



SDFI

Secure Digital
Forensic Imaging

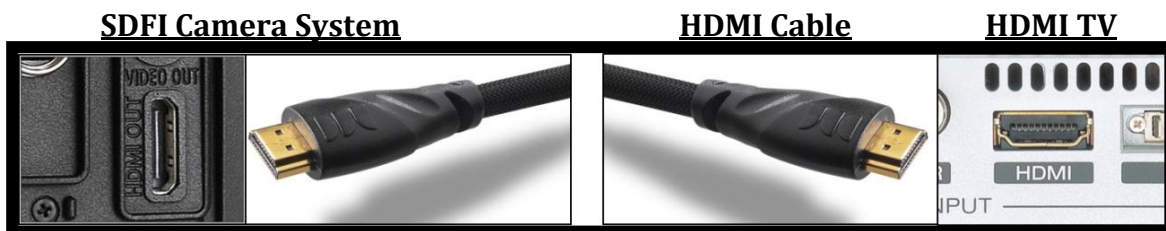
Secure Beyond Reasonable Doubt®

SDFI-TeleMedicine PD Camera System Technical Requirements

The main SDFI® components described below are in the order that they are used. SDFI users always supply their own computer, high-speed internet and a fast response HDMI compliant HDTV. SDFI does **NOT** provide storage for forensic data and subsequently has no access to forensic data. Users are solely responsible for the regular backup and ongoing protection of the data collected.

You will need the following:

- ❖ Our high-resolution digital camera(s) capable of capturing and saving RAW and JPG files.
- ❖ Our non-destructive image management software. **(single user license)**
- ❖ One unused and **unrestricted USB 3.0 port** with full read/write access, unless transferring images by other means.
- ❖ A Windows 7/10 computer (64-Bit with minimum 8 GB RAM). Hard drives used cannot be compressed. SDFI software will not work on compressed hard drives.
- ❖ Internet browser: Internet Explorer 10 or higher, Firefox and Chrome.
- ❖ Whitelist all @SDFI.com and @filesanywhere.com email addresses
- ❖ 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® file portal access to download installation package.
(An exception to download .exe files is necessary)
- ❖ Internet access to all of: <https://global.gotomeeting.com>, <https://assist.zoho.com>, <https://join.zoho.com/>, *.zoho.com, *.zohoassist.com for technical support.
(All remote connections are chaperoned. SDFI cannot access PC without a user present)
- ❖ A large fast response LCD, LED or plasma television **(Optional - not supplied)** with one unused and unrestricted HDMI connection port. A wall-mounted unit with an extendable arm is recommended and optional. This is to be connected to the camera in the space you work in.





SDFI

Secure Digital
Forensic Imaging

Secure Beyond Reasonable Doubt®

SDFI-TeleMedicine Technical Requirements (Continued)

If you use the SDFI File Portal (purchased separately), the information below applies.

SDFI® uses an ultra-secure process as simple as “Click, Save and Call” for the SDFI-Telemedicine process. When the SDFI user makes an AES 256-bit encrypted file available, the process is as follows:

1. Recipient users receive a notification **only** e-mail message from the SDFI user’s email address (***NOTHING is EVER attached to e-mail!***)
2. Recipient users will **CLICK** on the link inside the notification e-mail. The link will take them directly to <https://fileportal.SDFI.com>. Our site uses TLS, RCA, with AES 128 CBC SHA 128 bit key encryption. The site is HIPAA, GLBA, SOX, SSAE16, PCI and ISO27002 compliant.
3. Recipient users will **SAVE** the SDFI Secure Case File on their computer (note: Users choose where they save the SDFI Secure Case File). This file is an AES 256-bit encrypted container, downloaded off the <https://fileportal.SDFI.com> web site. Again, our site uses TLS, RCA, with AES 128 CBC SHA 128 bit key encryption. The site itself is HIPAA, GLBA, SOX, SSAE16, PCI and ISO27002 compliant. It is secure beyond HIPAA!
4. Recipient users must pick up the phone and **CALL** the SDFI user who sent the SDFI secure file and ask for the SDFI Secure Case File passphrase (the sender’s e-mail address will be in the notification e-mail message. NOTE: SDFI passphrases can be up to 256 characters that include upper case, lower case, special characters and spaces). **SDFI® is “Secure Beyond Reasonable Doubt!”**

The SDFI Intelligent User Guide for SDFI Secure Case File recipients can be found here:

www.sdfi.com/downloads/SDFI_YELLOW_DOWNLOAD_GUIDE.pdf

ADDITIONAL NOTES:

- Through SDFI -TeleMedicine, digital forensic evidence is **never** sent via e-mail or as an e-mail attachment. All files are independently and locally encrypted with AES 256-bit encryption **before** the SDFI-TeleMedicine process is initiated. SDFI users will also receive an automated time stamped email as part of the “Click, Save, Call” process. All activity is securely logged.
- The SDFI File Portal is defaulted to auto purge a file that was uploaded after 7 days. The SDFI File Portal is also defaulted to allow the recipient of a SDFI Secure File to have 5 download attempts within 5 days to download the SDFI Secure File.
- The SDFI process is secure beyond HIPAA⁽¹⁾.

Contact your I.T. department for help. Please have I.T. call SDFI® directly at 310-492-5372 ext. 3 or email support@SDFI.com with any questions.

(1). SDFI reference document:

http://www.sdfi.com/downloads/SDFI_is_beyond_hipaa_security.pdf