**Next-gen security
Customizing access profiles for peak performance**

Presented by
Sofie Webers, Head Document Management, SGS Pharma
Cristina Iannaccone, Document Management Associate, SGS Pharma

Meet the Speakers

Sofie Webers

Title: Head Document Management

Organization: SGS Pharma – Clinical Research

With 18 years at SGS Health Science, Sofie is currently responsible for the overall management and maintenance of the eTMF system. She played a key role in the transitioning from paper TMF to eTMF, streamlining Document Management and enhancing digital accessibility.

Cristina Iannaccone

Title: Document Management Associate

Organization: SGS Pharma – Clinical Research

Cristina is a Document Management Associate since 2022, specializing in eTMF activities from initiation to archiving. With a strong focus on quality control, user management and training, she ensures compliance and efficiency throughout the document lifecycles.

SGS

Disclaimer and Disclosures

- *The views and opinions expressed in this presentation are those of the author(s) and do not necessarily reflect the official policy or position of CDISC or SGS Pharma.*

- *The author(s) have no real or apparent conflicts of interest to report.*

Agenda

1. EMA Guidelines: The Security Foundation
2. How do we bring these guidelines to life?
3. Conclusions

SGS

1. EMA Guidelines: The Security Foundation

Protecting Trial Integrity Through Controlled Access and User Qualification

SGS

Treatment Blinding Maintenance

Ensuring unblinded access is restricted without permission

Access Authorization Recording

Keeping a retrievable record of document access permissions

Permission Change Tracking

Recording changes to user roles and access rights

Unauthorized Access Prevention

Implementing measures to block unauthorized system entry

Role-Specific Training

Providing training based on specific user roles

EMA Guideline on computerised systems and electronic data in clinical trials

2. How do we bring these guidelines to life?

2.1 Tailored Security Profiles

2.2 Controlled Access to Blinded Documents

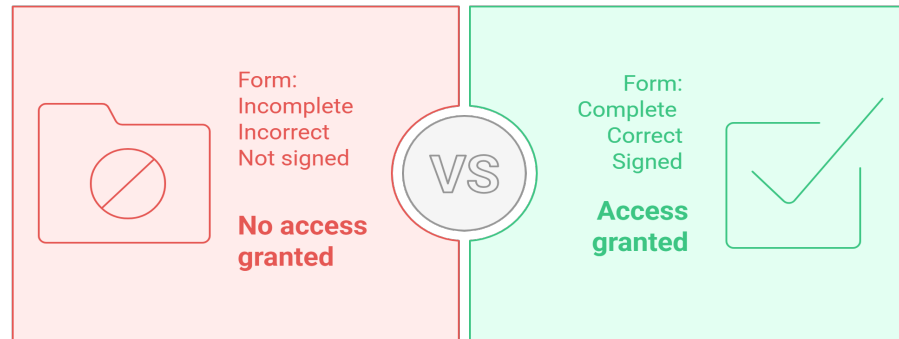2.3 Controlled Document Sharing & Seamless User Transitions

2.4 Yearly User Account Revision Process

2.5 Triannual System Upgrades

SGS

2.1 Tailored Security Profiles

Completion of Account Management Form:

➤ By the Line Manager for Internal users
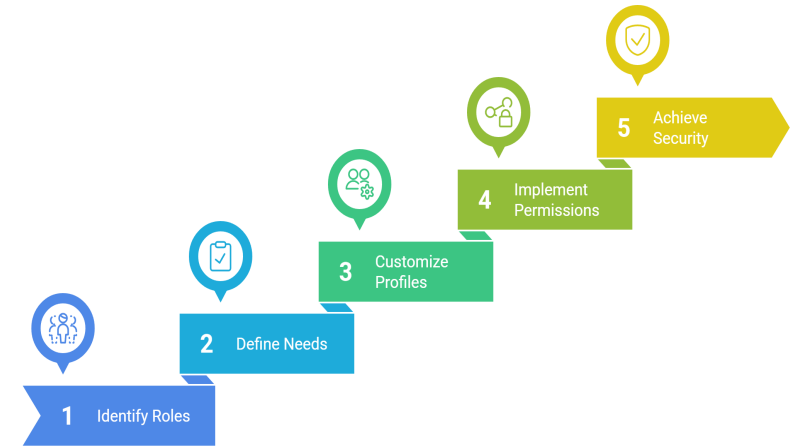
➤ By the Project Manager for External users

Form:
Incomplete
Incorrect
Not signed

No access granted

VS

Form:
Complete
Correct
Signed

Access granted

All signed forms are stored in our eTMF

2.1 Tailored Security Profiles

Identify Roles

Profile Type 👤	Trial Access 🔎	Document Access 📁	Workflow Participation 👥
SGS Internal	All trials	All draft & final documents (source, rendition, audit trail)	✓ Review ✓ Co-authoring ✓ eSignature
Sponsor	Trial-specific	All final documents (source, rendition, audit trail)	✓ Review ✓ Co-authoring ✓ eSignature
Third Party	Trial-specific	Limited to assigned documents	✓ Review ✓ Co-authoring ✓ eSignature
Auditor	Trial-specific	All final documents (rendition and audit trail only)	✗ No workflow participation

1 Identify Roles
2 Define Needs
3 Customize Profiles
4 Implement Permissions
5 Achieve Security

Effective eTMF security requires role-based access profiles tailored to diverse stakeholders, preventing unauthorized access that would compromise data integrity and regulatory compliance

cdisc

SGS

2.1 Tailored Security Profiles

Training
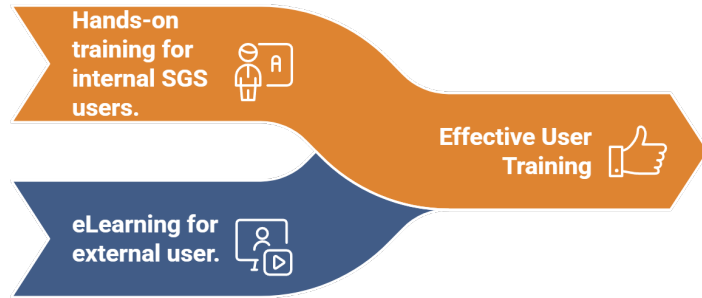
- ➤ Focused Learning
  - ✓ Only relevant tasks covered
  - ✓ No information overload

Hands-on training for internal SGS users.

eLearning for external user.

Effective User Training

- ➤ Time Efficiency
  - ✓ Reduced training costs
  - ✓ Minimized time requirements
  - ✓ Faster backup assignments

- ➤ Clear Role Definition
  - ✓ Precise understanding of system responsibilities
  - ✓ Enhanced compliance

Enhanced productivity with reduced training time

2.2 Controlled access to blinded documents

Automated Safeguards for Blinded Document Management

Fully Automated Blinding

Signed access request

Manual Metadata Assignment

- ✓ Require signature of Line Manager of unblinded group

- ✓ Manage classifications through backend settings

- ✓ Eliminate manual metadata assignments

- ✓ Automate document classification upon upload

- ✓ Prevents accidental exposure of sensitive information

- ✓ Eliminates human error in document handling

- ✓ Ensures consistent regulatory compliance
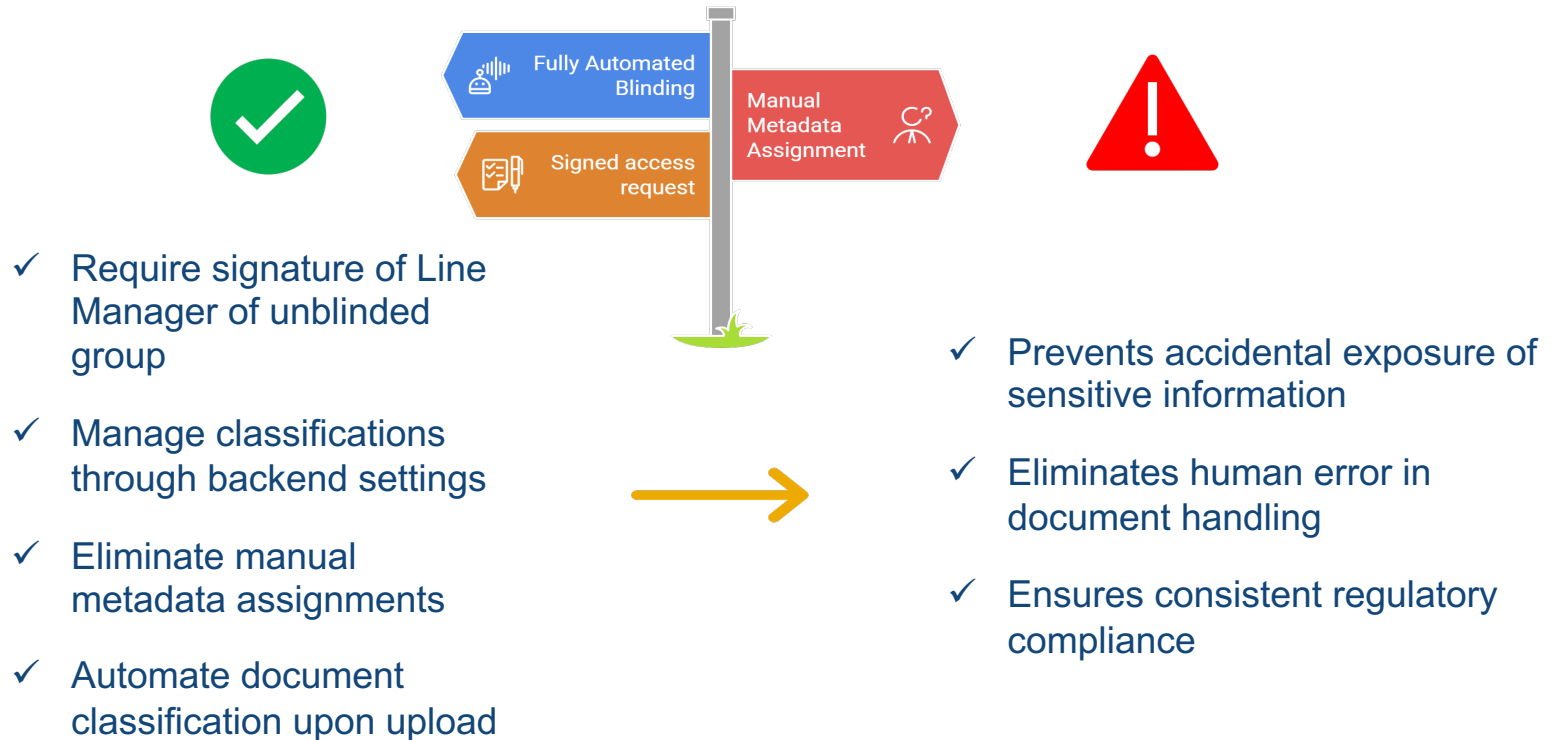
2.2 Controlled access to blinded documents

Automated Safeguards for Blinded Document Management

Our system applies security at the classification level.

Example 1: Classification 11.02.01 (Randomisation Plan) - editable by SD/SDAP* only, hidden from others

Example 2: Classification 11.04.02 (Statistical Reports) - editable by PK/STAT, viewable by all

Document Type	Classification	PLANNED DOCUMENT	READ/WRITE	READ ONLY	SERVICE	SERVICE APPLICABLE?
11 Statistics	11.02.01 Randomisation Plan	Randomisation list specification (RLS)	SD/SDAP group	none	Randomisation	APPL
11 Statistics	11.02.01 Randomisation Plan	Medication list specification (MLS)	SD/SDAP group	none	Randomisation	APPL
11 Statistics	11.04.02 Statistical Report	Statistical Report	PK group STAT group	All users	Statistical Report	NAP
11 Statistics	11.04.02 Statistical Report	PK(PD) Report	PK group STAT group	All users	PK(PD) Statistical Analysis	APPL

* Secure Data Analytical Programming: Dedicated separate group handling all unblinding data e.g. randomization data

2.3 Controlled Document Sharing & Seamless User Transitions

The "Workflow Participant" Role

Study A
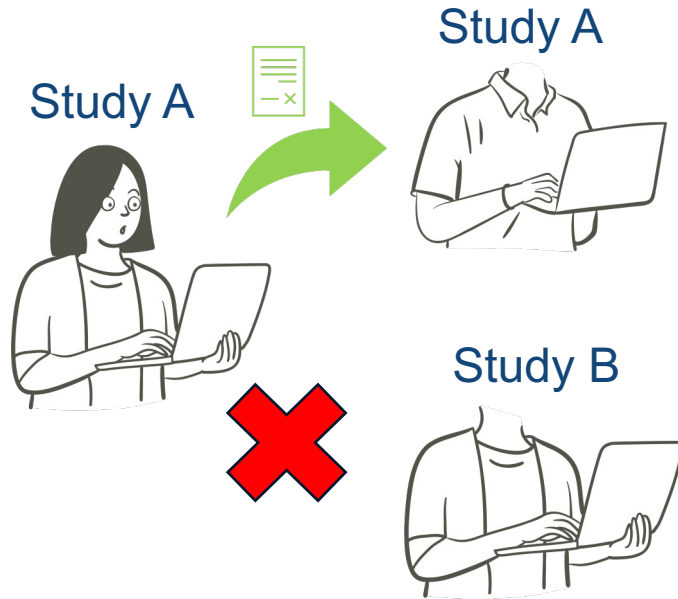
Study A

Study B

- ➢ Study-Specific Selection
  - ✓ Users can only see and select individuals assigned to the same study

- ➢ Invisible Protection
  - ✓ Unauthorized recipients don't appear as selectable options

No risk in incorrect document distribution

2.3 Controlled Document Sharing & Seamless User Transitions

User Management Challenges: Transfer Between **Departments**

Old Group

New Group

✔️ Access to Blinded Documents

1. Ownership of blinded documents reassigned
2. Change user profile

✔️ Access to Old Blinded Documents
❌ No access to higher versions of these documents

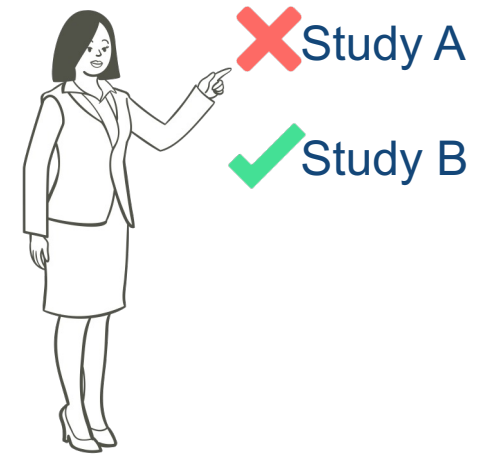No improper access retention after department changes

2.3 Controlled Document Sharing & Seamless User Transitions

User Management Challenges: Transfer Between Organizations

Old Organization

New Organization


✔️ Study A

❌ Study A

✔️ Study B

1. Access fully revoked
2. Creation of new login credentials

No improper access retention after organization changes
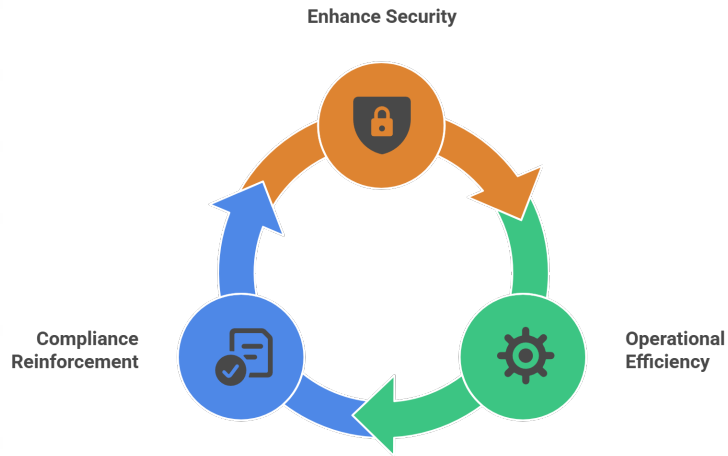
2.4 Yearly User Account Revision Process

Maintaining System Integrity Through Annual Review

➢ User Assessment Distribution
  - ✓ Complete user list provided to Line Managers and Project Managers
  - ✓ Account details include last login date

➢ Stakeholder Evaluation
  - ✓ Line Managers and Project Managers review access requirements
  - ✓ Users identified for:
    - ✓ Continued access
    - ↻ Account updates
    - ✕ Access termination

➢ Implementation by Superusers
  - ✓ Superusers execute required actions

List Users

Evaluate Access Needs

Inactivate or Update Accounts
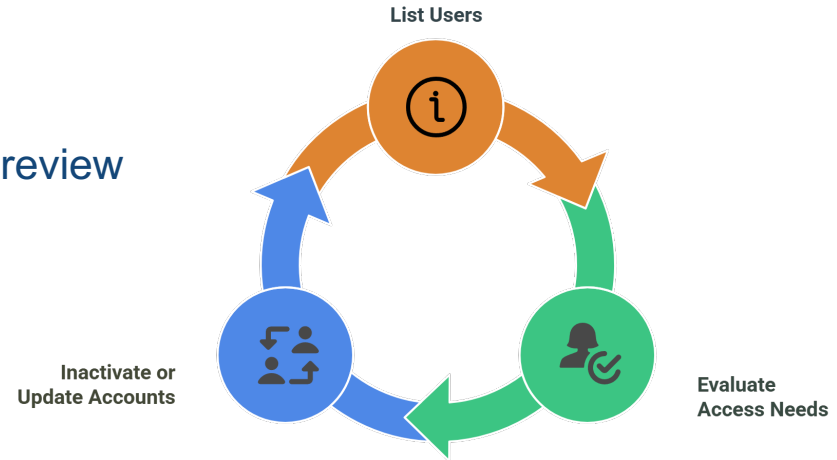
2.4 Yearly User Account Revision Process

Three Dimensions of Access Management Excellence

Enhance Security
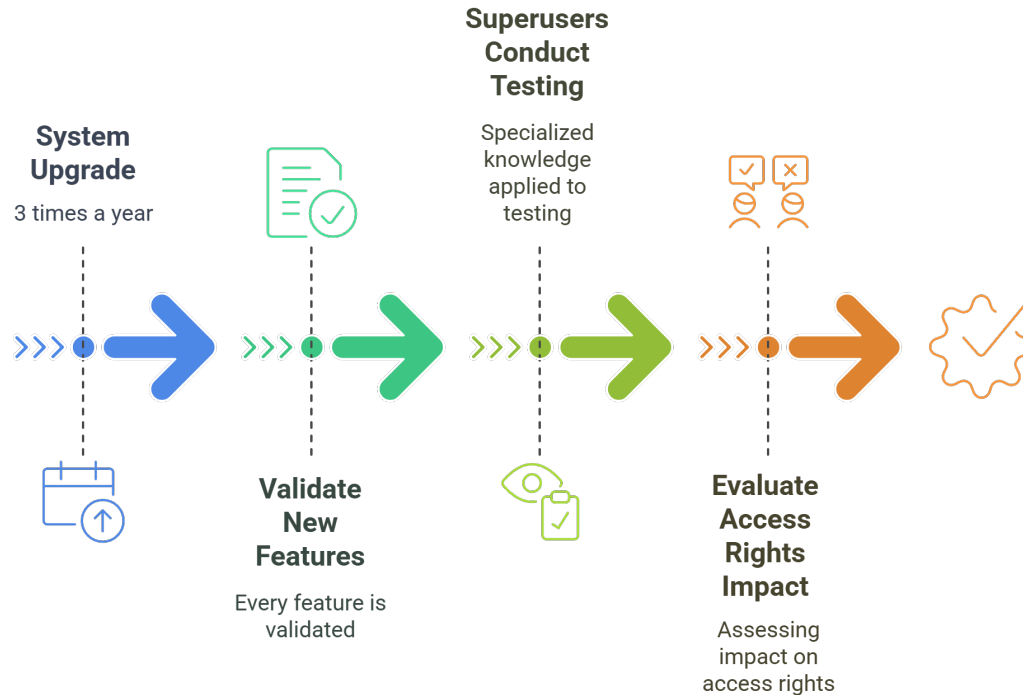
Compliance Reinforcement

Operational Efficiency

➤ Security Enhancement
  - ✓ Outdated accounts identified and removed
  - ✓ Access aligned with current responsibilities

➤ Operational Efficiency
  - ✓ System resources optimized
  - ✓ User database streamlined and up to date

➤ Compliance Reinforcement
  - ✓ Documented verification of all user accounts
  - ✓ Support for regulatory audit readiness

Annual review strengthens everyday access management

2.5 Triannual System Upgrades

System Upgrade and Access Rights Validation Process

System Upgrade

3 times a year

Validate New Features

Every feature is validated

Superusers Conduct Testing

Specialized knowledge applied to testing

Evaluate Access Rights Impact

Assessing impact on access rights

Security continuity preserved through structured validation

2.5 Triannual System Upgrades

Ensuring User Awareness & Access Verification

System-wide Update Notifications

Users are informed of new features and changes and a detailed documentation is provided

Communication Monitoring

Tracking of non-delivery messages to ensure communication reliability

Access Verification Process Initiated

Contacting LM/PM for user status confirmation

System Updated Based on Verification

Making system changes based on verification results

Robust communication ensures appropriate system access maintenance

3. Conclusions

Balancing Security and Flexibility in Client Solutions

SGS

Balancing Security and Flexibility in Client Solutions

High standard of security and compliance

Adaptability to Client-specific Requirements

No document ever ends up in the wrong hands, because juggling sensitive data is no casual task

Thank You!

Contact us

clinicalresearch@sgs.com

EUROPE: +32 15 27 32 45
AMERICAS: +1 877 677 2667

www.sgs.com/cro