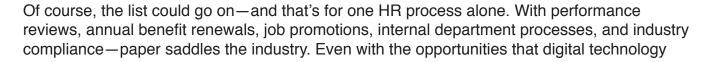July 07, 2016

Paper-laden HR departments reap savings, security benefits with e-signatures

By Pem Guerry and Lisa McCoole

Human resources professionals are well acquainted with the massive amounts of paper pushing necessary for just about any process. HR departments, after all, seem to live and die by documentation.

Consider a small sample of forms necessary for employee onboarding alone. HR reps will likely need to work with new employees to collect and sign a(n):

- Employee contract/offer letter
- I-9 form
- W-4 form
- Direct deposit form
- Benefits approval form
- Consent for background checks
- Consent for drug testing
- Confidentiality/nondisclosure agreement
- Compliance form(s)
- Acknowledgement form(s)
- Noncompete agreement
- Employee handbook acknowledgement/consent
- Performance objectives and goals document

Of course, the list could go on—and that's for one HR process alone. With performance reviews, annual benefit renewals, job promotions, internal department processes, and industry compliance—paper saddles the industry. Even with the opportunities that digital technology

affords, an [ADP survey](#) found that 60% of all HR department respondents store some employee records in paper files.

Where paper hurts

The most obvious problem with managing paperwork in its paper form is how much it affects your bottom line. Department heads must plan to spend money on ink for printers and photocopiers; paper reams; envelopes; mailing, shipping and courier services; faxing; storage; and filing—all of which accumulate quickly, especially within larger enterprises where there are hundreds or thousands of employees to manage.

Paper-based HR workflows also interrupt important processes. When mailing documents for signatures, it can take several days to get them completed and back to the office. Also, because paper forms can't establish mandatory fields in the way digital forms can, some places to sign or initial will be missed—meaning time must be devoted to completing the forms correctly a second time.

Even for HR departments that may take advantage of digital storage and other applications, unless e-signature technology is integrated into HR workflows, documents must leave their digital environment and be printed solely for the sake of a signature. Again, this interrupts a streamlined process and snags workflows with inefficiency.

Implementing technology strategically

While HR digital technology, such as cloud-based forms software and e-signatures, can transform day-to-day operations, HR professionals cannot walk blindly into adoption. There are several [key elements to the technology](#) and implementation to carefully consider so that you establish a solid, secure, and legally sound foundation for digital work.

E-signatures are not made equal

Electronic signatures eliminate the paper crutch. Documents can remain digital from start to finish because they can be sent by HR professionals to employees (or colleagues, vendors, etc.) for signing online within a secure, cloud-based platform. Because of the Electronic Signatures in Global and National Commerce (ESIGN) Act of 2000, these e-signatures carry the same legal weight as any wet ink signature.

But the type of e-signature software used matters a great deal to the long-term validity of HR

documents. Of course, a legally sound and valid document is essential for compliance and corporate best practices.

Some documents, such as the I-9 form, must stay on file and remain valid for an employee's entire tenure with a company—which could be a matter of days or decades. And that's really the bare minimum. Because lawsuits could occur well after an employee leaves a company, it's wise to keep many HR documents on file for several years after an employment relationship ends, as those documents may need to be verified in court.

An independent e-signature, or digital signature, is a specific type of e-signature that permanently embeds the legal evidence, including cryptographic information that verifies a signature has come from the correct party, into a signed document using published standards. As such, this signature's validity can be proven with any free PDF viewer—online or offline—with no reliance on a vendor.

A dependent e-signature, by contrast, stores its legal evidence on a vendor's server, where it is accessible only by a link. That is, users must rely on an Internet connection, a working link, and a relationship with the vendor to access proof of validity. What's more, dependent e-signatures are based on private, proprietary standards that exist outside the public domain, meaning they may easily crumble under legal scrutiny.

Both independent and dependent e-signatures can be appropriate for signing documents. However, when important or high-value transactions are involved, or if any document needs to remain valid for at least 6 months, independent e-signatures will provide the highest level of assurance that the digital documents will remain secure and valid into the unforeseeable future.

Authentication strategy matters

HR holds scores of sensitive information in its files—and many documents, like personnel reviews or financial documents, are strictly confidential. So digital documents must only be accessible by authorized individuals.

This is where identity authentication technology and strategy are essential. HR professionals will need to balance usability with security, so it's important to know what authentication options are available to match the right method with the right documents.

- **E-mail-only authentication.** Requires a user to log in to his e-mail account and click a link to access documents.

- **Text message authentication.** Requires a user to provide a one-time password sent via a text message.
- **Shared secret questions.** Requires a user to answer personal security questions previously provided, such as a pet's name.
- **Know your customer (KYC) authentication.** Requires a user to correctly input his or her Social Security number and date of birth.
- **Knowledge-based authentication.** Requires a user to correctly input his or her Social Security number and date of birth and then to correctly answer a series of questions based on information found in public databases.
- **Multi-factor authentication.** Combines two or more authentication methods. This doesn't have to be complex. For example, many find that the combination of e-mail authentication and text message authentication is convenient, since almost everyone has a mobile phone that's easily accessible.

Restriction controls are essential

Documents may contain medical, personal, or otherwise confidential information. When documents are kept purely digital, once they are signed, they can be stored in a central digital repository where they can be accessed by anyone with the right credentials. Credentialing boundaries should be set both within technologies and company policies.

Following the right steps for implementation, secure e-signatures and digital documentation will save money, space, and time so that you can focus on what's most important: bridging corporate and employee wellbeing.

Pem Guerry is the executive vice president at SIGNiX, an Independent E-Signature™ solutions provider that makes signing documents online safe, secure, and legal for any business. SIGNiX offers an independently verifiable cloud-based digital signature solution, which combines workflow convenience with superior security. Learn more about what makes SIGNiX different at www.signix.com.

Lisa McCoole is vice president of Channel Sales at Treeno Software, a leader in the Enterprise Document Management industry. Learn more about Treeno at www.treenosoftware.com.