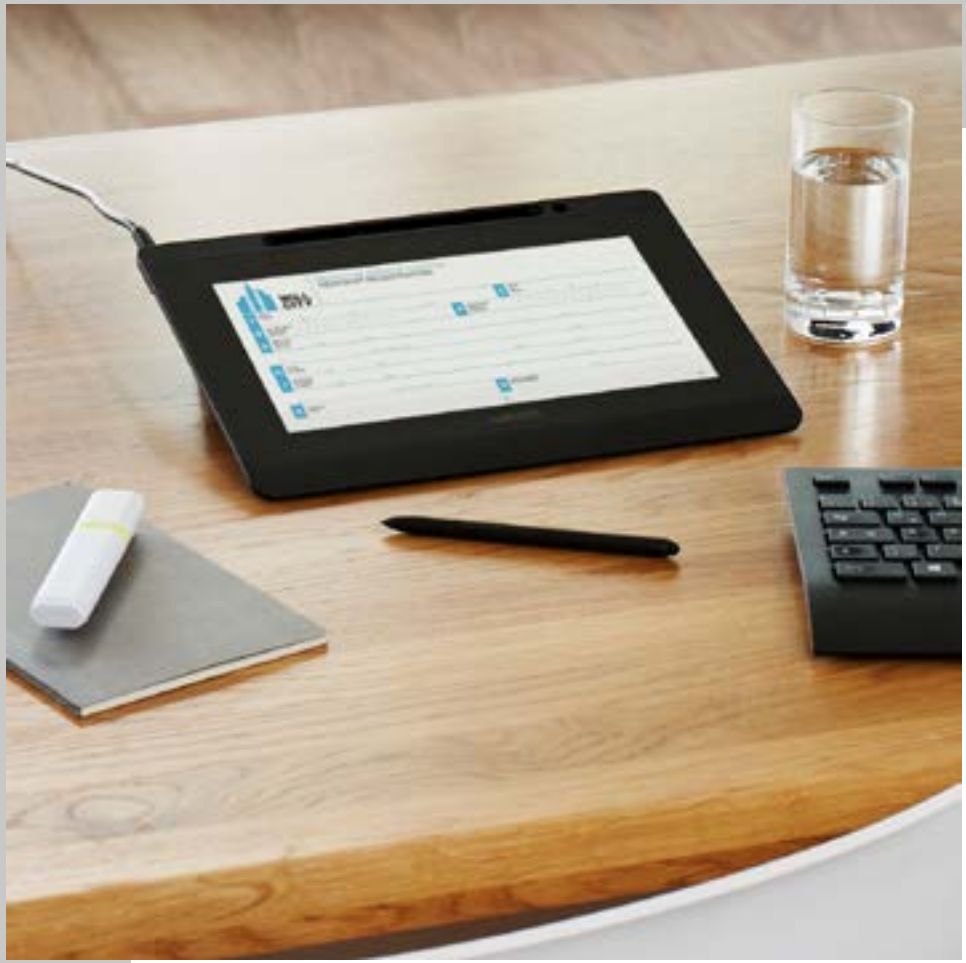
Best Practice Guide

Five Simple Rules

for Utilizing Electronic Signatures



wacom® for Business

BACKGROUND

Signed in 2000, the ESIGN Act ensures that electronic signatures have the same legal force as wet-ink on paper signatures, provided that minimum standards, such as those in this guide are met.

KEY RECOMMENDATIONS

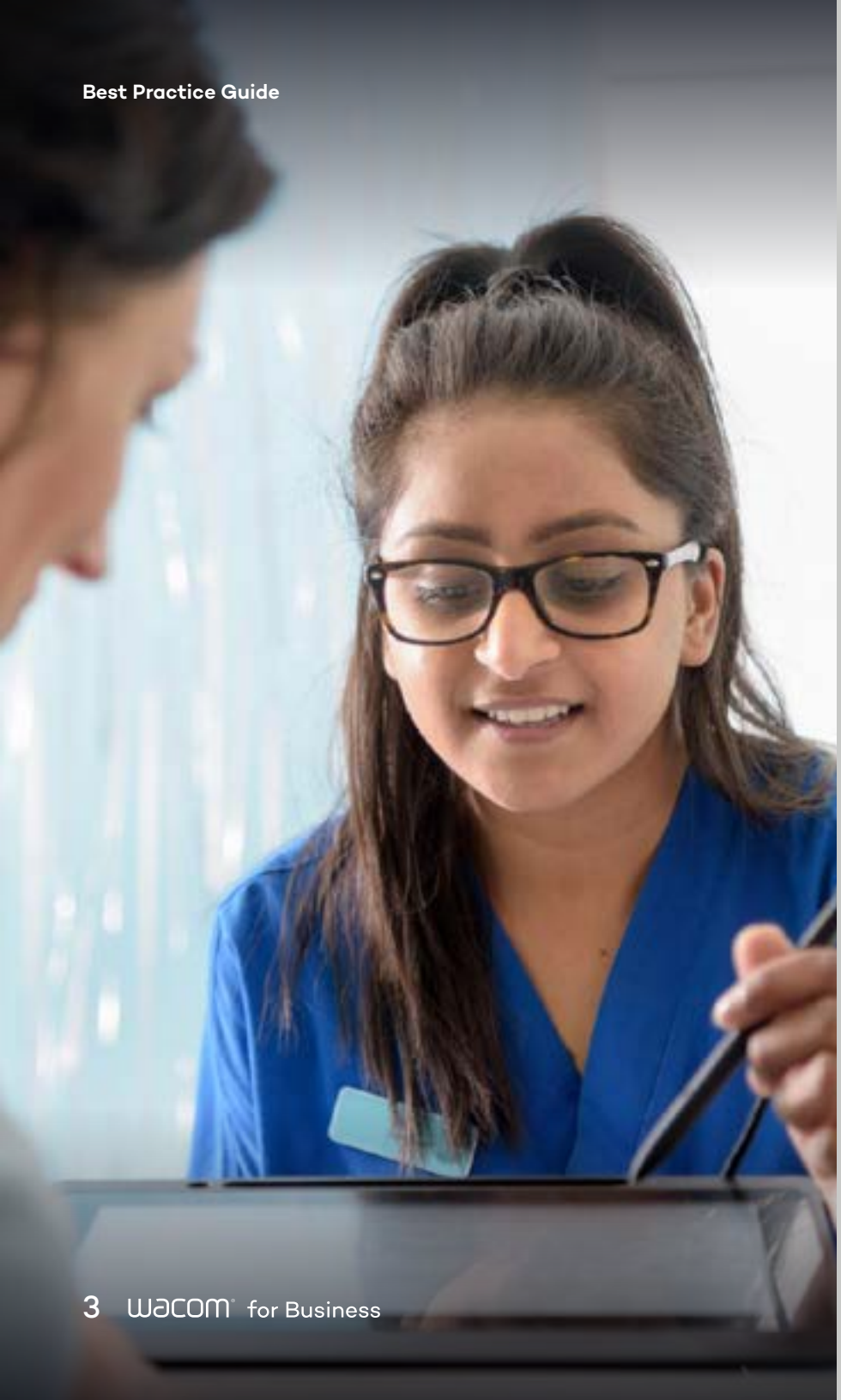
- Display the terms
- Provide copies of all documents to consumers
- Verify's signers identity
- Clearly demonstrate consent
- Maintain message integrity and an auditable trail

Laws and Regulations
Governing eSignatures in the US

In the United States, electronic signatures have the same legal force as wet-ink or pen-on-paper signatures provided that the specific guidelines laid out in the legislation are met.

The two primary laws addressing electronic signatures in the United States are the Electronic Signatures in Global and National Commerce Act (E-Sign)[1] and Uniform Electronic Transactions Act (UETA)[2]. The ESIGN act is a federal law and is the broadest general regulation for the use of electronic signatures. The ESIGN law requires states and corporations to recognize electronic signatures as having the same force of law as a "wet" or pen-on-paper signature. UETA is a state-level statute that provides for uniformity among state regulations for paper documents like checks and eSignatures. It has been adopted by 47 states, plus Washington DC.

Per this legislation, an electronic signature must include an auditable data trail to ensure the three key components of legally binding signatures are present: intent, non-repudiation and authentication. In order to ensure that your electronic signature utilization meets this criteria, we recommend following the five simple rules outlined below.



#1:
Display the terms

Whenever a consumer signs a document, it must be clear what they are signing. This can most easily be achieved using an interactive pen display monitor where consumers can review documents and sign on the same screen. We recommend a minimum 10" screen for easy viewing. Alternatively, you can use a signature pad and provide a copy of the form being signed on a second monitor or on a laminated piece of paper.

#2:
Provide copies of documents

Each signer need to be provided with a copy of all consents on paper or via email. They must be told how they can access the information in the future, how they can withdraw their consent (and any associated costs/consequences) and how they can update their contact information if needed. Whatever format the information is provided in should be annotated in their record.

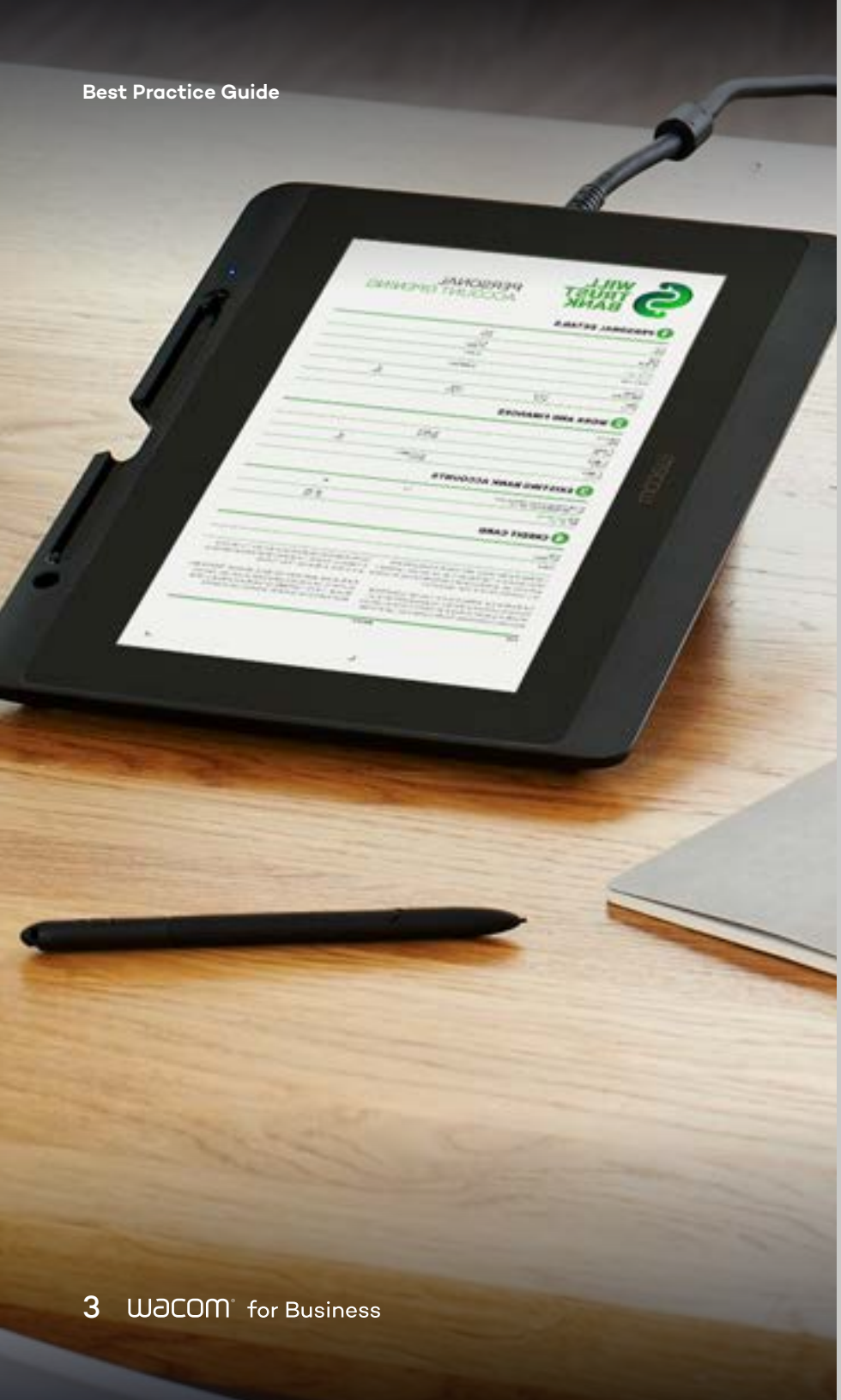
#3:
Verify the signer's identity

It is the responsibility of the organization who retains the form to verify the signer's identity and to be able to attribute that signature to the signer. Identity verifcation ca can be done many different ways including photo ID, fingerprints or signature verification. Maintaining a record of ID verification is the responsibility of the organization.

In addition to verifying the signer's identity, when utilizing a remote-signing solution organizations must ensure that the signer is the named individual in the agreement. This attribution data can include email address, passwords/PINs, IP address and date/time stamps. All attribution data must be stored securely with the document and be unable to be edited after signing.

#4:
Clearly demonstrate consent

One requirement present in all eSignature laws is the concept of affirmative consent. It is not sufficient for a customer to "opt-out" of any consent or service. Each customer needs to proactively opt-in. Consent can be determined by a number of things including an electronic signature affixed to each document individually. This should be one of your primary considerations when implementing a new eSignature solution.



#5:
Maintain an auditable trail

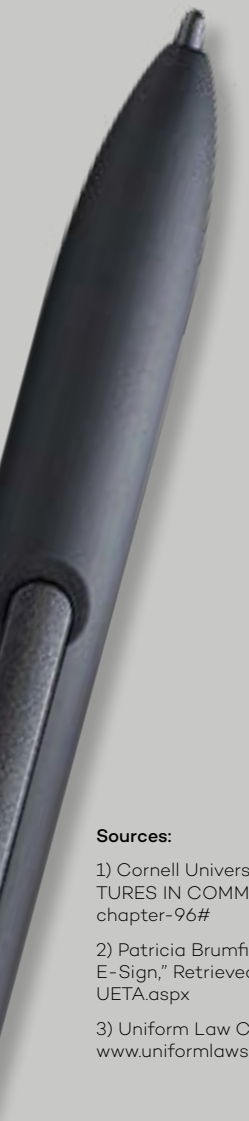
Just as with paper records, copies of electronic files must be maintained for the time required by law. Further, signed documents must store the signature attached to the signed file. This signature data should include a time and date stamp as well as the individual's name (either typed or printed clearly). The file should not be editable and an auditable process must be in place to verify that a document has not been changed after signing.

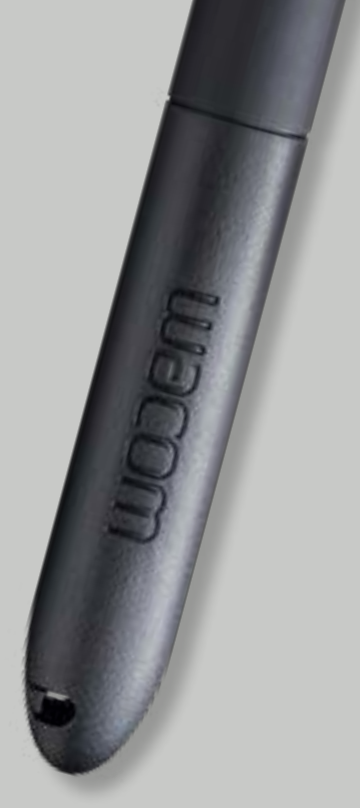
In addition, the record must be held by securely and be accessible to the customer upon request. This is an important consideration when choosing an eSignature software as some SaaS cloud vendors can maintain copies of signed documents on a central server by default.

Instead, we would recommend using an on-premise set up that includes an encrypted signature pad or pen display which connects directly into your workstation. Key data should be stored on-premise or on enterprise-owned secure servers, which may be located elsewhere. This can help ensure data is stored securely and provides your staff with a better user experience. It also ensures that all copies of the consent or other record reside within your system and can be retained even if you change service providers.

One additional best practice is to document your process and audit it for ongoing compliance. This will yield numerous benefits when selecting a vendor, implementing new processes and will help cover you in case of an audit by any accrediting institution.

More human
More digital





Connect with Wacom today to demo digital pen and ink solutions for your business:

1-503-525-3100 /// esign@wacom.com

Wacom for Business leverages decades of leadership in digital pen technology to help organizations digitize processes that require in-person interaction. We enhance Wacom and third-party pen-enabled devices with software that stores and displays biometrically accurate digital ink. These integrations empower our global network of partners to seamlessly incorporate handwritten electronic signatures and annotation into organizational workflows. The result: Paperless processes with a familiar yet digital pen and paper feel. Moreover, our WILL™ 3.0 (Wacom Ink Layer Language) standard for universal ink is powering new applications that will ensure the next generation of customer experiences are more human, and more digital.

Sources:

1) Cornell University Law School, "15 U.S. Code Subchapter I - ELECTRONIC RECORDS AND SIGNATURES IN COMMERCE," Retrieved: February 13, 2017 from https://www.law.cornell.edu/uscode/text/15/chapter-96#

2) Patricia Brumfield Fry, University of Missouri School of Law, "Why Enact UETA? The Role of UETA After E-Sign," Retrieved February 13, 2017 from http://www.uniformlaws.org/Shared/Docs/Why%20Enact%20UETA.aspx

3) Uniform Law Commission, "Why States Should Adopt UETA," Retrieved February 13, 2017 from http://www.uniformlaws.org/Narrative.aspx?title=Why%20States%20Should%20Adopt%20UETA

wacom® for Business

business.wacom.com

Wacom Technology Corporation 1455 NW Irving Street, Suite 800 | Portland, OR 97209 USA
esign@wacom.com · 1-503-525-3100