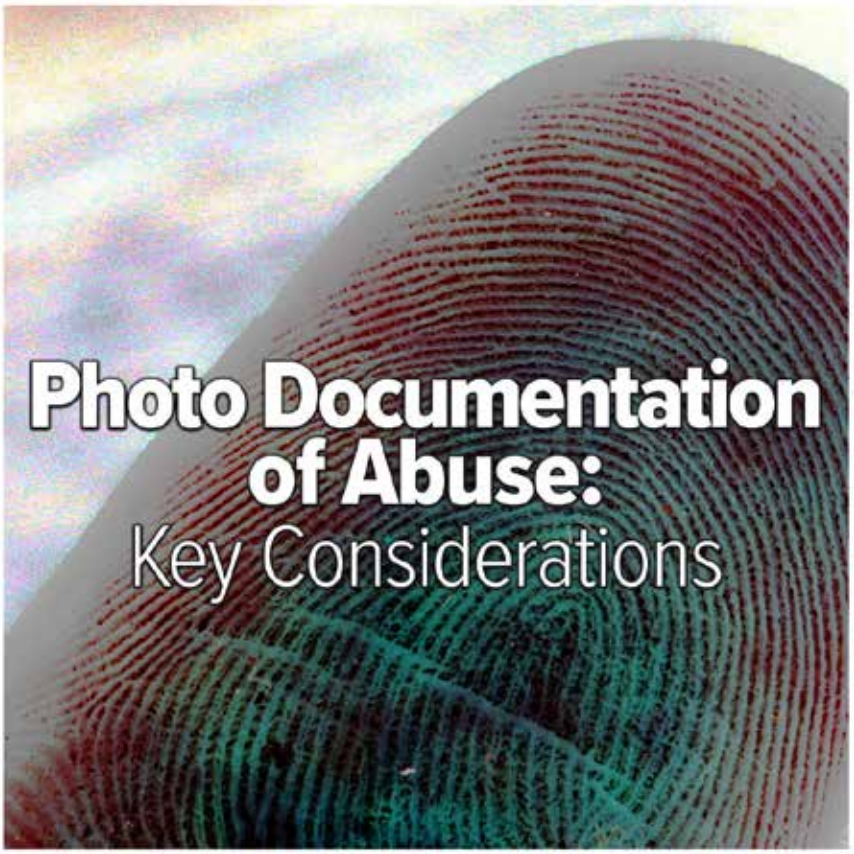

Written by Ward Allen, Diana Faugno, Valerie Sievers, & Brijida Rodarte

IT IS A DIFFICULT PART OF THE PROCESS of serving an abused child: documenting the evidence of abuse to ensure justice for the victim. That's why the National Children's Alliance's (NCA) latest edition of its Standards for Accredited Members mandates that to achieve this high level of practice in serving children, Children's Advocacy Centers (CACs) must collect "diagnostic-quality photographic documentation" of exam findings, and protect, store, and release these images in a secure, sensitive way.

Here are a few common questions and their answers informed by our years of working with CACs to implement our photo documentation systems.

How Can I Ensure My Images are "Diagnostic-Quality"?

How can you meet this all-important definition, take diagnostic-quality photos, and select a photo-documentation system that empowers a CAC to build a solid body of evidence and achieve

justice for kids? We have developed some tips for CACs on how to ensure their evidentiary imaging is up to the Standards—and stands up in court.

1. Know How to Tell a Good Photo From a Bad Photo

First, make sure the image shown is at 100% (1 screen pixel to 1 image pixel, also shown as "original size") and not scaled down to your screen's resolution on your secure evidence computer. This is the only way to evaluate the quality of the image. (Most basic Windows computers offer a photo-viewing program, a free tool that allows you to view your image at 100% size.) Now, look at the photo and ask yourself these questions:

- Does the image represent the subject matter?
- Is the image clear and in focus?
- Is the image properly exposed—not too light or too dark?
- Is the image straight and aligned—not twisted or skewed?

If the answer is "Yes" to all of these, then your images are diagnostic-quality and the photo documentation system is capable of delivering the image quality you need. If not, it may be time to examine your practices or find a new photo-documentation system.

2. Determine Whether Your Existing or Prospective System is Easy to Use

Medical personnel are obviously patient-centered, so it is important that you can easily pick up a photo-documentation system and capture diagnostic-quality pictures, quickly and effectively. It needs to be compact, portable, and easy to operate.

3. Think About a Situation When You Bring a JPEG To Court

What will happen if the defense team questions the photo's validity? Think of any way the defense team might challenge your images and get them thrown out of court. Proving in court that a JPEG has not been manipulated requires a review of the Federal Rules of Evidence, Article X, Contents of Writings, Recordings, and Photographs Rule 1003, Admissibility of Duplicates. It states, "A duplicate is admissible to the same extent as the original unless a genuine question is raised about the original's authenticity or the circumstances make it unfair to admit the duplicate."

4. Ensure Your CAC has Saved a RAW File for Each JPEG Captured

If the defense attorney or their expert witness mathematically proves that your JPEG is not original—and they can—the court may determine it unfair to admit the duplicate JPEG image. Smart defense attorneys know this and may use this argument to have evidence ruled out. So, be sure you are ready with that RAW file.

Some may wonder what the differences are between a RAW file, a JPEG file, and their role in forensic photo-documentation. Simply, a RAW file is a digital negative: a data-file format, not an image-file format. RAW data cannot be manipulated in any way, shape, or form because it is technically not an image. RAW files also hold metadata. Metadata passed along to the JPEG image-file format includes date, time, and camera-setting details. Digital cameras create JPEGs from RAW data inside digital cameras. JPEG files can be easily changed and manipulated via image-management software, whereas RAW files cannot. In order for you to create a RAW file, you should use a DSLR high-resolution camera. See this link for more information.

Who Pays For The Photos And Video Captured During A Forensic Medical Exam?

If your state accepts STOP Grant Funds—and every state in the U.S. does—then "the state or territory or another governmental entity incurs the full out-of-pocket cost of forensic medical exams for victims of sexual assault."

Note: *The target of the STOP Program is adult and youth victims. "A person who is 11 to 24 years old" defines a youth.*

Title 34 U.S.C. 10449 reads as follows: "A State, Indian tribal government, or unit of local government shall not be entitled to funds under this subchapter 1 unless the State, Indian tribal government, unit of local government, or another governmental entity…

(A) Incurs the full out-of-pocket cost of forensic medical exams…

Note: *Title 34 U.S.C. 10449, Sub-section (A), above, is not limited by a person's age. That means that under Title 34 U.S.C. 10449, all living victims of sexual assault are covered.*

The Department of Justice, under 28 CFR, Part 90 – Violence Against Woman, Subpart A – General Provisions, Section 90.2 – Definitions, is clear on this subject and states the following:

> 1) In addition to the definitions in this section, the definitions in 42 U.S.C. 13925(a) apply to all grants awarded by the Office on Violence Against Women and all subgrants made under such awards.
>
> 2) The term "forensic medical examination" means an examination provided to a victim of sexual assault by medical personnel to gather evidence of a sexual assault in a manner suitable for use in a court of law.

In short, charging or billing a patient for a forensic medical exam could lead to the loss of DOJ federal funding for your entire state.

The updated October 2017 "FAQs About STOP Formula Grants" published by the United States Department of Justice, Office on Violence Against Women, repeats the definition and the specific purpose of a forensic medical examination.

To see how to be reimbursed for forensic exams, click this link and scroll to your state.

Are the Photos and Video Captured During a Forensic Exam Considered Forensic Evidence or Part of the Medical Record?

If photography and video capture is part of the forensic exam, then the state pays for it and the photos and video are forensic evidence and part of the forensic record. If your organization—through a state law, a policy, or a protocol—normally captures ano-genital photographs/videos of children as part of your everyday medical practice and your organization charges that patient, their health-care insurance and/or your organization processes the cost of capturing those photographs/videos through a "health-care clearinghouse", then the photos and related video are medical.

How Long Do We Need To Keep Our Photos?

If the photos you captured during the forensic exam were paid for by the state, then State Criminal Statutes of Limitations apply. See State Criminal Statutes of Limitations in Sexual Abuse Crimes. Any case could go federal. If it does, then photos should be made available "any time without limitation".

If medical photos were captured during a forensic exam, as described above see State Medical Record Laws.

Either way, photos and video captured during an exam must have a secure, sustainable, and backed-up storage system to protect the photos and videos.

How Can We Securely Store Our Photos?

Do not store forensic evidence in a medical record. Medical Break Glass Policy is not compatible with a Legal Chain of Custody. See the seven-minute video on this specific subject.

Hacking is indeed a big concern with all the data out there, and rightfully so. In May 2017, it was globally reported that 150 countries had been hacked. Here in the U.S., the U.S. Department of Health and Human Services Breach Portal reported over 4.5 million medical-record breaches in 2017. Between January 1, 2018 and April 25, 2018, there were over 1.7 million breaches. Both reports only include breaches affecting 500 or more individuals. Also refer to the Ponemon Institute's Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. They report health-

care related breaches constituted $6.2 billion in losses. According to identity fraud experts, more than 140 million individuals in the United States—roughly 50% of the population—have had their health-care records lost, breached, or stolen. In 2015, IBM noted that health care had the highest rate of data breaches compared to any other industry.

The safest and easiest way for you to protect your forensic evidence, including pictures and video—paid for and belonging to the state—is to sequester your forensic photos and video away from medical records. Ensure that nested, end-to-end encryption is used, such as the 256-Bit Advanced Encryption Standard, when you store and release photos.

Beware of the Cloud

Store encrypted storage volumes on your own network and on your own network computer—not in the cloud or on a desktop computer. Neither are a safe place.

Cloud storage, like real clouds, drifts and moves like the wind. Like real clouds in the sky, computer clouds can dissipate or merge with other clouds that are located in other countries who do not have the same data protection laws we do. Using cloud computing means that you do not have control of your data. More important, if you miss a cloud-storage payment, you may lose all of your data.

When you use cloud services, like most cellphone and tablet apps do, the service and the app usually requires your authorization to collect data, including personal data, usage data, patient data, and your photographs. Do not do it!

Always Read Your User Agreements!

Make sure you know what you are getting into by storing your data with these services. Many cloud services and apps that utilize secure mobile colposcopes, iPads, iPhones, Android, or secure storage on major data providers, require user agreement terms that are untenable for CACs.

Before you sign up for a service, take the time to read the language and determine whether you are really willing or able to abide by the terms offered. Below are samples of text from real consent agreements for "secure" cellphone based colposcopes—with language that may make it impossible to keep your data secure, sequestered, and accessible. Some examples include:

> "YOU AGREE TO THE TERMS AND CONDITIONS SET FORTH IN THIS PRIVACY POLICY, INCLUDING TO THE POSSIBLE COLLECTION AND PROCESSING, MONITORING, STORING AND SHARING OF THE INFORMATION […]"
>
> "Each Session may include the Clinician's name, the patient's ID (actual or made-up), the clinical image, image date, Clinician's diagnosis, general geo-location of Clinician's mobile device […]"
>
> "[…] may transfer and disclose Non-personal Information to third parties at its sole discretion and without restriction."
>
> "[…] we cannot guarantee that unauthorized access or use will never occur […]"
>
> "Cancelling your Account may cause inability to access your Account and/or the loss of certain information (including, without limitation, the Sessions and/or clinical images or any Personal Information)."
>
> "We may transfer information collected about you, including Personal Information, to affiliated entities, or to other third party service provides[…] across borders.[…]you consent to such transfer of information."

Take the steps to ensure that your patients are not charged for forensic-medical exams and use the information here along with the references linked in this article to protect the forensic evidence that is gathered on behalf of your patients.

About The Authors

Ward Allen's full technical experience spans almost four decades in both Canada and the United States. It includes the utilization of both analog and digital photography systems; various computer network communications systems directly

related to the development, introduction, use, and management of digital photographs; and ongoing development of digital forensic imaging solutions for CAC, SANE, SART, and SAFE programs.

Diana K. Faugno (MSN, RN, CPN, SANE-A, SANE-P, FAAFS, DF-IAFN, DF-AFN) is a Founding Board Director for End Violence Against Women International (EVAWI), is the current president of the Academy of Forensic Nurses, as well as a retired-fellow in the American Academy of Forensic Science and a Distinguished Fellow in the Academy of Forensic Nursing. She now works for Life Safe as a forensic nurse in Marietta, Georgia.

Valerie Sievers (MSN, RN, CNS, SANE-A, SANE-P, DF-AFN) is a Forensic Clinical Nurse Specialist with more than 35 years of health care experience as a registered nurse, advanced-practice nurse, educator, and consultant. She is currently owner of MedLaw Consultants, LLC, editor of Forensic Nursing Exchange, and serves as a board member of the Academy of Forensic Nursing.

Brijida Rodarte is the Deputy District Attorney for Riverside, California and a member of the Sexual Assault & Child Abuse Team.