



SDFI

Secure Digital
Forensic Imaging

Secure Beyond Reasonable Doubt®

SDFI-TeleMedicine Security

A Summary of the Five Compounded Levels of SDFI Security

SDFI-TeleMedicine security is compounded fivefold making the SDFI-TeleMedicine system **Secure Beyond Reasonable Doubt®**. It is unlikely that images managed by the SDFI-TeleMedicine system could ever be tampered with.

The defined process file encoding and intricate level of advanced encryption prevent tampering at many levels:

- The first element of security is defined by a specific storyboard of overlapping images. A picture is taken from a wide angle, allowing the subject matter to *fill the screen*. That picture is supported by additional pictures incorporating closer views each captured approximately 50% closer than the last picture taken.
http://www.sdfi.com/downloads/SDFI_Digital_Protocol.pdf
- The second element of security is in the SDFI Camera System. The camera system stores data in RAW format. RAW is a non-destructive file format which means the original data will always remain unchanged thereby precluding modification or alteration.
- The third element of security is the high level data encryption used and supported by the use of long passphrases. AES 256-bit encryption is utilized to ensure digital evidence is protected from access and alteration.
- The fourth element of security addresses physical safekeeping of the forensic data managed by the SDFI-TeleMedicine System. Users are expected to keep a secure backup copy of the secured forensic data, preferably off-site away from your corporate network. (NOTE: SDFI Forensic Data is independently secured and cannot be viewed by I.T. personnel ensuring Chain of Custody).
- The fifth element of security is triple layer encryption that is used when sending forensic evidence. Independent AES 256-bit encryption over a SSL certificate signature algorithm set at PKCS #1 SHA-256 with RSA encryption and temporarily resting on self-encrypting hard drives are used to ensure no one, including SDFI and/or an internet service provider can access or view SDFI Secure Case Files.
http://www.sdfi.com/downloads/SDFI_File_Portal_Security.pdf



SDFI

Secure Digital
Forensic Imaging

Secure Beyond Reasonable Doubt®

Fourth Element of Security

The fourth element of security addresses the physical safekeeping of the digital evidence. Image files along with other related digital data can be stored on hi-capacity NTFS external hard drives or on your corporate network. NOTE: SDFI strongly recommends storing forensic data on your corporate network. Data stored on a corporate network remains encrypted to AES 256-bit standards. This exercise keeps the data safe from harm (e.g. computer crash, viruses, theft).

Your organization is solely responsible for the regular backup of your data and the physical protection of your data storage devices.

Fifth Element of Security

The fifth element of security is a combination of layers of encryption algorithms used when transferring images via the Internet. Both AES 256-bit and a SSL connection with PKCS #1 SHA-256 with RSA encryption are used independently to prevent access or viewing of digital evidence, including access by SDFI or internet service providers. SDFI Secure Files only rest temporarily on self-encrypting hard drive devices that are separately encrypted with AES 256-bit ciphers.

Upon request, the SDFI System User accesses the local or networked AES 256-bit encrypted secure work area containing the digital evidence. The specific individual's folder is selected and independently encrypted with AES-256 bit encryption. A separate independent long passphrase is used, made up on the spot, for each SDFI-TeleMedicine Secure Case File sent out. This independent self-decrypting SDFI-TeleMedicine Secure File prevents anyone from knowing about, viewing or tampering with the encrypted image data inside. Not even your own organization's I.T. personnel, SDFI or an internet service provider could know what is contained in the SDFI-TeleMedicine Secure Case File.

The first encryption algorithm protects the forensic data inside the SDFI-TeleMedicine Secure File. A second and completely separate PKCS #1 SHA-256 with RSA encryption algorithm is activated when a user accesses the SDFI File Transfer Portal through the SDFI web site. The process makes SDFI-TeleMedicine "Secure Beyond Reasonable Doubt®".



SDFI

Secure Digital
Forensic Imaging

Secure Beyond Reasonable Doubt®

The SDFI-TeleMedicine Workflow Process

Digital images are captured in a storyboard sequence by our SDFI high resolution macro camera system. This system is pre-configured to store images in RAW format and JPG format on a high capacity memory card. The captured RAW/JPG files are transferred from the camera to a Windows XP/Vista/7 computer via a USB 3.0 card reader that we supply. Memory cards are used as a temporary method of transferring pictures from the camera the computer. Memory cards are continually erased, formatted and reused. If required, memory cards can be wiped to Department of Defense standards with SDFI-TeleMedicine security software.

The RAW/JPG files are uniquely renamed while still on the memory card and then moved into a secure encrypted computer hard drive. This hard drive is backed-up to either a protected external drive or corporate network. Network storage is strongly recommended. Upon demand, a copy of the individual's folder is separately encrypted to AES-256 within the already encrypted AES-256-bit computer environment. It is then uploaded through a SSL connection set at PKCS #1 SHA-256 with RSA encryption and onto a protected Isilon server.

A notification e-mail containing a hyperlink is sent to the intended recipient from the protected server. NOTE: The sender acquires an e-mail address by contacting the recipient directly and asking for it. The SDFI-TeleMedicine Secure Case File can now be downloaded onto a Windows based computer by the recipient, but it cannot be decrypted/opened without the long passphrase. The unique passphrase must be communicated by telephone from the sender to the recipient before access to the SDFI TeleMedicine Secure Case File is granted.

This simple process makes SDFI-TeleMedicine Secure Beyond Reasonable Doubt®. After the unique passphrase is entered into the SDFI-TeleMedicine Secure File, a copy of the individual's folder is exported into a standard yellow computer folder on the recipient's Windows based computer, usually on the desktop. The recipient can then view the pictures. The recipient is now responsible for the downloaded unprotected folder. Both a RAW file and a JPG of each picture are sent to the recipient. The RAW file is used as proof that the image is valid, the JPG is for examination and presentation. RAW files are proprietary to the camera and the camera company. They cannot be changed.



Document Summary

SDFI-TeleMedicine is Secure Beyond Reasonable Doubt® and well beyond HIPAA security.² Our simplified process combined with five major compounded elements of advanced security supported by additional security measures, each wrapped around a defined business model ensures that SDFI-TeleMedicine digital forensic pictures es are kept safe and secure.

Your organization is solely responsible for the regular backup of your digital data and the physical protection of your data storage devices.

Please send technical questions to:

SDFI-TeleMedicine
ATTN: Technical Support
E-Mail: Support@SDFI.com
Phone: 310-492-7372

2. SDFI Reference Document: http://www.sdfi.com/downloads/hipaa/SDFI_Is_Beyond_HIPAA_Security.pdf