



National Practitioner Data Bank-Healthcare Integrity and Protection Data Bank (NPDB-HIPDB)

Integrated Querying and Reporting Service (IQRS) User Review Panel (URP)

Sandy Rosenblatt

October 19, 2004



Fall 2004 IQRS URP

IQRS Security

(Sandy Rosenblatt)



IQRS Security

- Recent Security Enhancements
- Spring 2005 Security Enhancements
- Security Is Everyone's Responsibility



IQRS Security

Recent Security Enhancements

- Customer Service Center Password Restrictions
- Enhanced Authentication Procedures
- IQRS Security Notice



IQRS Security

Recent Security Enhancements - Password Restrictions

- Passwords Cannot Be Viewed By Customer Service Center
 - Administrator calls Customer Service Center to reset password
 - System generated password is displayed on the Customer Service Center screen
 - Administrator must create a new password immediately after logging on to the IQRS
 - Passwords are not displayed on the Entity Profile Screen
- Benefits
 - Administrator maintains confidential password
 - Maintains integrity of data



IQRS Security

Recent Security Enhancements - Enhanced Authentication Procedures

- Password Reset
 - Administrator calls Customer Service Center to reset password
 - To verify caller's identity:
 - Administrator's name must be on the Entity Profile or
 - Require a faxed authorization on company letterhead from the Certifying Official
 - Instruct caller to update User Account with the correct Administrator information
- Benefits
 - Stronger authentication process
 - Accurate information stored on Entity Profile



IQRS Security

Recent Security Enhancements - IQRS Security Notice

- Available from the Entity and Agent Registration Confirmation Screens
- Points to the July 2004 Newsletter “Ensure IQRS Security”
 - Data Bank Confidentiality
 - Entity Administrator Responsibilities
 - Passwords
- Next scheduled update in Spring 2005
- Benefits
 - Important security information is always available



IQRS Security

Spring 2005 Security Enhancements

- Administrator Password Restrictions
- Customer Service Center Support
- Maintaining Stronger Passwords
- Password Expiration Rules



IQRS Security

Spring 2005 Security Enhancements - Password Restrictions

- Passwords Cannot Be Viewed By Administrator
 - User calls Administrator to reset password
 - System generated password is displayed on the Administrator's screen
 - User must create a new password immediately after logging on to the IQRS
 - Passwords are not displayed on any IQRS Screens
- Benefits
 - User maintains confidential password
 - Reduces risk of unauthorized use of User's password



IQRS Security

Spring 2005 Security Enhancements - Customer Service Center Support

- Extended Customer Service Center functions
 - Access to a view-only version of the IQRS
 - Enter entity's DBID and User ID
 - Walk through any process
 - Can not update data or submit queries or reports
- Benefits
 - Provide more assistance while maintaining security



IQRS Security

Spring 2005 Security Enhancements - Maintaining Stronger Passwords

- **Current Password Rules**
 - Must have 8 – 14 characters
 - Must have at least 1 alphabetic and 1 numeric character
 - Must be different from the previous 4 passwords
- **Additional Password Rules**
 - Must not be a word found in the dictionary
 - Must not be a common Data Bank phrase (NPDB, IQRS)
 - Must not be your User ID
 - Must not be a simplistic or systematic sequence (abc123)



IQRS Security

Spring 2005 Security Enhancements - Maintaining Stronger Passwords

- Password Tips
 - Use upper and lower case letters
 - Use special characters
 - Do not use personal information—your name, names of family members, entity name, birthdate...
- More tips to make a password easy to remember
 - Make up nonsense words that are pronounceable, such as “BingzIng3” or “zoRpgoRp11”
 - Combine two short words with a special character, such as “4Truck+in” or “my2Birds”
 - Pick a phrase and use the first letter of each word. For example, “Will It Rain Today” could produce “W+i+r+t?04”



IQRS Security

Spring 2005 Security Enhancements - Password Expiration Rules

- General Password**

Property	Current Value	New Value Spring 2005	New Value Comments
Password Expiration	180 calendar days	90 calendar days	Required to change password every 90 days.
Password Expiration Notice	5 calendar days	5 calendar days	Message is displayed 5 days prior to password expiration.
Grace Login Period	Indefinite	30 calendar days	Within 30 days after password expiration.



IQRS Security

Spring 2005 Security Enhancements - Password Expiration Rules

- New Entity Passwords**

Property	Current Value	New Value Spring 2005	New Value Comments
Password Expiration	180 calendar days	30 calendar days	To allow time for the Entity Registration Confirmation Document to reach the entity.
One Time Use	No	Yes	Password must be changed after first use.
Grace Login Period	Indefinite	None	No grace login after password expiration.



IQRS Security

Spring 2005 Security Enhancements - Password Expiration Rules

- Reset Passwords**

Property	Current Value	New Value Spring 2005	New Value Comments
Password Expiration	180 calendar days	3 calendar days	System generated password is valid for 3 calendar days.
One Time Use	Administrator: Yes User: No	Yes	Password must be changed after first use.
Grace Login Period	Indefinite	None	No grace login after password expiration.



IQRS Security

Security is Everyone's Responsibility

- Security Measures Discussed Today:
 - Password Restrictions
 - Enhanced Authentication Procedures
 - IQRS Security Notice
 - Customer Service Center Support
 - Maintaining Stronger Passwords
 - Password Expiration Rules
- Security Measures for every day use:
 - Never write down password, remember it
 - Log out of the IQRS at the end of your session
 - Verify the date and time when your account was last accessed
 - Do not share Data Bank reports
 - Securely store or shred Data Bank Reports



Fall 2004 IQRS URP

Questions / Comments