Keeping Data Secure

Data capacity and CQI team
Mathematica

OFFICE OF FAMILY ASSISTANCE
An Office of the Administration for Children & Families

OPRE

HMRF
HEALTHY MARRIAGE & RESPONSIBLE FATHERHOOD

Mathematica
Progress Together

nFORM
Information, Family Outcomes, Reporting, and Management

This video will cover:

- nFORM security requirements
- Logging into nFORM
- Personally identifiable information (PII)
- Protecting client PII

nFORM security requirements

nFORM is a secure system

- **Compliant with federal security requirements**
  - nFORM's Authority to Operate does not allow direct data connections between nFORM and grant recipient systems
- **Grant recipients may only access the nFORM "production" environment**
  - Do not enter any test data or fake data
- **Data sharing agreements between Mathematica and each grant recipient document data security roles and requirements**

Secure access through user accounts

- User access defined by number of accounts for grant and account types
- User name is an email address; one account per email address
- Multifactor authentication: password + text or phone call
- Strong passwords (at least 8 characters, letters, numbers, special characters)

Keeping user accounts secure

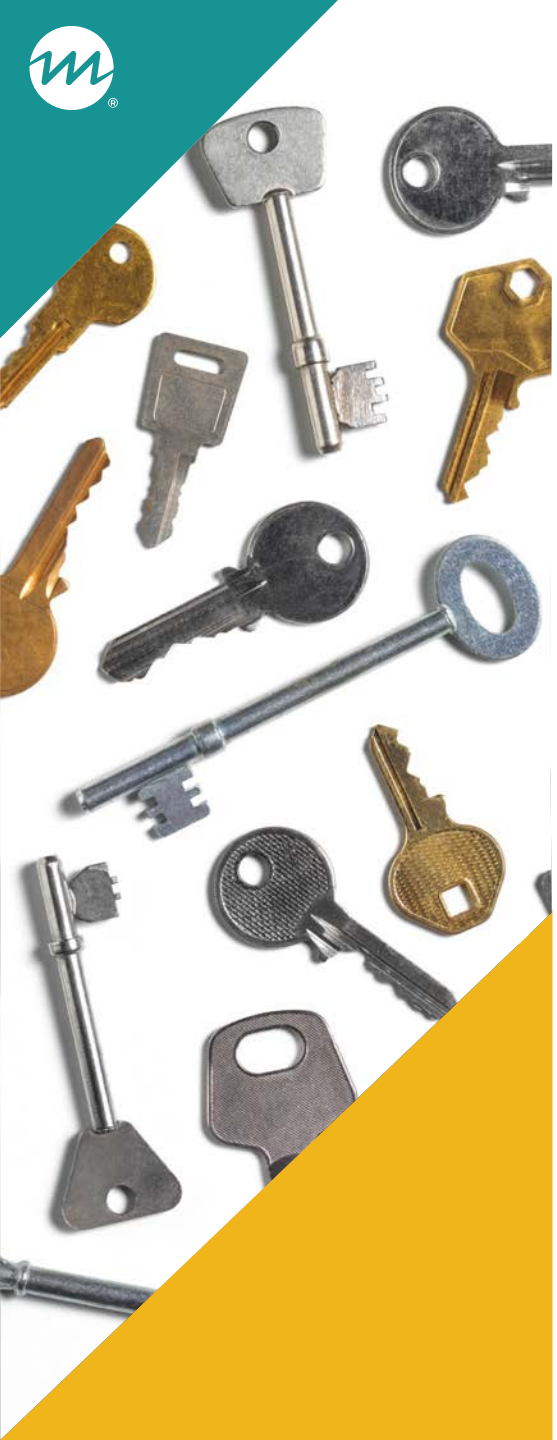
- **Must change password every 60 days**
- **Limited to 5 failed log-in attempts**
- **Must log in again after 15 minutes of inactivity**
  - A pop-up message will tell you when you have 1 minute left
  - Activity is saving information or navigating to a new page in nFORM
  - Typing, moving your cursor, and clicking a radio button, check box, or dropdown menu are not considered activity; you will be logged out if you type for more than 15 minutes without saving
- **Automatic deactivation after 60 days without logging in**
  - If not activated within 30 days, deactivated accounts are automatically locked

Logging into nFORM

Practices for protecting clients' privacy

Collecting PII in nFORM

- **Some nFORM data is considered PII**
  - Client names, contact information (address, phone numbers, email, social media information), birthdates, IPV screening, individual service notes, open-ended survey responses (such as youngest child's first name)
  - Other information, when linked to client name, may also be PII
- **Clients are also asked for sensitive information including whether they receive government benefits, and whether they are in jail or prison**

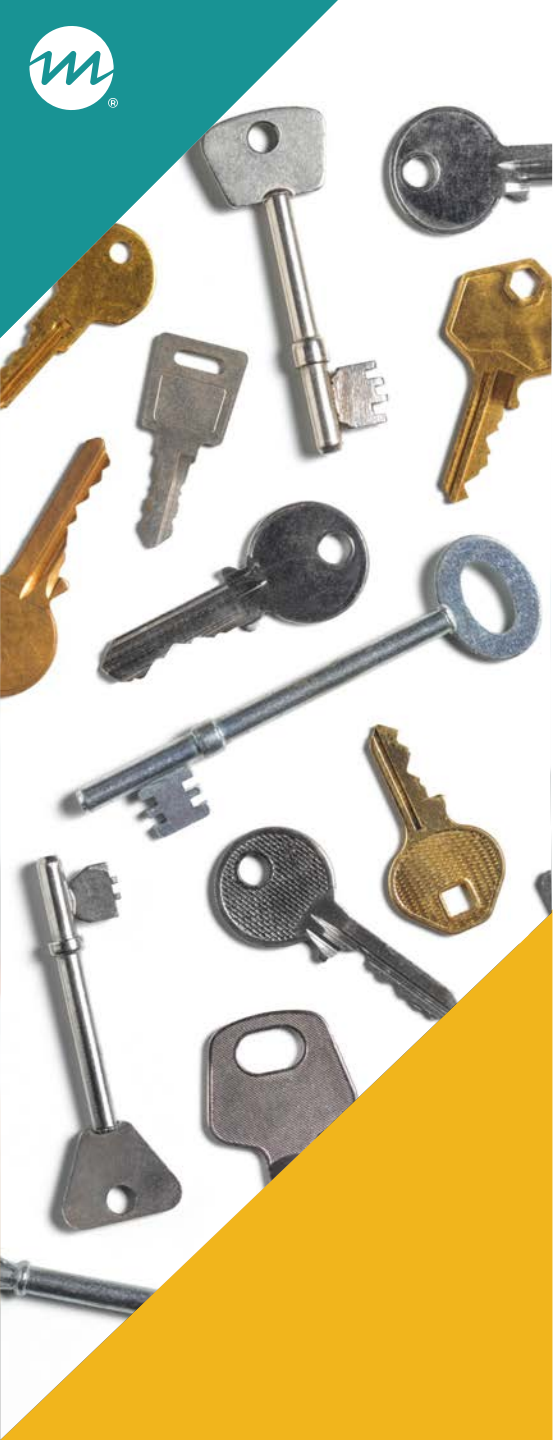


General practices for protecting clients' PII

Only refer to clients by their client ID numbers - never email PII, including to other program staff and the TTA help desk.

Keep discussions and phone calls about clients confidential and out of earshot of unauthorized people.

Make sure no one can see PII on your computer monitor, and lock your computer when you leave it. Keep your passwords secure and do not allow anyone to use your computer accounts.



General practices for protecting clients' PII (contd.)

Keep all project materials with PII locked when not in use. Never leave documents containing PII unattended on your own desk or in shared work spaces.

Securely shred hard copies of any paper surveys or other information when no longer needed.

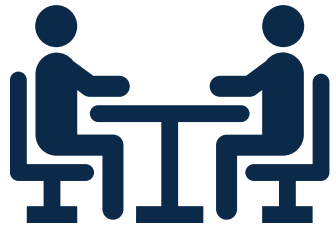
Do not save PII to any unencrypted device including shared network drives or flash drives.

Before data collection

- **Have dedicated, separate devices for grant staff to access nFORM and for clients to complete surveys**
  - Ensure all devices are locked when not in use
- **If your Family Assistance Program Specialist (FPS) approves use of paper surveys for your program, identify how you will securely transport, administer, store and ultimately destroy the paper surveys to protect client confidentiality**

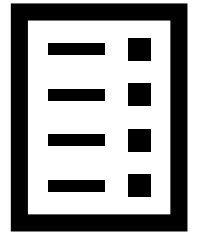
During data collection

- **Share ACF's Privacy Act Statement with clients so they are aware of how their data will be used and kept safe**
  - Provide access to ACF's Privacy Act Statement on HMRF Grant Resource site during outreach and recruitment
  - When completing the application form during enrollment
  - Before clients begin each web survey
- **A PDF of ACF's Privacy Act Statement is available in English and Spanish on the HMRF Grant Resource site**

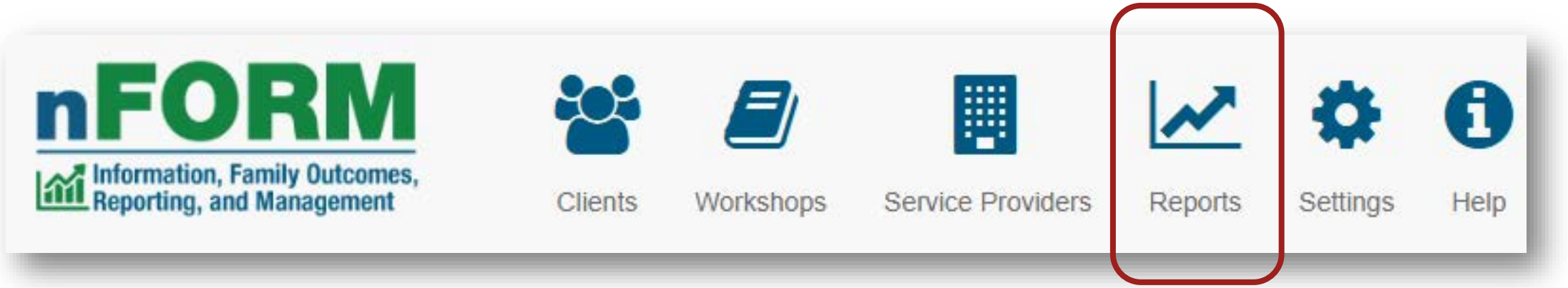


During survey administration

- **For in person data collection, provide adequate space to ensure clients have privacy when completing surveys**
  - If administering web or paper surveys to a group of clients, ensure that hard copies of survey login sheets and completed paper surveys are collected and securely shredded when no longer needed
- **Follow the ACF-approved methods to administer surveys to clients remotely**
  - Review the tip sheet on Options for Virtual Survey Administration for approved practices



Monitoring data collection



Keep client confidentiality in mind as you use nFORM's data tools and reports

- Only people who need access should be given access
- Never email reports, or any other materials, that include client names or other PII
- Only refer to clients by their client ID
- Be mindful of who can view your screen

Addressing security incidents

- **Grant staff should immediately report suspected or confirmed PII-related security incidents to their site administrator**
- **Site administrators should immediately report the issue to Mathematica by contacting the help desk at nFORMCQITA@mathematica-mpr.com**
  - Include only the Client IDs in the ticket; never include client name or other PII
- **Grant recipients must also comply with their IRB or research board's requirements**

Learn more about PII

- Review Module I of the nFORM User Manual for additional details about protecting PII
- Contact the data capacity and CQI help desk with any questions at nFORMCQITA@mathematica-mpr.com

Thank you!