

Appendix F

Media Encryption

[Media Security and Encrypted DICOM CDs](#) are of interest to many organizations as patient privacy issues have become a major concern. These concerns have forced a number of organizations, such as the UK's NHS (National Health Services), to mandate encryption on removable media. Although many of these organizations have differing ideas on how to implement encryption, DatCard has chosen to implement AES 256-bit (Advanced Encryption Security) encryption throughout its suite of products. AES-256 is an encryption standard currently being considered for use by DICOM. Although other types of encryption may be as secure as AES-256, DatCard believes this standard will be the final choice of the committee based on its ease of use and implementation. AES encryption allows discs to be decrypted without loading specialized software on the receiving computer. When a user attempts to open an encrypted disc, they will be prompted to enter a password. If the password is supplied correctly, the viewer will automatically decrypt the images and display them without loading any additional software. This is in contrast to many other methods of disc encryption, which require the loading of proprietary software on a PC by someone with administrative user privileges.

Password Protection

The patient privacy that is provided by encryption can only be as strong as the chosen password. Each organization seems to have their own ideas on passwords: some believe that all passwords should be long and complex to improve protection, while others are more concerned about usability and ease of administration and therefore choose passwords that are well-known and memorable. DatCard Systems encourages organizations to establish good security policies that best fit their practice of medicine and business for the exchange of medical information. Organizations must also address the concerns of lost or incompletely transmitted passwords, patient physician referrals, and emergency access of discs in life-threatening situations.

PacsCube's Media Encryption

- The PacsCube suite provides standardized encryption throughout its suite of products. The process encrypts all pieces of Patient Health Information (PHI) to include results and is selectable by the user allowing the facility to create both encrypted and unencrypted pieces of media to suit the organization's needs. In addition, password generation is configurable to meet the unique security requirements of each organization. Finally, the PacsCube provides a password management system to help with lost passwords and also supports ION Medical HIVE (Healthcare Information

Verification and Encryption), a web-based password escrow and authentication service for remote authorized access to discs without passwords.

The following encryption features are available:

- AutoBurn – offers profile-driven encryption and password generation.
- AutoBatch – offers batch level encryption and password generation.
- iRecall – offers users encryption and password generation.
- Password Management – offers:
 - Printing of passwords by Media ID
 - Emailing of passwords by Media ID
 - Password retrieval by Media ID
 - Password retrieval by HIVE registration ID
- DCS Media Import – When the media importer encounters an AES-encrypted piece of media, the importer will prompt for a password and decrypt the images so that they may be imported into PACS.
- DCS DICOM Viewer – Encrypted pieces of media will prompt for a password and provide access to ION Medical HIVE for remote authorized access to discs without passwords.



Note – Password generation is unique to each CD/DVD job, therefore if a job spans multiple pieces of media each piece of media will have the same password for ease of use.