HR Electronic Records – United States

Electronic Archiving of Paper Originals

Legal Framework for Electronic Archiving

Although some countries require certain types of documents to be kept and archived in their original paper form, for most categories of documents, including HR-related records, there is no such requirement, and it is generally acceptable to use electronic versions of paper records (i.e., scanned copies of paper originals) during most government agencies' inspections and audits or in court proceedings.

The evidential or probative value of electronic versions of paper records may be more easily challenged before a court than it would be for the originals. This is mainly because the original records could be tampered with or changed before being scanned, and, unless proper technology has been used (e.g., encryption and timestamping), it may not be easy to detect such changes from a scanned copy. In specific situations, it may be good practice for employers to retain archives of paper originals in the event such originals would be requested by a specific investigator, auditor, judge or authority.

Are electronic scanned copies of paper originals legally valid?

The United States legal and regulatory framework for electronic archiving is a complex patchwork of various laws and regulations that are technology neutral and do not require certifications as in other countries. While there are some federal laws and regulations addressing electronic archiving, the regulatory landscape is further impacted by various state laws. Generally, no matter which law is at issue, for an electronic record to have the same legal effect as a hard copy document, the electronic archiving system must create an accurate, durable record that cannot be altered or modified and can be easily accessed.

Numerous laws implicating HR records do not prescribe a particular format. For example, no particular format for records is required under the Family Medical Leave Act (FMLA), the Fair Labor Standards Act (FLSA), Title VII of the Civil Rights Act of 1964 (Title VII), the Americans with Disability Act (ADA), the Age Discrimination in Employment Act of 1967 (ADEA), the Employment Retirement and Insurance Security Act (ERISA), the Occupational Safety and Health Act (OSHA), and the Immigration Reform and Control Act of 1986 (IRCA). However, if a party chooses to store such records electronically, the law or relevant regulations may require that the electronic archiving system itself meet certain requirements.

In addition, the federal Electronic Signatures in Global and National Commerce Act (E-SIGN), though primarily known for establishing a general rule that validates electronic signatures, also contains requirements for electronic record validity and retention. E-SIGN provides that, with limited exceptions, a record or contract relating to interstate or foreign commerce may be maintained in electronic format so long as:

- the record accurately reflects the information set forth in the contract or other record; and,

- the record remains accessible to all persons who are entitled to access by statute, regulation, or rule of law for the period required in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.

Under E-SIGN, federal and state agencies are permitted to require the retention of records in tangible or hard copy format only if "there is a compelling government interest relating to law enforcement or national security for imposing such a requirement."

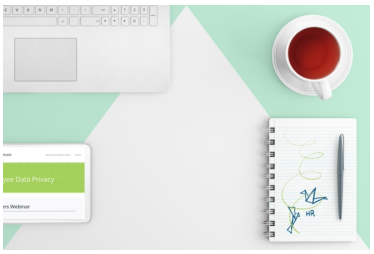
Moreover, the Federal Business Records Act, 28 U.S.C. §1732, provides reproductions of business records the same evidentiary status as originals so long as both the original record and the scanned copy were prepared in the regular course of business. This law further allows for the destruction of paper originals unless their preservation is required by law. Whether such records will be admissible and given full legal effect in a state court action will require an analysis of each state's statutes and evidentiary rules. Under the Uniform Electronic Transactions Act (1999) (UETA), which has been enacted in all states except New York, an electronic record cannot be denied admissibility in court simply because it is in electronic format. While New York has not adopted the UETA, its electronic signature law is similar to the UETA.

The UETA allows a record to be retained in electronic format so long as the electronic record:

- accurately reflects the information set forth in the record, and
- remains accessible for later reference.

Employers will still need to establish the necessary foundation for admissibility, such as through the Duplicate Writings Evidentiary Rule, the Original Lost or Destroyed Evidentiary Rule, and/or the Business Records Act.

In addition, many states have adopted a portion of the Uniform Photographic Copies of Business and Public Records as Evidence Act, which specifically provides for the destruction of the original document following the reproduction of the record unless preservation of the original is required by law or the original is held in a custodial or fiduciary capacity. Similarly, a handful of states have adopted some version of the Uniform Preservation of Private Business Records Act, which provides that if, during the regular course of business, a company makes a reproduction of an original business record by a process which accurately reproduces the original, preservation of the reproduction satisfies any law.



Are there any legal requirements for electronic archiving systems (EAS)?

As noted above, there are no overarching federal government regulatory certifications or encryption technology requirements for HR records. In fact, E-SIGN notes that any state laws that are not technology neutral will be preempted by E-SIGN. That said, any archiving of paper files in electronic format should create an accurate, durable, legible record that cannot be altered or modified and that can be readily accessed from a reliable, secure, and backed up system.

Form I-9: If a company wishes to maintain I-9 forms in electronic format instead of paper format under the IRCA, an employer must have an electronic system that has controls to ensure the integrity, accuracy, and reliability of the system; has controls to detect and prevent the

unauthorized or accidental creation of, addition to, alteration of, deletion of, or deterioration of an electronic I-9 Form, including the electronic signature; has controls to ensure an audit trail so that any alteration or change to the form since its creation is stored and can be accessed; has an inspection and quality assurance program that regularly evaluates the electronic generation or storage system and includes periodic checks of electronically stored I-9 forms (including electronic signatures); has an indexing system so that any particular record can be immediately accessed; has the ability to display a legible and readable copy on a video display terminal; and has the ability to reproduce legible paper copies. In addition, copies of I-9 forms must be available on three days' notice of inspection by the Immigration and Customs Enforcement (ICE). If the employer is unable to meet these requirements, the employer should use and retain paper I-9 forms.

There are also additional requirements which apply to the use of electronic I-9 forms, including any documents being electronically retained by the employer for I-9 purposes:

- System(s) may not be subject to any contractual/licensing agreement which would prohibit the federal government from accessing it at the employer's workplace.
- There must be an effective records security program which: limits access to authorized employees; provides for backup and recovery of records; includes employee training to minimize the risk of alteration/erasure; and, records all modifications to records including the date of access, the identity of the person who accessed the data, and action(s) taken.
- If the Form I-9 will be signed electronically, the system must include a method to acknowledge that the attestation has been read by the signatory, and this method should be attached to, or logically associated with the Form I-9. In addition, the system must: affix the signature at the time of electronically signing; create and preserve a record verifying the identity of the signer; and, if requested by the employee, provide a printed confirmation.
- Employers should also maintain documentation of the business processes and ensure it's available if requested by the federal government.

Form W-4: The IRS sets specific requirements for the storage of the electronic Form W-4:

- The storage system must (a) ensure adequate and complete transfer of the electronically signed Form W-4 to the archiving system, (b) index, store, retrieve, permit legible/readable viewing and, (c) have the ability to produce hard copies of the Form W-4.
- There must be system controls in place to protect the integrity of documents and prevent unauthorized activity.
- The electronic system must ensure that the information received from the employee is the same as the information sent to the IRS. All occasions of employee access that result in the filing of a Form W-4 should be documented.
- If the W-4 will be filed electronically through the employer's system, the system's design and operation must make it reasonably certain that the individual filing is the employee identified in the form.
- The electronic Form W-4 must include all of the information contained in the paper W-4.
- Employees must sign the electronic form under penalty of perjury. The form must

contain instructions immediately after the withholding section and immediately before the location of the electronic signature that make the perjury declaration mandatory.

- The electronic signature must be the final entry in the form. Note that the signature can be in any electronic form as long as the employer can establish a reasonable degree of certainty that the person who completed and submitted the form is the person who signed it.

- Employers must be able to print a hard copy if requested by the IRS.

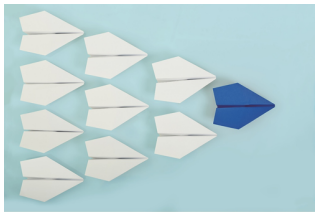
The FLSA and Department of Labor (DOL) do not require a particular form for payroll records, though the records must contain certain information about the employee and hours worked. However, whatever form the records take, the records are to be kept in a place where they can be made available within seventy-two hours. In addition, any electronic system must have viewing equipment, any reproductions or copies must be "clear and identifiable by date or pay period," and any records must be available on request.

Similarly, an employer maintaining electronic copies of FMLA, EEOC, ADA, or OSHA records must do so in a system that provides adequate projection or viewing equipment, provides reproductions that are clear and identifiable by date (or pay period if applicable), and makes the records available on request and as needed under the appropriate timelines within the applicable regulations or laws.

Likewise, any benefits information (such as pension and welfare benefit plan records under ERISA) may be retained in electronic format so long as certain requirements are met and a paper document does not have independent legal significance (such as a notarized document). The electronic records must be retained in a system that has controls to ensure the integrity, accuracy, authenticity, and reliability of the records; maintains records in reasonable order and in a safe, accessible place so that the records can be readily inspected or examined; allows records to be easily converted to legible, readable paper copies; is not subject to any agreement or restriction that would compromise or limit the ability to comply with ERISA's reporting or disclosure requirements; and has adequate records management practices established and implemented (such as labeling records and backing up electronic copies). In addition, all electronic records must be legible and readable from a video display terminal and on paper.

Protected health information (PHI) maintained under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) must be maintained in a system that is assessed for potential risks and vulnerabilities, has security measures sufficient to reduce the risks and vulnerabilities, has regular review for activity such as audit logs, access reports, and security incident tracking, and has both physical and technological security. The system is also required to have a contingency plan including data backup and a disaster recovery plan for restoring any lost data. The HIPPA Security Rule (45 CFR pt. 164.302 et seq.) establishes additional requirements for safeguarding PHI.

HR Best Practices: With limited exceptions, such as for a notarized document or other hard copy document that has independent legal significance, an electronic scanned copy of a



paper original is legally valid. If the authenticity of an employee record is questioned, the employer may be required to provide evidence that the scanned copy accurately represents the original. Electronic copies that accurately reflect the original in an unalterable form will generally have the same value as the original paper copy. There is no specific certification required, as various laws and regulations remain technology neutral.

The general principle is that the electronic records must be retained in a system that has controls to ensure the integrity, accuracy, authenticity, and reliability of the records; maintains records in reasonable order and in a safe, accessible place so that the records can be readily inspected or examined. One caveat to all laws and regulations is if a legal hold exists for anticipated or on-going litigation. In that instance, the original should be maintained in its original format.

Last updated May 2023.