QualityNet *e*Xchange

William A. Matos
Director, Division of Systems Architecture and Data Management
Information Systems Group
Office of Clinical Standards & Quality
Centers for Medicare and Medicaid Services

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

HCQIP
MEDICARE'S HEALTH CARE QUALITY IMPROVEMENT PROGRAM

Overview

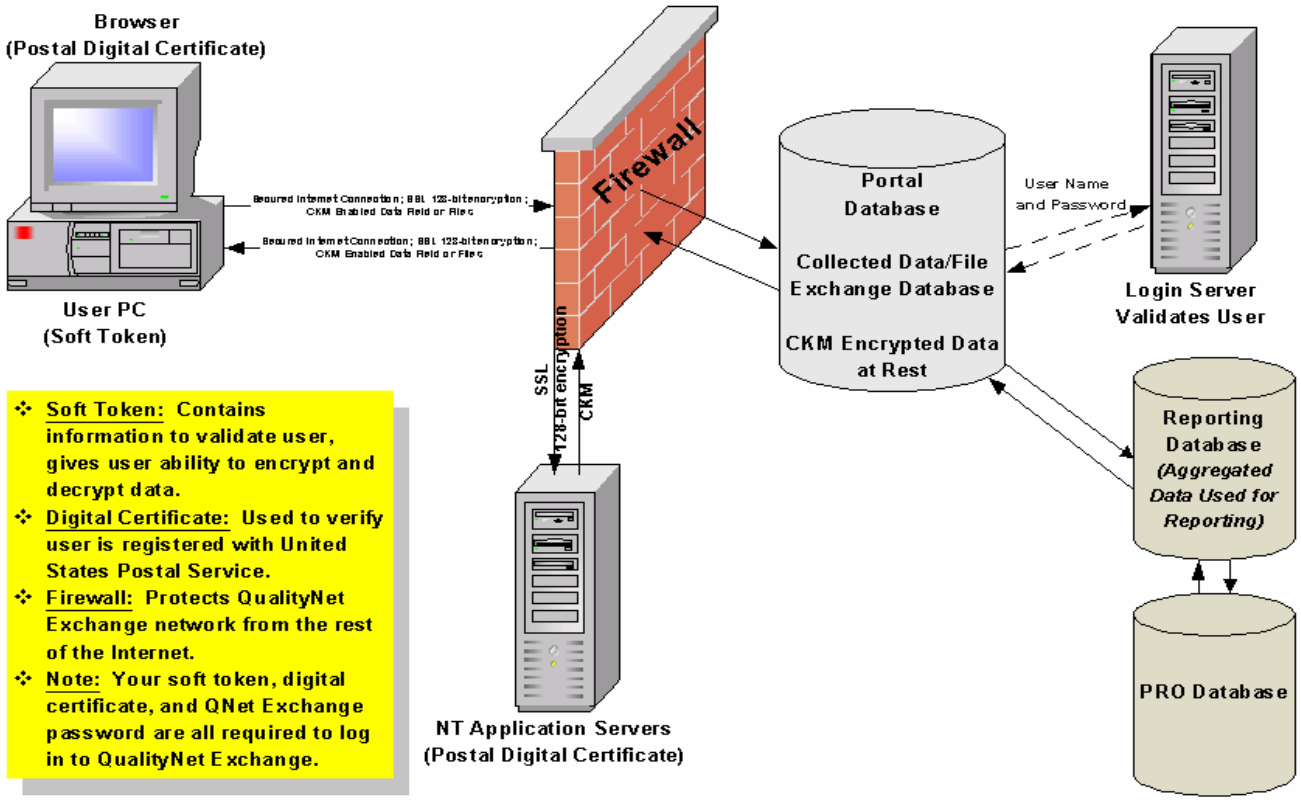
- What is it
- Security Features
- Registration
- Authentication
- Clinical Warehouse
  - Data Collection
  - File Exchange
- Information Dissemination
- Future Changes

QualityNet *e*Xchange

- Secure Internet web applications
- Internet portal for hospitals and other providers to report and exchange privacy and QIO sensitive data securely with QIOs
- Internet portal for ESRD facilities to report and exchange privacy and confidential data securely with CMS and ESRD Networks
- Digital signatures of CMS forms

QualityNet *e*Xchange

QualityNet *e*Xchange



PKI,CKM, and Oracle

- US Postal is currently providing certificate authority, registration authority, certificate distribution, and in-person-proofing
- TecSec CKM has been integrated into the QualityNet web applications for authentication and data encryption
- Oracle database roles along with CKM credentials are used to limit both access and the ability to decrypt data at rest

Security Features- Identifying Users

- Digital Certificate – Issued by the USPS
- Used to identify the computer to the QNet server
- Digital signatures

- User Token
- Tiny, safeguarded file
- Password protected
- User information - Credentials

Registration to QualityNet *e*Xchange

- Currently two separate processes
  - Registration to US Postal website where private and public keys are distributed to individual users along with in-person-proofing at local Post Office
  - Registration to QualityNet Exchange site where designated administrators sign-off on users for access and roles

Authentication to QualityNet *e*Xchange

- Users must have these components for authentication to QualityNet Exchange
  - US Postal x509 certificate for bi-directional (verification of user and web server) 128 bit SSL to QualityNet Exchange
  - Pass the Certification Revocation List (CRL)
  - CKM token
  - QualityNet Exchange Database ID
- Users login into QualityNet Exchange web application that seamlessly verifies all security components through a single sign-on

Clinical Warehouse - Data Flow

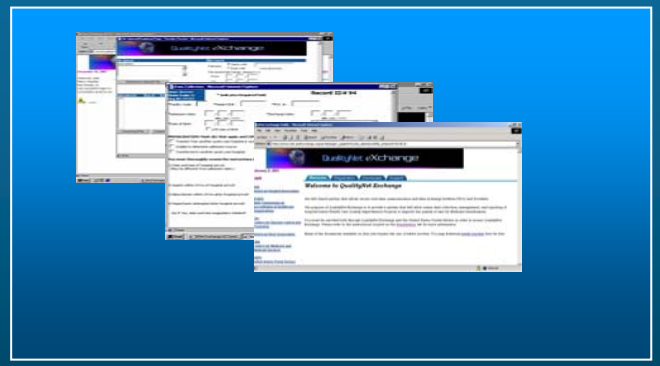
QIOs

Providers

Vendors

CDACs

Data



QIO Clinical Warehouse

Clinical Warehouse - Data Flow

Information

QIOs

- Clinical indicators
- Provider specific
- State aggregates
- Quality improvement reports

QIO Clinical Warehouse

Information

Providers

- Comparisons to state and national norms
- Immediate feedback reports

Information

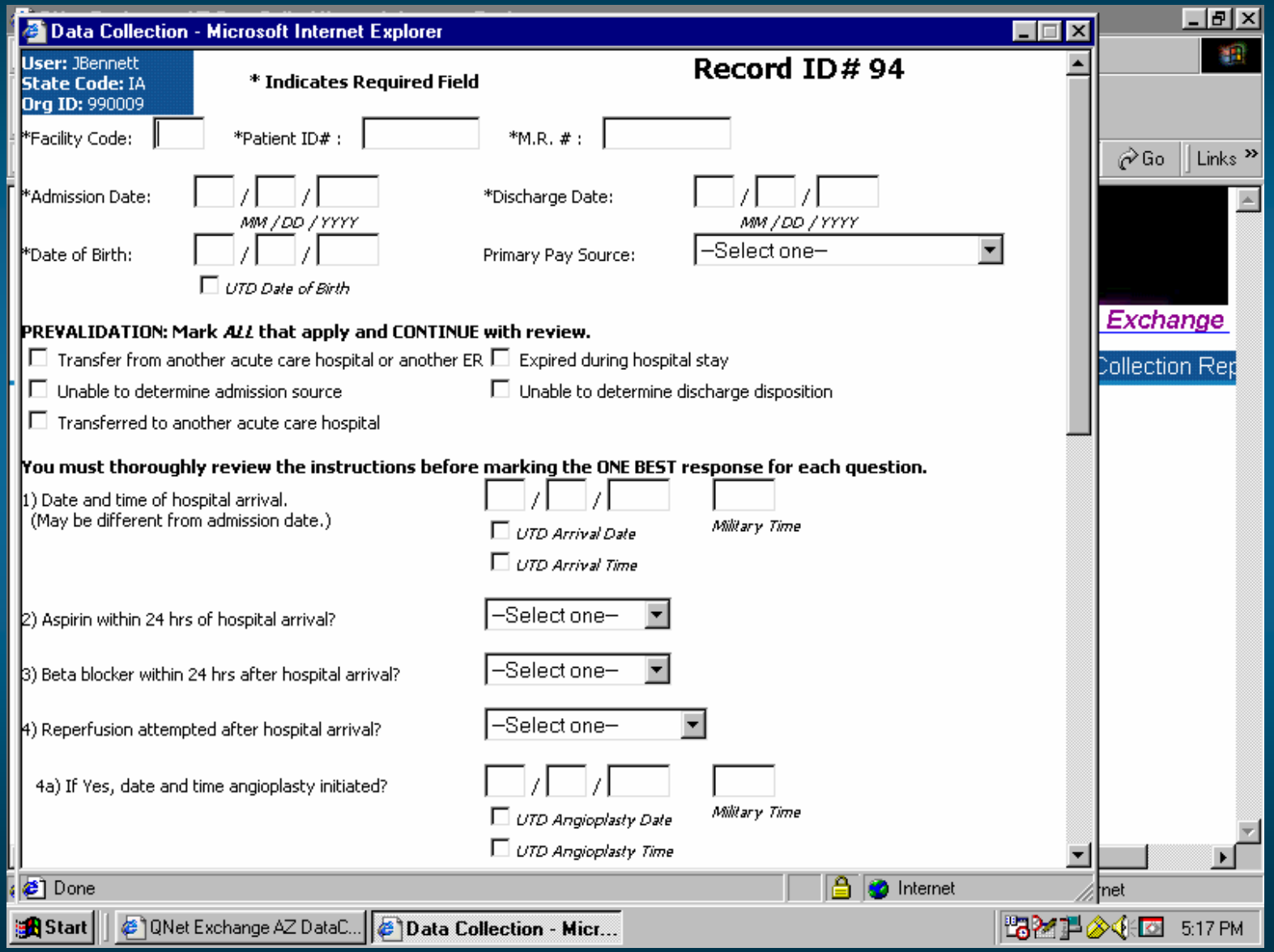
CMS

- Aggregate reports
- State & national indicators

Data Collection

- Abstraction tools
- File import according to specifications

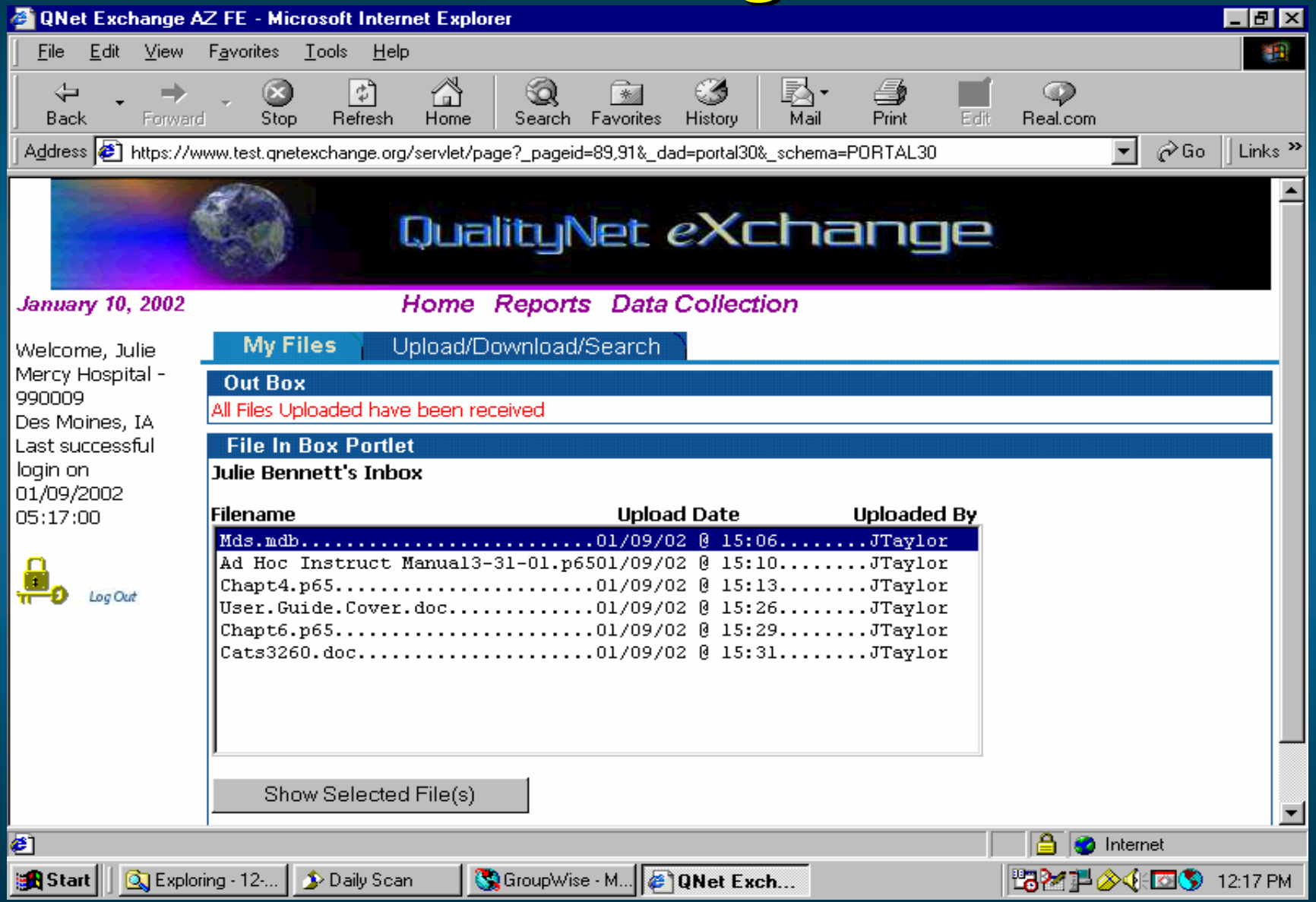
Online Data Collection



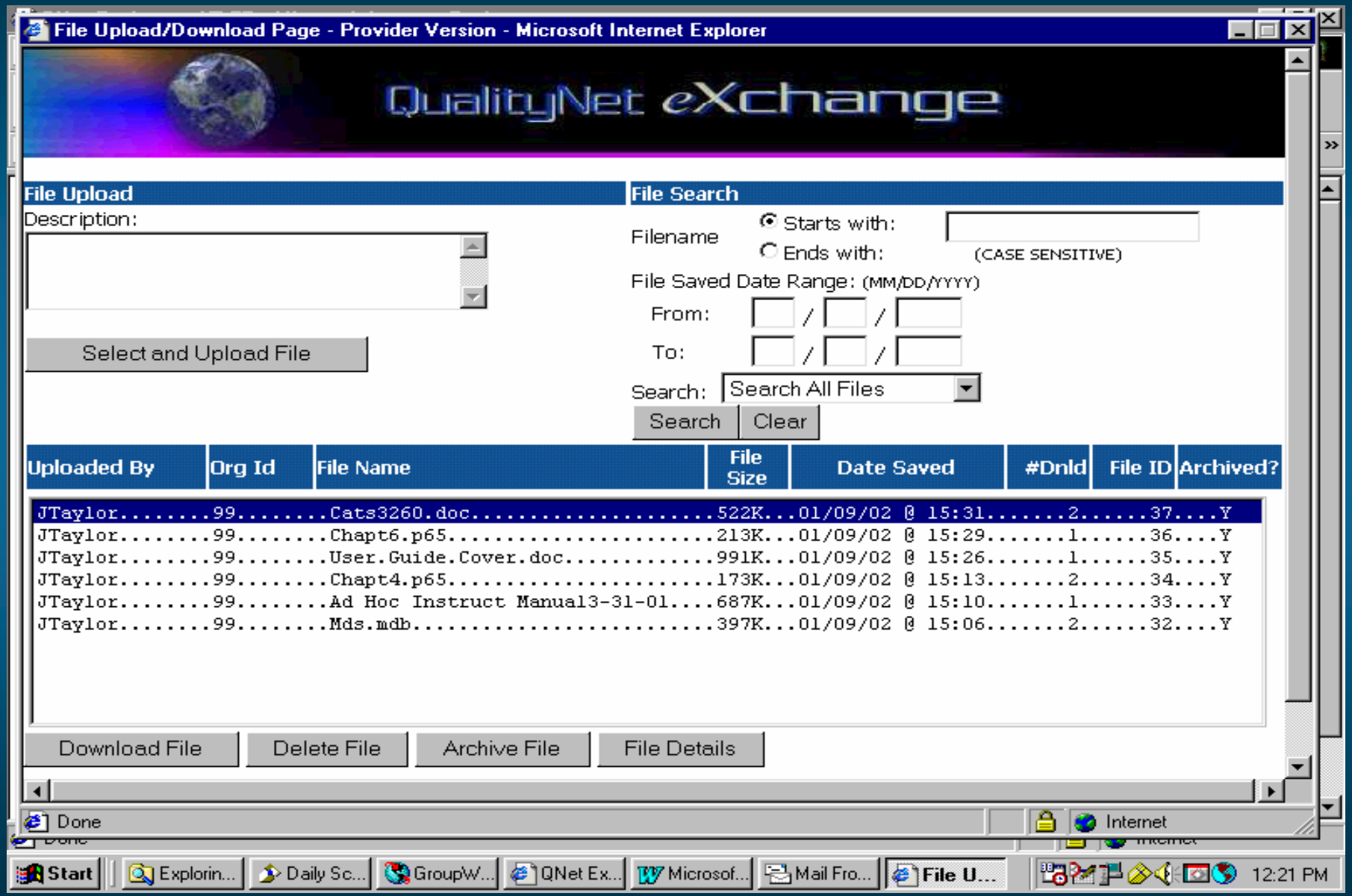
Functionality - File Exchange

- Secure distribution channel for any file
- Safe transfer of confidential or private data
- Encryption is transparent to users
- Files are encrypted at rest
- Monitoring activity in real-time by user (who, what, when and how often)

File Exchange Screen



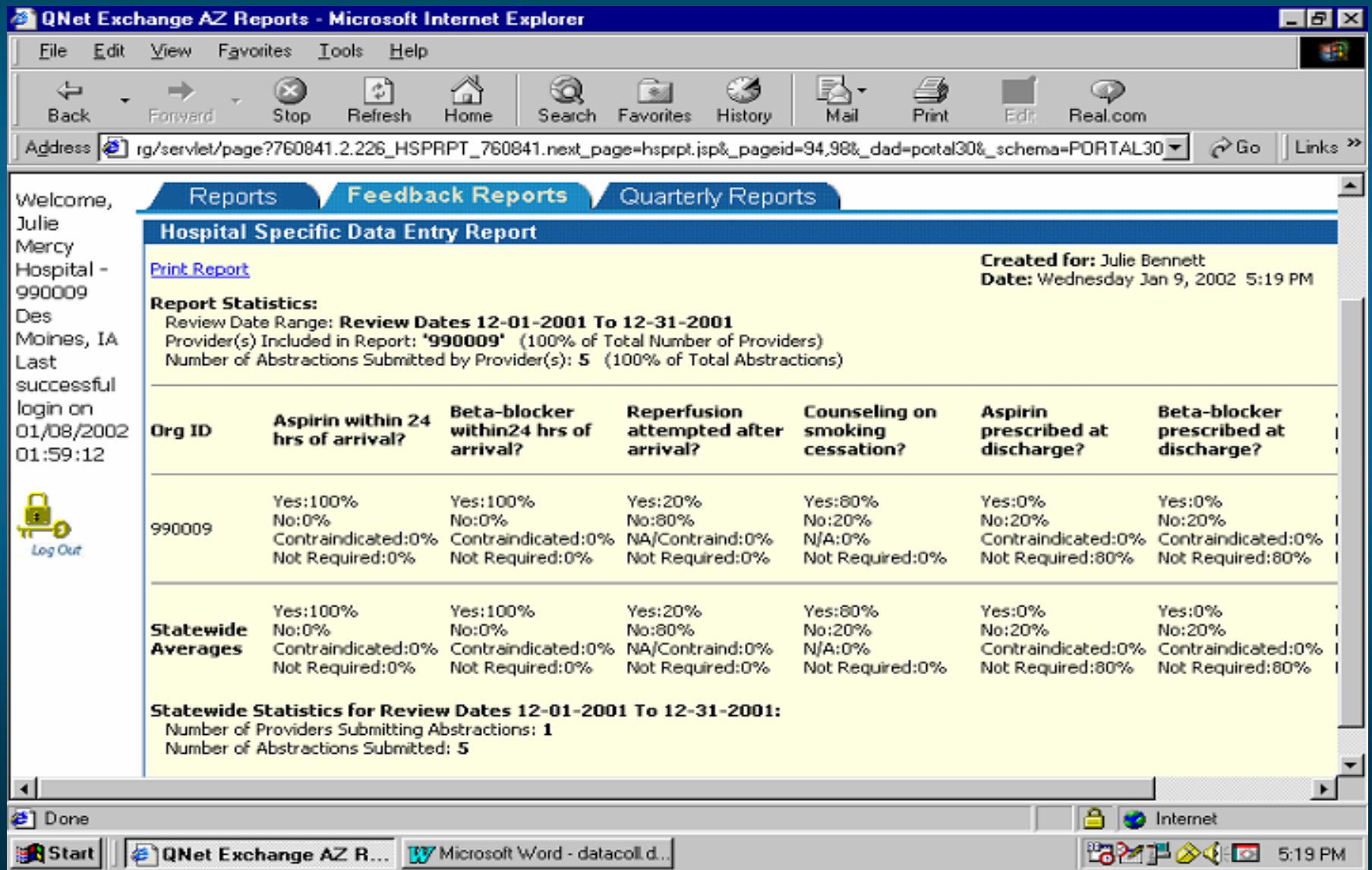
File Exchange Screen



Information Dissemination

- Immediate feedback reports
- Aggregate data reports
- Aggregate reports posted by QIOs
- Quality improvement progress by providers

Feedback Reports



QualityNet *e*Xchange Future Changes

- Single registration for everything through QualityNet Exchange web site
- QualityNet Exchange will pass required information to US Postal for certificate creation
- US Postal will still provide in-person-proofing at local post office
- QualityNet Exchange will manage distribution of US Postal Certificates by merging onto CKM tokens prior to delivery

QualityNet *e*Xchange Future Changes

- IFMC will fully automate the process for sign-off of users and distribution of tokens with US Postal certificates on them
- Users will only need to call IFMC QualityNet Exchange Help Desk for support questions