

# SDFI<sup>®</sup> - TeleMedicine

Secure Digital Forensic Imaging – Secure Beyond Reasonable Doubt<sup>®</sup>

## White Paper on SDFI<sup>®</sup> - TeleMedicine Advanced Security

**\* TECHNICAL REQUIREMENTS are on PAGE 3 & 4. \***

### Introduction

The electronic world is perhaps the greatest enabler any generation has ever seen. Innovations such as personal digital assistants, cell phones, satellites, e-mail, VoIP like Skype, texting and digital cameras have made us more efficient and given us unprecedented access to information. With the broad and open use of these digital technologies come issues of security and trust. Threats of image and document manipulation, eavesdropping and data theft have prevented many organizations from fully embracing the benefits of the electronic world. SDFI-TeleMedicine brings the trust and security of the physical world into the electronic world, so much so that SDFI-TeleMedicine is considered to be, “Secure Beyond Reasonable Doubt<sup>®</sup>!”

### Origins... A Brief History of SDFI-TeleMedicine

The desire to create a solution that could meet the specific needs of a Sexual Assault Forensic Nurse Examiner, FNE or SAFE began early in 2001. Extensive time was spent at SART centers in an effort to see and understand the requirements of the entire “Sexual Assault Response Team”. A business workflow “blueprint” was created during that time allowing for a clear understanding of both the actual internal workflow process and the overall business needs. An original copy of the results of each sexual assault exam is passed on to other agencies that thrive outside the examiner’s internal business model. Furthermore, there are multiple external agencies that are required to handle digital evidence, each with different roles and responsibilities.

To complicate the matter of security, any solution that might be offered would have to survive a Kelly-Frye hearing, The Daubert Test of Reliability, be beyond HIPAA<sup>(1)</sup> and the HI TECH Act, meet and/or exceed state and federal security standards, be non-proprietary and be designed to move gigabytes of digital data across existing Internet lines, securely, in a very simple and easy way.

After an extensive amount of time, money, effort along with years of research SDFI-TeleMedicine, the company, was conceived and designed to serve the clinical, medical and legal communities.

SDFI-TeleMedicine is being used at multiple medical locations throughout the United States and is used and supported by hundreds of Police Departments and District Attorneys offices.

<sup>(1)</sup> SDFI Reference Document: [http://www.sdfi.com/downloads/hipaa/SDFI\\_is\\_beyond\\_HIPAA\\_Security.pdf](http://www.sdfi.com/downloads/hipaa/SDFI_is_beyond_HIPAA_Security.pdf)

# SDFI<sup>®</sup> - TeleMedicine

Secure Digital Forensic Imaging – Secure Beyond Reasonable Doubt<sup>®</sup>

## Many Applications Are Enabled By SDFI-TeleMedicine

SDFI-TeleMedicine, being non-proprietary, lends itself to a multitude of industries and agencies including Clinical/Medical, Coroners & Medical Examiners, Law Enforcement, Fire Investigation, Wound Care, Risk Management, , SANE, SART and SAFE programs around the nation and around the world. This list is a small sampling of the areas that will take advantage of this secure and advanced photo documentation technology.

## The SART Business Workflow Process

SDFI-TeleMedicine technologies were designed to support and enhance existing business workflow procedures and processes, not challenge them. Forensic Nurse Examiners work in a unique environment given the subject matter and the nature of the job. FNE's must deal with living victims of sexual assault, rape and domestic violence. FNE's may also be required to examine alleged suspects.

Unlike a murder crime scene that can be held for forensic photographers, FNE's must take legal court ready digital pictures of living individuals. Evidence collection includes pictures of body cavities including oral and genital pictures. In some cases survivors have been violently sexually assaulted and violently beaten. This means that FNE's have a limited amount of time to collect and capture evidence that resides in and on the victim and/or on their clothes. The sensitive nature of these close-up pictures demand the highest level of security, beyond what is typically expected within the medical and forensic communities.

The digital evidence, specifically these kinds of graphic digital pictures, are moved from the camera's memory card and put into a secured computer within minutes of the examination. With SDFI-TeleMedicine, even the pictures on the camera's memory card are secure from manipulation.

The digital evidence files must be uniquely identified and then filed away until called upon by any one of many law enforcement agencies or district attorneys around the nation. If required, digital collected evidence can be sent to law enforcement within minutes after the exam is completed.

Now, with SDFI<sup>®</sup>-TeleMedicine, a Forensic Nurse Examiner is able send an almost unlimited amount of digital evidence to the police detective and/or to the prosecutor securely, almost instantly and directly via the Internet.

# SDFI<sup>®</sup> - TeleMedicine

Secure Digital Forensic Imaging – Secure Beyond Reasonable Doubt<sup>®</sup>

## **TECHNICAL REQUIREMENTS** **PAGE 3**

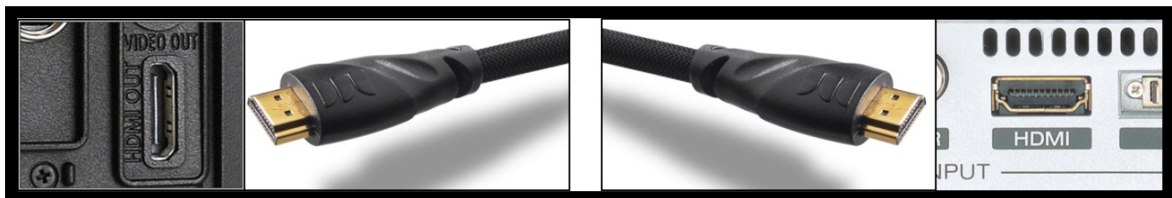
The main components are described below in the order that they are used in. **The SDFI<sup>®</sup> process is secure beyond HIPAA<sup>(1)</sup>.** (*SDFI users always supply their own computer, high speed internet and a fast response big screen HDMI compliant T.V.*) Users are solely responsible for the regular backup and ongoing protection of the data collected).

- ❖ Our Hi-Resolution Digital Camera(s) Capable Of Capturing RAW and JPG Files.
- ❖ Our Encryption Software Delivering AES 256-bit Encryption. **(SINGLE USER LICENSE)** (*This means ONE single Windows Username Windows Login*)
- ❖ Our Non-Destructive Image Management Software. **(SINGLE USER LICENSE)**
- ❖ **Full and Continuous “Local” Administrator Access on the Computer Being Used.**
- ❖ **One Unused and Unrestricted USB 2.0 Port with full Read/Write Access.**
- ❖ **Internet Access to ALL of: <http://www.SDFI.com> for system updates and information.**
- ❖ **Internet Access to ALL of: <https://fileportal.sdfi.com> for SDFI<sup>®</sup> File Portal access.**
- ❖ **Internet Access to ALL of: <https://www2.gotomeeting.com> for technical support.**
- ❖ **A Windows XP/Vista/7 Computer, Less 18 Months Old, With 750GB of Unused Network Storage Space. Space on a secured network is preferred. NOTE: The SDFI computer does NOT need to be located in the exam room. (Required - Not Supplied)**
- ❖ **IMPORTANT NOTE ABOUT HARD DRIVE DISK SPACE: The local hard drive, where the SDFI software will be installed and all network storage space used must NOT be compressed. SDFI software will NOT work in or on compressed hard drives.**
- ❖ **A High Speed Connection to the Internet. (Required - Not Supplied)**
- ❖ **A fast response 32” to 55” LCD, LED or Plasma Television with one unused and unrestricted HDMI connection port. A wall mounted unit with an extendable arm is recommended. (Required - Not Supplied)**

**SDFI Camera System**

**HDMI Cable**

**HDMI TV**



<sup>(1)</sup>. SDFI Reference Document: [http://www.sdfi.com/downloads/hipaa/SDFI\\_is\\_beyond\\_HIPAA\\_Security.pdf](http://www.sdfi.com/downloads/hipaa/SDFI_is_beyond_HIPAA_Security.pdf).

# SDFI<sup>®</sup> - TeleMedicine

Secure Digital Forensic Imaging – Secure Beyond Reasonable Doubt<sup>®</sup>

## **TECHNICAL REQUIREMENTS** **PAGE 4**

**IF YOU DO NOT HAVE ACCESS AS SHOWN BELOW, YOU CAN'T DO YOUR JOB**

All users MUST be able to receive e-mail notifications from:

**Support@SDFI.com**

Contact your I.T. department for help. If they don't understand, have them call SDFI<sup>®</sup> and we will help.

**IF YOU DO NOT HAVE ACCESS AS SHOWN ABOVE, YOU CAN'T DO YOUR JOB**

Through SDFI<sup>®</sup> -TeleMedicine, digital forensic evidence is **NEVER** sent via e-mail or an e-mail attachment.

SDFI<sup>®</sup> uses an ultra-secure process as simple as: “Click, Save and Call”.

First, users receive a **NOTIFICATION ONLY** e-mail message from: **Support@SDFI.com**

Second, users will “**CLICK**” on the link inside the notification e-mail (It will take you directly to: **HTTPS://FILEPORTAL.SDFI.COM**).

Third, users will “**SAVE**” the SDFI<sup>®</sup> Secure File on your computer (NOTE: You can choose where you want to save the SDFI<sup>®</sup> Secure File).

Fourth, users will pick up the phone and “**CALL**” the person who sent the notification and the SDFI<sup>®</sup> Secure File to you and ask for the SDFI<sup>®</sup> Secure File Passphrase (The sender's e-mail address will be in the notification e-mail message.)

# SDFI<sup>®</sup> - TeleMedicine

Secure Digital Forensic Imaging – Secure Beyond Reasonable Doubt<sup>®</sup>

## The “SDFI-TeleMedicine” Workflow Process

A high capacity 8GB or higher storage memory card is used to initially store the digital pictures.

Memory cards are used as a temporary method of transferring pictures from the camera into a computer. (Memory cards are continually erased, formatted and reused every day. They can be wiped to D.O.D. standards with SDFI-TeleMedicine security software if required.)

Digital pictures are captured by our high resolution macro camera system that is pre-configured to capture in RAW format and JPG format.

The RAW/JPG files are transferred from the camera to a Windows XP/Vista/7 computer via memory cards and a memory card reader that we supply.

The RAW/JPG files are uniquely renamed while still on the memory card and then moved into a secure encrypted computer hard drive and backed-up to either a protected external drive or the network. Network storage is strongly recommended!

Upon demand, a copy of the individual’s forensic folder is separately encrypted to AES-256 within the already encrypted AES-256-bit computer environment. It is then uploaded through a SSL set at SHA-1+RSA 2048-bit encryption and onto a protected Internet server. A notification “e-mail hyperlink” is sent forth to the detective and/or the prosecutor from the protected server. NOTE: The Forensic Nurse Examiner acquires an e-mail address by contacting the recipient directly by phone and asking for it.

The “SDFI-TeleMedicine Secure File” can now be downloaded onto a Windows computer by the recipient, **but NOT opened** by the recipient without a long passphrase. The unique passphrase must be communicated by telephone to the recipient before access to the SDFI-TeleMedicine Secure File is granted. This simple process makes SDFI-TeleMedicine exceptionally “Secure Beyond Reasonable Doubt”<sup>®</sup>.

After the unique passphrase is entered into the SDFI-TeleMedicine Secure File, a copy of the individual’s forensic folder is exported into a standard “yellow computer folder” on the recipient’s Windows computer, usually on the desktop. The recipient can then view the pictures. (The unprotected pictures can now be stored elsewhere, in or on any storage system.) Both a RAW and a JPG of each picture are sent to the recipient. The RAW file is used as proof that the image is valid, the JPEG is for examination and presentation. The recipient cannot change the RAW files. RAW files are proprietary to the camera and the camera company. They cannot be changed.

# SDFI<sup>®</sup> - TeleMedicine

Secure Digital Forensic Imaging – Secure Beyond Reasonable Doubt<sup>®</sup>

## The Five Compounded Levels of “SDFI<sup>®</sup>” Security

SDFI-TeleMedicine security is compounded fivefold making SDFI-TeleMedicine “**Secure Beyond Reasonable Doubt**”<sup>®</sup>. It is unlikely and unreasonable that the digital picture evidence handled by the SDFI-TeleMedicine system could ever be tampered with. The defined process and the intricate level of advanced encryption and encoding prevent tampering at many levels. *(A number of additional security measures are not listed for security reasons.)*

- ❖ The first element of security is defined by a specific storyboard of pictures. A picture is taken from a wide angle, allowing the subject matter to “fill the screen”. That picture is supported by a number of closer views/magnifications; each captured approximately 50% closer than the last picture taken. (Please refer to the SDFI Forensic Photography: Digital Protocol. It can be downloaded from the [www.SDFI.com](http://www.SDFI.com) web site).
- ❖ The second element of security is in the camera system. The camera system captures RAW files. RAW files are “camera model specific” to the digital camera’s photo sensor and are specifically encoded making changes realistically impossible.
- ❖ The third element of security is high level data encryption on the computer. AES 256-bit encryption is utilized to ensure the digital evidence is protected from access, examination and alteration.
- ❖ The fourth element of security addresses the physical safekeeping of the digital pictures. **Users are expected to keep a secure backup copy of the digital evidence stored on a high-capacity, high speed external hard drive or on a corporate network.** (NOTE: SDFI forensic data is independently secured and cannot be viewed by I.T. personnel).
- ❖ The fifth element of security is a double layer of encryption that is used when sending data over the Internet. Both AES-256 bit and SHA-1+ RSA 2048-bit encryption is used independently to ensure that even an internet service provider cannot access or examine the forensic data files.

The remaining pages of this document break down and explain each of the five elemental security protocols including some of the additional security protocols that are in place.

A list of benefits related to the use the SDFI-TeleMedicine File Portal is included.

# SDFI<sup>®</sup> - TeleMedicine

Secure Digital Forensic Imaging – Secure Beyond Reasonable Doubt<sup>®</sup>

## The Five Compounded Levels of “SDFI<sup>®</sup>” Security

### *The First Element of Security*

The first element of security is defined by a specific storyboard of overlapping pictures. The first picture is taken from a wide angle, allowing the subject matter to “fill the screen”. That picture is supported by a number of closer views or magnifications each captured approximately 50% closer than the last. (Please refer to the SDFI<sup>®</sup> Digital Protocol).

The value of an overlapping forensic storyboard serves two critical purposes: One, the storyboard tells a story when presented in court. Two, the storyboard ensures that the pictures are of what the record(s) say they are.

SDFI Reference Document:

[http://www.sdfi.com/downloads/SDFI\\_Digital\\_Protocol.pdf](http://www.sdfi.com/downloads/SDFI_Digital_Protocol.pdf)

### *The Second Element of Security*

The second element of security is in the digital camera. The camera is set to capture RAW files. RAW files are camera model specific to the digital camera’s photo sensor.

The RAW data is encoded to the camera’s sensor. The development of such technology is kept as a corporate secret. RAW file data is based on a secretly held library of values and variables only known to the manufacture of the digital camera. Simple tests conducted by the camera manufacture or HASH tests can determine if the file was ever tampered with.

Just trying to manipulate one single RAW file would take considerable time, money, effort and planning. If you compound the time, money and effort for each of the storyboard pictures taken during the exam, each at different views, the realistic potential for image tampering is extremely low.



# SDFI<sup>®</sup> - TeleMedicine

Secure Digital Forensic Imaging – Secure Beyond Reasonable Doubt<sup>®</sup>

## *The Fifth Element of Security*

The fifth element of security is a combination of layers of encryption algorithms that are used when transferring forensic data via the Internet. Both AES 256-bit encryption and SHA-1 + RSA 2048-bit SSL encryption is used to ensure that even internet service providers cannot access or examine the digital evidence.

Upon request, the Examiner or Program Coordinator accesses the local or local networked AES 256-bit encrypted disk containing the forensic evidence. The specific individual's forensic folder is selected and independently encrypted with AES-256 bit encryption. A totally separate and independent long passphrase is used, made up on the spot, for each SDFI-TeleMedicine secure file sent out.

This totally independent self decrypting SDFI-TeleMedicine Secure File prevents anyone from knowing about, viewing or tampering with the encrypted forensic data inside. Not even your own I.T. personnel or your Internet Service Providers could know what is contained inside the SDFI-TeleMedicine Secure File.

The first encryption algorithm protects the forensic data inside the SDFI-TeleMedicine Secure File. A second and completely separate SHA-1 + RSA 2048-bit SSL encryption algorithms are activated when a user accesses the "SDFI" File Transfer Portal through the SDFI web site making SDFI<sup>®</sup>-TeleMedicine Secure Beyond Reasonable Doubt<sup>®</sup>

# SDFI<sup>®</sup> - TeleMedicine

Secure Digital Forensic Imaging – Secure Beyond Reasonable Doubt<sup>®</sup>

## *Additional Elements of Security*

Additional security measures are in place for users of the on-line SDFI File Transfer Portal.

Presented below is a **sample** of the “Global User Security Policy” for the SDFI File Transfer Portal. For obvious security reasons, the exact configuration is not shown here and is randomly adjusted.



The screenshot displays a configuration window titled "Global User Security Policy" with a blue header. It is divided into three sections: "Username Rules", "Password Rules", and "Visibility of Site Users in Contact List".

- Username Rules:** Minimum Length: XX (with a note: "Increase the number of digits for security"); Require Numbers: No (with a note: "ex: 'username123'").
- Password Rules:** Minimum Length: XX (with a note: "Increase the number of digits for security"); Require Numbers: Yes (with a note: "ex: 'pass123word'"); Cannot Start or End with Numbers: Yes (with a note: "Prevents 'password1', 'password2', etc."); Expire After: XX (with a note: "Days (0 means the password never expires)"); Cannot Be Reused Until After: XX (with a note: "Changes (0 means no password history rule)").
- Visibility of Site Users in Contact List:** In the Contact List: Show all users, site-wide.

At the bottom, there is a note: "Note: Security Policy changes take effect at the time of the next password change or user login." and two buttons: "Save" and "Cancel".

The FNE or sender of the SDFI-TeleMedicine file is in control of the “SDFI” File Portal at all times. A limit on the number of downloads can also be set, allowing for extended control of the already double encrypted and camera encoded evidence files.

All SDFI-TeleMedicine files are permanently removed from the file portal 10 days after they are uploaded. A one day, 24 hour, disaster recovery plan is in place at the file portal data center.

Beyond the 11 day mark, that SDFI-TeleMedicine Secure File that was up on the File Portal is just gone!

# SDFI<sup>®</sup> - TeleMedicine

Secure Digital Forensic Imaging – Secure Beyond Reasonable Doubt<sup>®</sup>

## About The SDFI<sup>®</sup> - TeleMedicine File Portal

### SDFI-TeleMedicine File Portal Benefits Include:

- ❖ The SDFI-TeleMedicine File Portal Service is an **OPTIONAL** service after the first year. **The “File Portal” is NOT a free service.**
- ❖ Optional minimal subscription fee, equal to \$75.00 per month, per installation, due annually, each January. If you process three or more cases a month, the SDFI File Portal pays for itself.
- ❖ Support offered via phone, e-mail and “remote access” during business hours. See [http://www.sdfi.com/sdfi\\_contact\\_us.html](http://www.sdfi.com/sdfi_contact_us.html) for business hours.
- ❖ Unlimited 23 hour of use per day of the SDFI-TeleMedicine File Portal.
- ❖ 95% system uptime.
- ❖ 2000 MB / 2 GB of SDFI Secure File transfer capability (Equal to 2000 floppy disks.)
- ❖ Free short term emergency “file transfer capability” upgrade upon request.
- ❖ SDFI File Portal is upgradable to 3GB, 5GB or 10GB or more. This is **NOT** a free service.
- ❖ Internet Transmission Security – Independent SSL High Grade Encryption (SHA1+RSA 2048 bit) ensures security of transmissions between computers and the SDFI-TeleMedicine File Portal. Verified by SecureTrust CA.
- ❖ Automatic e-mail notification delivered to sender when recipients download a “SDFI Secure File”.
- ❖ The SDFI File Portal web interface has an easy to see, easy to use screen layout.
- ❖ Able to access the SDFI File Portal through any current web browser.
- ❖ Able to instantly revoke access to any SDFI Secure File inside the SDFI File Portal.
- ❖ Able to instantly and permanently remove any SDFI Secure File.
- ❖ Automatic and permanent removals of SDFI Secure Files after 10 days.
- ❖ Able to create and store an e-mail address book of SDFI Secure File recipients.
- ❖ Extended alphanumeric login names and extended alphanumeric passphrases are used to ensure security.
- ❖ The SDFI File Portal passphrase expires after a set amount of time (User is required to change their online access passphrase at that time).
- ❖ All “SDFI Secure Files” are stored behind computer firewall network protection systems.
- ❖ All inbound “SDFI Secure Files” are scanned for viruses.
- ❖ How to “Intelligent User Guides” are available to system users via the SDFI web page.

# SDFI<sup>®</sup> - TeleMedicine

Secure Digital Forensic Imaging – Secure Beyond Reasonable Doubt<sup>®</sup>

## Document Summary

SDFI<sup>®</sup>-TeleMedicine is proud to state that SDFI<sup>®</sup> is Secure Beyond Reasonable Doubt<sup>®</sup> and beyond HIPAA security<sup>(1)</sup>.

Our simplified methodology combined with the 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 are kept safe and secure.

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

Please send any questions directly to:

**E-Mail:** [Support@SDFI.com](mailto:Support@SDFI.com)

**Phone:** 310-492-7372

**Web Page:** <http://www.SDFI.com>

**SDFI-TeleMedicine**  
**ATTN: Technical Support**  
**806 Buchanan Blvd STE 115-299**  
**Boulder City, NV 89005**

<sup>(1)</sup> SDFI Reference Document: [http://www.sdfi.com/downloads/hipaa/SDFI\\_is\\_beyond\\_HIPAA\\_Security.pdf](http://www.sdfi.com/downloads/hipaa/SDFI_is_beyond_HIPAA_Security.pdf)