultantly, Sheraton was assessed a $38 million dollar portion of the final settlement. If not for the discovery of those records, the plaintiffs would likely have been unable to win such a significant settlement on the part of Sheraton. ✧

(Ray Ellis, Jr., is the founder and director of the Loss Prevention Management Institute, an affiliate of HospitalityLawyer.com. He has spent more than 50 years addressing safety and security concerns in the hotel industry. His textbook, Security and Loss Prevention Management, available from the American Hotel & Lodging Educational Institute, is an authoritative source of information for hotel managers. E-mail: raycellis@gmail.com).