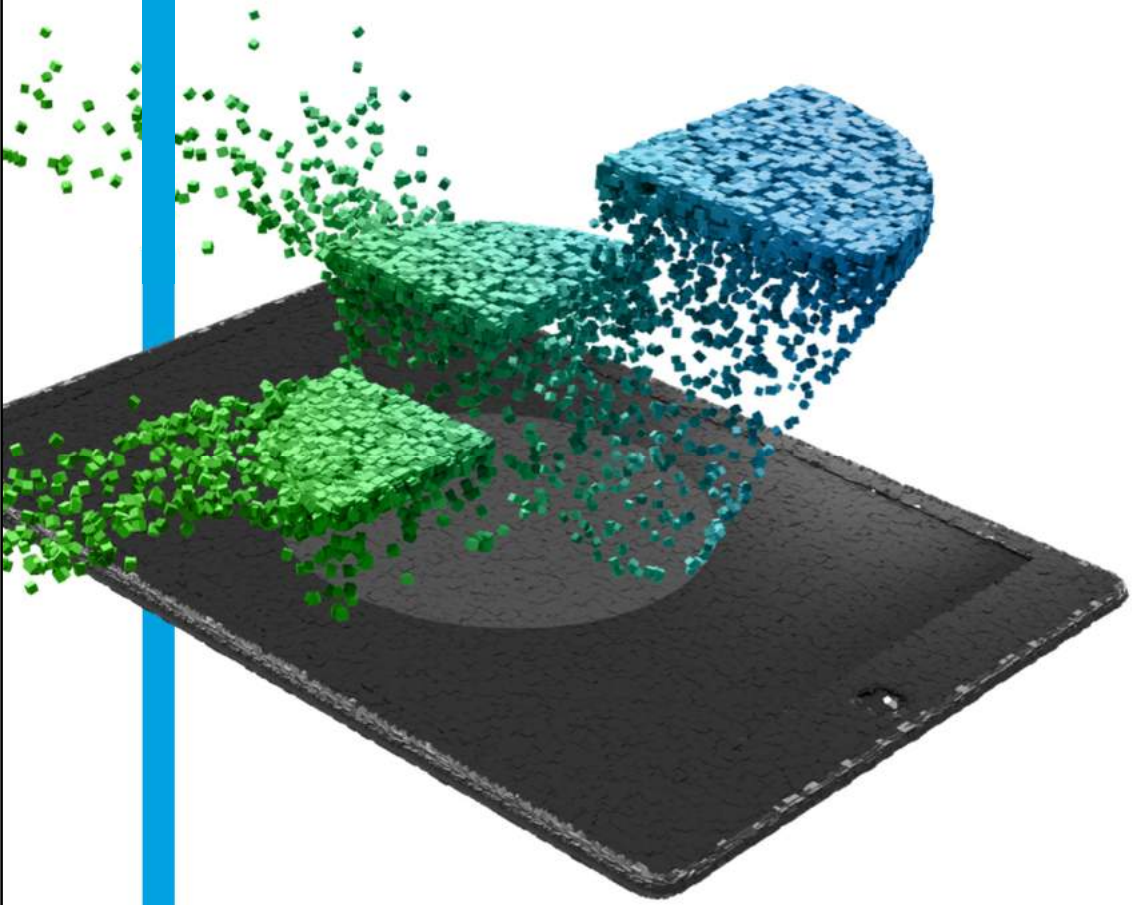
IMS Health & Quintiles are now IQVIA®



Electronic Informed Consent (eConsent)

A Vendor Perspective

8 October 2019

Karen Maduschke, Director of Client Engagement
Patient Solutions

IQVIA eConsent: The Global Industry Leader

More than 200 studies launched in over 50 countries, across nearly every therapeutic area

5,000 sites

15,000 site users

30 pharma clients

50,000 patients

60 languages

14 years

Countries

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Cameroon
Canada
Chile
China
Czech Rep
Denmark
Egypt
Estonia
Finland
France
Germany
Greece
Guatemala
Hong Kong
Hungary
Iceland
India
Israel
Italy
Japan
Korea
Latvia
Malaysia
Mexico
Netherlands
New Zealand
Norway
Peru
Philippines
Poland
Romania
Russia
Saudi Arabia
Singapore
Slovakia
South Africa
Spain
Sweden
Switzerland
Taiwan
Thailand
Turkey
Ukraine
United Kingdom
United States
Vietnam

Extensive experience with both central and local IRBs and Ethics Committees

Therapeutic Areas

Bone / Osteoporosis
Hematology
Ophthalmology
Cardiovascular
Immunology
Inflammation
Respiratory
Diabetes
Internal diseases
Rheumatology
Orthopedics
CNS / Neurology
Infectious Diseases
Pulmonology
Dermatology
Endocrinology
Nephrology
Vaccines
Gastroenterology
Oncology
Women's Health

Signature Modalities

eSignature - in about a dozen countries
Print-to-Sign – accepted globally

IQVIA™

eConsent Benefits

Why Use eConsent?

Paper consent forms are fraught with problems that cost time and money

Difficult language

Inconsistent messaging

No transparency / accountability

No audit controls

Frequent regulatory failures

Poor version management & control

eConsent Benefits Everyone in the Clinical Trial

Proven value for all stakeholders in the clinical trial process

Participants

- View multimedia education & flag question areas
- Better understand risks and benefits
- Higher levels of satisfaction
- Better adhere to protocol

Trial Staff

- Eliminate repetition in explanations and providing own definitions
- Version and document management
- Automatically record consent notes
- Streamlined re-consents

Monitors

- View real-time consent status across sites
- Easily access detailed audit trails
- Rely on date/time stamps
- Access optional consent element reporting

Sponsors

- Assured of the integrity of the consent process
- Fewer consent-related audit findings
- Global signature compliance
- Useful analytics
- Better recruitment and retention rates

eConsent System Components

One web-based system with controlled access for all stakeholders

A web portal that can be accessed from a desktop, laptop or any Internet-enabled device at the study URL:

- N. America & LATAM: https://iqvia.secureconsent.com
- EMAE & APAC: https://iqvia.secureconsent.eu

A patient-facing tablet that staff set up for each patient to use on site

- Devices are not taken home
- Require an Internet connection, as no data is stored on the device
- May use dedicated iPad or deploy on an eCOA / ePRO device
- Patients never need a login or password
- Provides a simple, secure, and mobile way for patients to read at their own pace

Data Security and Privacy

IQVIA™ TECHNOLOGIES

ELECTRONIC INFORMED CONSENT

System Overview and Security Features

SecureConsent is a fully validated electronic informed consent (eConsent) system in use for clinical research in the US since 2005 and in the EU since 2009. It was designed to improving quality, efficiency and transparency for sites and sponsors throughout the clinical trial process, while improving potential participants' comprehension, knowledge retention, and satisfaction compared to a paper-based consent process.

eConsent Hardware

The eConsent system is device-agnostic and can run on Apple, Android, or Windows based hardware, and the system can be deployed on numerous third-party /eCOA devices for patient-facing activities. Monitors, CRAs, Auditors, and Site Staff will be able to engage in ICF preview, reporting, analytics, and other administrative functions from both the mobile device and desktop systems, according to the role--based access. Touchscreen devices are ideal for patient-facing activities as they facilitate biometric advanced electronic signatures and simplify usability. The system runs from redundant HIPAA/PCI certified data centers where dedicated servers are hosted. These servers are Dell PowerEdge R710s running Windows Server 2012 and Microsoft SQL 2012. The tablets running eConsent do not store data locally, as anything that is captured is immediately transmitted to the secured servers over an encrypted connection. Data centers are all equipped with redundant firewalls, which are continually monitored and regularly audited by IT staff.

Security Features

1. SecureConsent is a validated FDA 21 CFR Part 11 and EC Annex 11 compliant system for electronic informed consent that runs under a controlled quality system.
2. The application and its supporting network infrastructure are regularly subjected to state-of-the-art vulnerability scans and penetration tests executed by a validated independent third party.
3. All data handled by SecureConsent are encrypted in transit and at rest. SecureConsent uses AES-256 encryption over the HTTPS/TLS protocol. No unsecured sessions are permitted under any circumstances. This means that even if the data is hacked or intercepted, it will be indecipherable and meaningless.
4. Study sites use SecureConsent on touchscreen tablets, but no data is ever stored on tablets. Data is immediately encrypted and transmitted to the central server upon capture. There is no risk of inappropriate disclosure should a tablet be lost or stolen.
5. Tablets are configured with AirWatch Mobile Device Management software, which limits the device to be used for its intended purpose, restricts the URLs that can be accessed, and allows the support team to remotely troubleshoot, disable or update the device, or locate it if it is lost.

Data Security and Privacy

- Data encryption (AES-256 in transit and at rest)
- Private hosting environments (US, France, Germany)
- Fully redundant systems
- Annual disaster recovery tests
- Certified by the US Department of Commerce and by the US-EU Privacy Shield program
- Sensitive information is data-fenced
- All data is stored in tamper-proof and unalterable databases
- Web application and network infrastructure tested by a validated independent third party

Regulatory Compliance

✓21 CFR-Part 11 Compliance

- Robust documentation of SDLC, SOPs & Policies
- Extensive, ongoing systems validations
- CAPA program
- Training Programs
  - GCP
  - Site-staff training and documentation
- Detailed audit trails
- External/Internal Audit Procedures
- Risk Assessment

✓ HIPAA/PCI Compliance

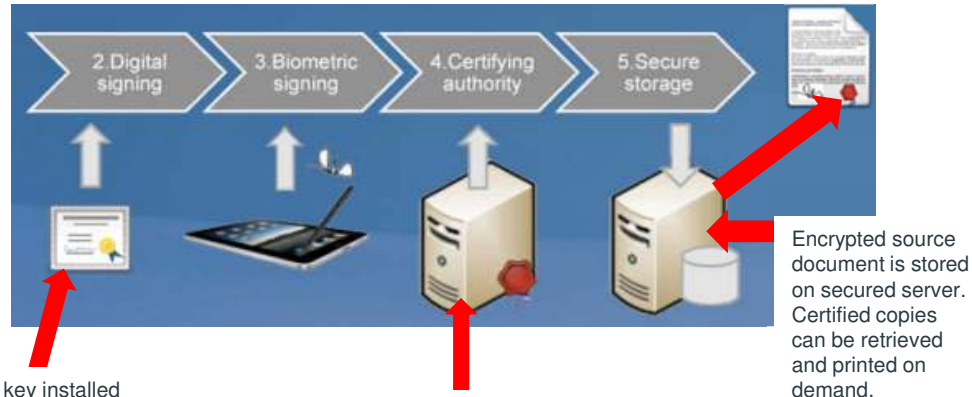
✓ Privacy Shield Certification
✓ EU Annex 11
✓ EU Data Privacy Laws
✓ EU eIDAS compliant

- ***EU Servers located in Frankfurt and Strasbourg***
- ***All PI/PHI stays in EU***
- ***Aggregated / De-identified data can be viewed outside of EU***

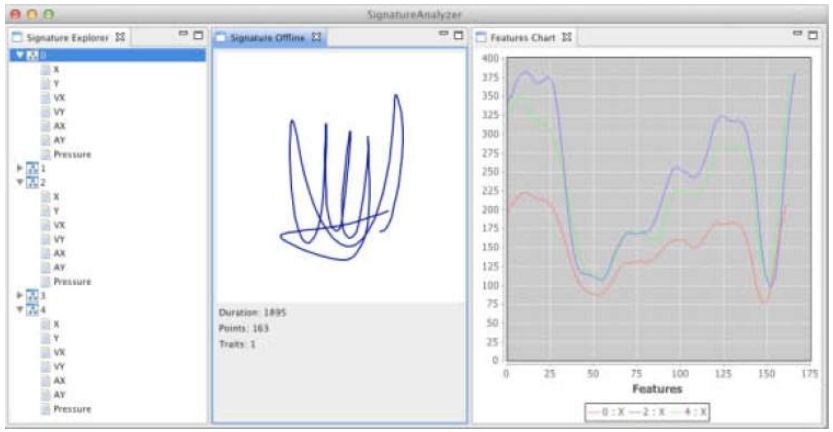
Biometric Electronic Signature

✓EIDAS-Compliant Signature

- EU Advanced Electronic Signature compliant
- Forensically identifiable – superior to wet-ink signature
- Legally binding
- No PKI key required by patient



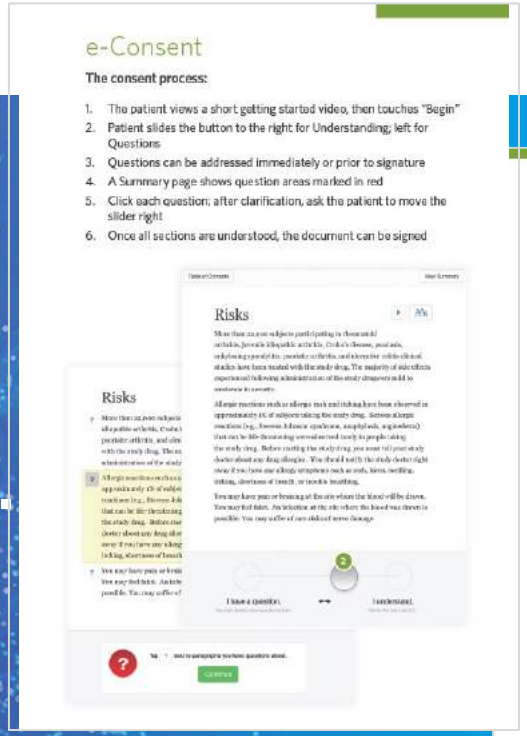
In case of dispute, the biometric signature can be extracted from the document to provide a forensic examiner with a signature analysis tool to verify the signer's identity.

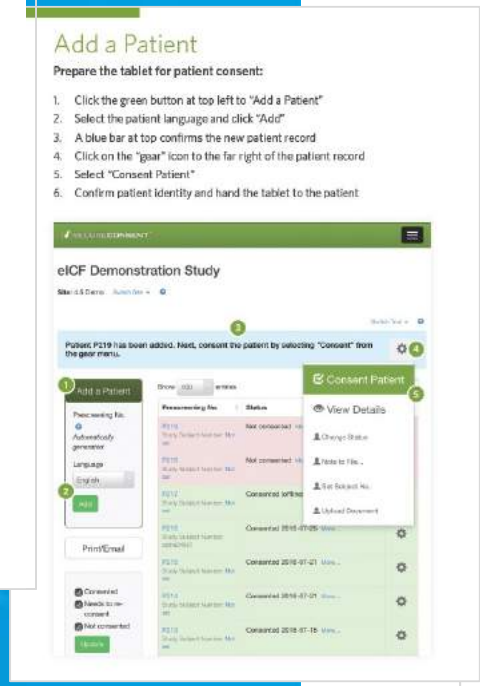


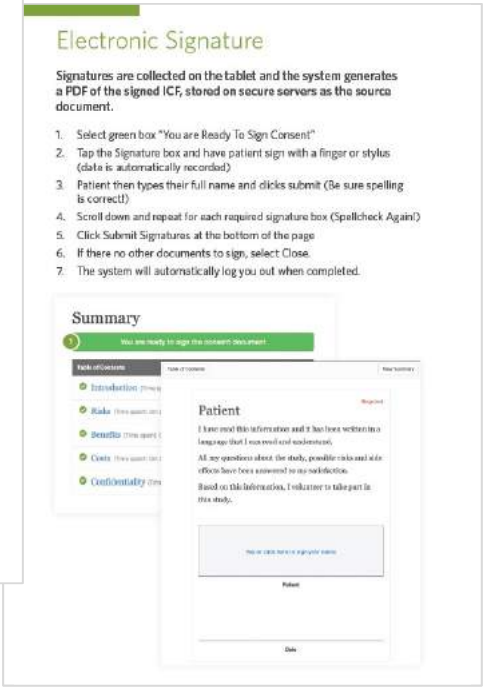
The legal validity of the signature is achieved in two ways:

1. The identity of the signer can be determined manually by an expert and automatically with very high certainty.
2. The signature is embedded and hashed within the document and cannot be removed except by injunction.

Demonstration….



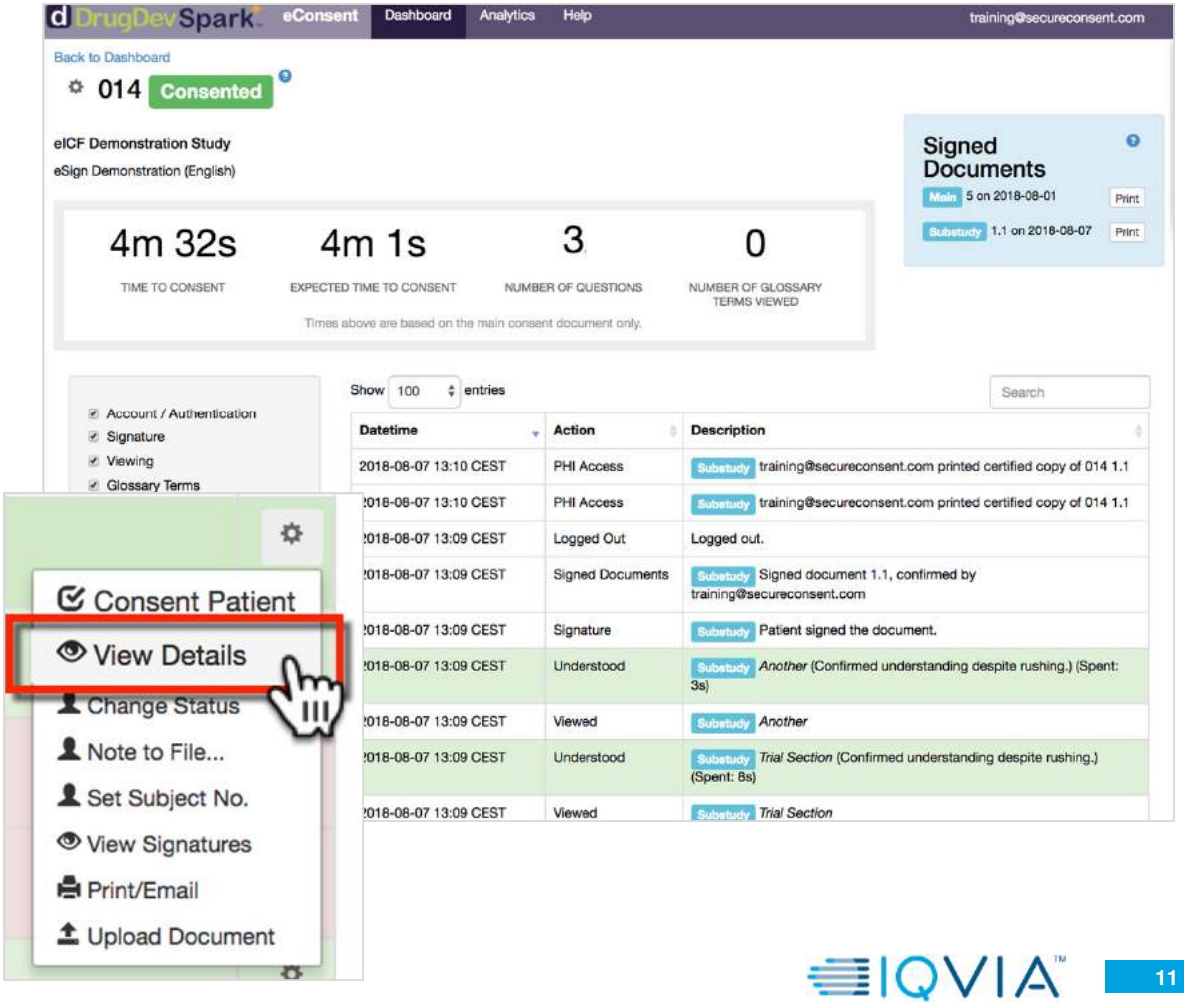




Audit Trail

The audit trail keeps a reliable, unalterable record of all consent-related activities

- The audit trail shows all activity taken by or on behalf of the participant:
  - Start of consent visit
  - Document version read by the patient
  - Study staff involved in consent visit
  - Question areas
  - Viewed glossary terms
  - Time to read consent and when all areas were marked as “understood”
  - Note to files
  - Electronically signed documents
- **With print-to-sign, source documents are kept on site and no PII is stored in the system; signed documents can NOT be printed from the portal**




Q
A

Thank you!

Karen Maduschke
Client Engagement Director, Patient Consent
karen.maduschke@iqvia.com