



# **JTC Quick Response Bulletin**

---

## Managing Evidence for Virtual Hearings

---

Version 1.0  
Presented 25 June 2020

## Abstract

As a result of stay-at-home orders tied to the COVID-19 pandemic, courts in most states are conducting virtual hearings: using technology to facilitate a hearing without the judge and the parties being physically gathered in one location. Evidence is a key aspect of those virtual hearings. Much can be gleaned from the ways other types of organizations do business virtually. However, courts have unique needs that require thoughtful attention as they impact how evidence is submitted, stored, and shared to support a virtual hearing.

## Document History and Version Control

Version	Date Approved	Approved by	Brief Description
1.0	6/25/2020	JTC	Released following circulation for comment.

## Acknowledgments

This document is a product of the Joint Technology Committee (JTC) established by the Conference of State Court Administrators (COSCA), the National Association for Court Management (NACM) and the National Center for State Courts (NCSC).



### JTC Mission:

To improve the administration of justice through technology

### Joint Technology Committee:

---

#### **COSCA Appointments**

David Slayton (Co-Chair)  
Texas Office of Court Administration

David K. Byers  
Arizona Supreme Court

Jeff Shorba  
Minnesota Judicial Branch

Rodney Maile  
Administrative Office of the Courts, Hawaii

Laurie Dudgeon  
Kentucky Administrative Office of the Courts

#### **NCSC Appointments**

Justice Deno Himonas  
Utah Supreme Court

Judge Samuel A. Thumma  
Arizona Court of Appeals, Division One

#### **Ex-officio Appointments**

Joseph D.K. Wheeler  
IJIS Courts Advisory Committee

#### **NACM Appointments**

Kevin Bowling (Co-Chair)  
Michigan 20<sup>th</sup> Judicial Circuit Court

Paul DeLosh  
Supreme Court of Virginia

Roger Rand  
Multnomah Circuit Court, Oregon

Kelly C. Steele  
Florida Ninth Judicial Circuit Court

Jeffrey Tsunekawa  
Texas Office of Court Administration

#### **CITOC Appointments**

Jorge Basto  
Judicial Council of Georgia

Casey Kennedy  
Texas Office of Court Administration

#### **NCSC Staff**

Paul Embley  
Jim Harris

Compiled and written by Lise Embley, technical writer, National Center for State Courts

### Additional contributors

---

Judge Sohail Mohammed, New Jersey Courts

Judge Jennifer Bailey, Eleventh Judicial Circuit (Florida)

Professor Ben Trachtenberg, University of Missouri School of Law

David Jackson, IJIS Institute

Rochelle Klempner, New York State Courts

## Table of Contents

Abstract.....	ii
Document History and Version Control .....	ii
Acknowledgments .....	iii
Table of Contents.....	iv
Introduction .....	1
Considerations .....	1
Self-Represented Litigants .....	1
Physical Evidence .....	2
Integrity/Protection of Submissions .....	2
Security and Privacy .....	3
File Management .....	4
Wet Signatures .....	5
Authentication .....	5
Court Records.....	6
Technology .....	6
Technical Support.....	6
Evidence Workflow.....	7
Prior to a Hearing.....	7
During a Hearing.....	8
After a Hearing.....	9
Instead of a Hearing.....	9
Platforms and Mechanisms for Sharing.....	9
Evidence Management Systems .....	10
Cloud Storage.....	11
Conferencing Platform .....	11
Physical Media.....	11
Email.....	11
Obstacles and Opportunities .....	12
Conclusion .....	12
Appendix A - Resources.....	13
Appendix B - Sample Notice of Filing, Use and Submission of Exhibits for Virtual Hearing.....	14

## Introduction

As a result of stay-at-home orders tied to the COVID-19 pandemic, courts in most states are conducting virtual hearings: using audio or video technology to facilitate a hearing without all the participants (the judge, the parties, attorneys, and others) being physically gathered in one location. While most courts are delaying jury trials, some are actively preparing for virtual jury trials.

Judges and court staff are adapting to virtual hearing challenges “on the fly” and learning as they go. As stay-at-home orders are lifted, courts will still have to mitigate ongoing risks associated with public gatherings; virtual hearings will likely continue in many places. Courts are sharing examples and emerging best practices as well as advisories to benefit the court community as a whole. A critical aspect of this effort is how evidence will be handled during virtual hearings.

## Considerations

Most videoconferencing platforms provide tools that can be used to view and share evidence during a virtual hearing. Much can be gleaned from the ways other types of organizations share information and do business virtually. However, courts have unique needs that require thoughtful attention, particularly to how evidence is submitted, stored, and shared.

### Self-Represented Litigants

To ensure full access by self-represented litigants (SRLs), courts should provide an easily accessible mechanism for submitting evidence. Any evidence submission application should be mobile responsive; SRLs may need to provide evidence via mobile device even if that evidence does not originate on the device.

Step-by-step instructions and brief videos can be used in addition to text-based information to educate the public about court processes, including evidence submission and use during a hearing. It is particularly important to educate SRLs about the public nature of evidence submitted and provide clear guidelines to help prevent sensitive or confidential information from being shared in a way that could make it part of the public record, searchable via the web.

Courts may also wish to provide practical information to SRLs, including how to create and view PDF and PDF/A documents, the best lighting for a virtual hearing, court rules regarding privacy, and what to expect during the hearing. Because SRLs may not have access to adequate technology or the luxury of a quiet, private space to participate in a hearing, courts may wish to offer SRLs access to a technology-equipped room at the courthouse. Courts should also consider giving SRLs the opportunity to participate in a pre-hearing “dry run” complete with audio and video checks as well as an opportunity to try sending and receiving evidence using the court’s preferred platform.

## Physical Evidence

Documents and digital evidence such as social media posts and text messages are the most common kinds of evidence to manage during a virtual hearing. However, many hearings require the ability to review physical evidence. Items can be photographed or videotaped clearly and those images made available to multiple participants at different locations simultaneously during a virtual hearing while the court retains the original object. Screen sharing can also be used to allow parties to view physical evidence such as clothing, weapons, etc.

If the witness can't physically touch the item, courts may wish to have a process for certifying that the item being shown during the hearing is the same one provided to the court. While it is already common for parties to stipulate to the authenticity of evidence (or to make admissions during discovery that essentially stipulates to the legitimacy of some records), this should ideally occur in advance of virtual hearings.

There may be additional issues for documentary evidence when the law requires surrender of the original document to the court. Depending on local law requirements, this may be important in mortgage foreclosures, particularly, which have been mostly "paused" during the COVID-19 pandemic. As pandemic-related restrictions are removed, courts anticipate a significant increase in these cases.

Even with virtual hearings and digitized evidence, courts may require that physical copies of evidence be submitted to the court prior to the virtual hearing. Since avoiding person-to-person contact is the point of virtual hearings, courts should not implement physical evidence policies or timelines that would require parties to deliver evidence to the courthouse in person. When necessary, courts should allow submission by mail and/or via a "no touch" drop box outside the courthouse.

## Integrity/Protection of Submissions

Data manipulation and alteration pose a significant risk that courts must not overlook. File format, storage, and transfer methods can impact the integrity of the evidence. Documents and text messages can be modified to change the date, time, and content. Accounts can be "spoofed" to make it appear that a message came from someone other than the individual who actually sent it. Good evidence handling practices are important to ensure that digital evidence is protected from both intentional and unintentional modification.

Screenshots and printouts (to PDF/A) of messages that include identifying information link the message to the sender; testimony or affidavit that the copy is a true and accurate representation of the text messages serves as authentication. When possible, copies of text messages or emails should include

the electronic timestamps showing the date and time of each message as well as the contact information of the sender (phone number and/or email address).<sup>1</sup>

Data protection requires fairly significant technical understanding. The FBI's [Criminal Justice Information Services Policy Resource Center](#) provides excellent guidance for best practices in creating, viewing, modifying, transmitting, dissemination, storing and destroying criminal justice information, including evidence. While not written specifically for the court community, these guidelines address many of the issues courts face with managing evidence in a virtual hearing.

In addition, Federal, state, and local government agencies, including entities within the court system and prosecuting attorneys' offices in particular, have access to Criminal Justice Information Services (CJIS) data, which means that, by law, they must maintain CJIS compliance. In doing so, they gain access to the information they need to perform their duties while preserving individual civil liberties. Failure to comply with CJIS can result in denial of access to any FBI database or system, fines, and even criminal charges. Courts should understand and seek to comply with CJIS information security requirements and guidelines contained in the [CJIS Security Policy](#).<sup>2</sup>

To prevent modification, documents should be "flattened" or "locked" in PDF/A format,<sup>3</sup> an archival and preservation format that ensures documents will look the same regardless of the software used to view them. Digital signatures in PDF/A format are secure enough to be legally binding in most industrialized countries. Cryptographic hash values can be used by experts to authenticate and verify some kinds of digital evidence.

Access to evidence shared and stored digitally should be controlled and access points limited. Electronic audit logging should be enabled to document when files are accessed and by whom. As courts move to more digital processes, the need for a robust evidence management system will only increase. Ad hoc approaches facilitate urgent requirements but must not be left in place any longer than is necessary to implement a more secure approach.

## Security and Privacy

Tied closely to data integrity is security and privacy. When the court record is digital, there is a much wider potential audience than when the court's record is tucked away in a paper file at the courthouse. Courts must be particularly attentive to SRLs submission of evidence to prevent the unintentional submission

---

<sup>1</sup> [Text Messages as Evidence: A How-To Overview](#). MassLegalServices.org. Massachusetts Legal Assistance Corporation. 24 October 2019. Web.

<sup>2</sup> ["CJIS Security Policy Resource Center."](#) FBI, US Department of Justice, 2 June 2016, [www.fbi.gov/services/cjis/cjis-security-policy-resource-center](http://www.fbi.gov/services/cjis/cjis-security-policy-resource-center).

<sup>3</sup> For information about converting documents to PDF/A, see ["Converting Files to PDF/A Format"](#) at [research.gov](http://research.gov).

of information that should not be made public. Parties typically are responsible for ensuring that sensitive or confidential information is redacted so that it is not shared in this way. In addition, automated redaction software<sup>4</sup> could be implemented to identify and redact many kinds of obvious personal identifiable information (PII) like social security numbers, phone numbers, etc.

The location of parties and witnesses in virtual hearings may also present security and privacy concerns that courts must anticipate. Some courts require witnesses to swear under oath that no one else is present or listening and/or use their device's camera to pan around the room to demonstrate that no one else is present.

Email is widely accessible and familiar to most people, but it is not a particularly secure method of transmission for sensitive information. People commonly make errors in email communications: wrong subject line, failing to attach the intended file, or attaching a completely unrelated file. One email may be followed immediately or at a later date with another, leaving the possibility of confusion about which is the most current version. Email can be misdirected, intercepted, or easily forwarded.

More significantly, the court's network and data security are at stake when email is the mechanism used to submit evidence: one of the most common entry points for destructive viruses is email. An innocuous-looking link can introduce a virus that can effectively disable a court for months and cause millions of dollars in damage. And email is not at all well suited to sharing large numbers of files or files of significant size.

Consider the sensitivity, the type of hearing, the level of security required, and utilize the appropriate medium. For example, file sharing via either a conferencing platform or a cloud storage platform that is Health Insurance Portability and Accountability Act (HIPAA) and CJIS compliant are both more secure than email. Courts should also ensure that evidence for use in one hearing cannot be accessed by parties or attorneys in a different case.

## **File Management**

Some courts use separate folders to collect evidence for each case. In the example below, the judge has a folder for each case. Within that folder, exhibits are clearly named, making them easy to locate. Each Exhibit should be saved as an individual file and labeled according to submitting party, i.e. D-1 for Defense Exhibit # 1, S-1 for State Exhibit # 1.

---

<sup>4</sup> For more information about automated redaction, see the State Justice Institute/National Center for State Courts report, *Automated Redaction - Proof of Concept* (2017).



Name	Status	Date modified	Type	Size
D-1 (Plea Form)	✓	4/22/2020 9:00 PM	Microsoft Word Doc...	12 KB
D-1 (Plea Form)	✓	4/22/2020 9:03 PM	PDF File	32 KB
S-1 (Victim Statment)	✓	4/22/2020 9:02 PM	Microsoft Word Doc...	12 KB
S-1 (Victim Statment)	✓	4/22/2020 9:03 PM	PDF File	32 KB

Some courts are using a single virtual “bucket” for all the evidence that will be needed for all cases in a single day. In that approach, attorneys and SRLs are responsible to redact sensitive or private information and must remember to remove their evidence from the shared location after the hearing. Whatever is left at the end of the day is purged from the folder by court staff. While this approach may be relatively quick and easy to implement, it would almost certainly fail scrutiny under PII-protection standards in HIPAA, CJIS, and General Data Protection Regulation (GDPR)<sup>5</sup> on the grounds of privacy and lack of audit trails.

When evidence for more than one hearing is stored in a shared location, someone could inadvertently (or intentionally) access sensitive information without appropriate authority. Evidence management systems handle permissions very effectively, but courts can also segment evidence by case and use individual logins when managing evidence in cloud storage platforms. Protecting privacy and ensuring accountability are key components of data security and integrity.

File retention rules clearly apply to paper documents. Some courts extend those rules to digital files, as well. However, digital storage space is more readily available than physical storage space, and digital files can exist in more than one place simultaneously. Courts can’t actually “return” digital files but must decide whether to delete or retain them for a specific period of time or indefinitely.

### Wet Signatures

Most courts are operating under temporary rules that allow for virtual hearings, including allowing electronic signatures. Identify statutes and rules that reference wet signatures and work to have those permanently removed/changed. Temporary changes that are working effectively may be fairly easy to make permanent.

### Authentication

Tied to the issue of wet signatures is notarization, a process often used to authenticate documents or establish identity. Some courts require parties to have documents such as wills, power of attorney, and living wills notarized - the official process for witnessing and authenticating the signing of important transactions.

---

<sup>5</sup> For more information about potential US implications of the European Union’s GDPR, see JTC Resource Bulletin (2018), [GDPR for Courts](#).

In many jurisdictions, business records must be authenticated for purposes of the hearsay rule.

Known impacts of requiring notarization are primarily negative: costs and process complexity that increase barriers to justice processes. Many industries that once relied on notaries (e.g., real estate) now rely heavily on electronic signatures. Some courts have eliminated notary requirements and are now using “acknowledgments” - check boxes similar to those you tick before submitting an insurance claim, electronically filing a tax return, or doing a software upgrade.

When an authentication requirement cannot be eliminated, courts can still encourage parties to waive the right to demand certain formalities (such as notarization), especially when the authenticity is not in dispute.

### **Court Records**

Some courts have adopted fully digital processes that support both in-person and virtual hearings. If paper is still required as the court’s official record, an important step would be to make the electronic record the court’s official record. This also clears the way for accepting evidence digitally.

### **Technology**

Courts must make long-term plans to address the technology required to support evidence management regardless of whether hearings are virtual or in-person. Virtual and hybrid hearings (some participants at courthouse facilities and some remote/virtual) are likely to be the norm moving forward. Plans must consider the needs of virtual participants particularly.

While smart phones are widely used even among homeless and impoverished populations, some people may not have adequate cellular data or WiFi bandwidth or have other technology obstacles to participation. Courts must ensure all who need to have access to adequate bandwidth and a device with a screen large enough to view evidence clearly. Some courts have converted space at the courthouse<sup>6</sup> or are looking to convert some portion of little-used law libraries into public kiosks for individuals to participate in virtual proceedings. Others are looking to partner with public libraries and social service agencies to create private spaces for virtual participation in court hearings.

### **Technical Support**

In virtual, hybrid, and in-person hearings, participants or jurors may require technical assistance. Each court or court system must determine the level of assistance, if any, it will provide to participants who have difficulty with the technology. Judges or staff assisting with a virtual hearing should be familiar enough with the conferencing platform to screen share and circulate documents.

---

<sup>6</sup> In response to the COVID-19 pandemic, every courthouse in New York has created a space in the courthouse for SRLs to attend virtual hearings, even when the Judge is in the next room.

Judges, clerks, other court officials, and jurors should have ready access to technical support assistance. Court staffing may need to be adjusted to have fewer courthouse clerical assistance roles and more “tech support” type roles.

## Evidence Workflow

The court must provide a way for evidence to be submitted electronically and clearly communicate the process for doing so. While each judge and each court may have unique aspects of their workflow, evidence management processes occur before, during, and after a hearing. In some instances, evidence submission can eliminate the need for a hearing.

The following considerations may be useful to courts as they manage evidence in virtual hearings.

### Prior to a Hearing

It is helpful to hold a conference prior to the hearing to discuss the process and “test drive” the technologies that will be required. Planning is key. Individual judges/courts should provide detailed instructions<sup>7</sup> outlining the process of submitting evidence, including:

file formats	File format should be acceptable to the court and the parties. Some courts require evidence to be converted to a preferred format while others simply specify that the evidence be “readily accessible” and compatible with the court’s systems. Where practicable, digital evidence should also be retained in its original format, along with any required, proprietary viewing software.
naming conventions for exhibits	Evidence files should be marked in a consistent way so they are easy to locate and can be labeled and identified clearly for the record.  Courts may wish to specify naming conventions or prepend submitted evidence files with a sequenced document identifier (e.g., S-1 Victim Statement, or DEF_001_BankofAmerica_Statement). Any changes made to evidence files (including filenames) should be non-destructive and reversible.
exhibit numbering	If Bates-stamped numbers are preferred, they can be added to PDF files automatically using Adobe Acrobat or other PDF Bates numbering tool. Photos can also be pasted into PDFs and Bates stamped.
document preferences	PDF or PDF/A, image orientation, whether documents should be submitted in color or black and white, and if multi-page documents are acceptable or if each document should be submitted in a separate file.

<sup>7</sup> See Appendix B - Sample Notice of Filing, Use and Submission of Exhibits for Virtual Hearing.

markup restrictions	Whether highlighting or marking documents is permitted. In some instances, both marked and unmarked versions of evidence should be submitted. The Judge may review and annotate document-based evidence electronically; many PDF viewers provide annotation features.
file size limitations	Litigants may have smaller file size limitations than each other and the court
deadlines	For submitting evidence (e.g., 5 days prior to hearing) and for filing any objections to exhibits.
platforms and mechanisms for sharing	Parties should be informed about the court's evidence submission platform and provided with step-by-step instructions for use.
how recordings will be handled	Private recordings that may need to be shared more securely. Some courts are using conferencing platforms to make recordings part of the hearing recording. In some instances, parties may need to share videos in advance.
screen sharing	For security and privacy, conferencing platforms should be set to block participants other than the judge and/or clerk from screen sharing. For a participant to share evidence during a hearing, the individual managing the video conference platform would need to temporarily permit screen sharing.
stipulations	Required if giving up rights to examine real evidence.
physical evidence	Who should have physical custody of evidence. Pictures or videos can be used to display physical evidence virtually, regardless of who retains physical custody of the item. In some instances, it may be sufficient to hold evidence up for display during a virtual hearing. Courts must specify which method is preferred/required.
contact information	Phone and/or email for all recipients (SRLs, opposing counsel, court clerk, law clerk, secretary, etc.).
technical support options	Contact information (website, phone number) for technical assistance

### During a Hearing

Evidence for each day's hearings should be stored locally and available to the judge on his/her device. To prevent confusion, documents should generally be organized into individual case folders. Parties should "come" prepared to have digital access to any evidence to be used during the hearing. Usually, this means downloading all exhibits to a device available during the hearing to avoid any delays due to bandwidth, WiFi access, or other technical issues.

During the hearing, additional evidence may be emailed or shared via video conference platform using either “screen sharing” (giving screen control briefly to someone other than the judge) or the platform’s document sharing functionality, if the judge allows it. Evidence that is presented during the hearing (e.g., exhibits used in rebuttal) may be viewed via screen sharing, circulated by email, or shared via link to a cloud storage platform.

Any document submitted during the hearing that was not previously available for pre-hearing filing can be forwarded electronically to appropriate parties while the hearing proceeds, provided the opposing party does not object. If the document is very lengthy and/or the opposing party requests additional time, the judge may then grant a short adjournment (from a few hours to a day).

### **After a Hearing**

After the hearing, the “view” versions of evidence (e.g., copies circulated electronically) no longer matter unless the evidence was annotated in some way during the hearing. Any document or page annotated becomes a new Exhibit that must then be filed and/or uploaded to the case file. For instance, if a detective report is used during the hearing and the Witness annotates this exhibit (drawing with pen the path the perpetrator followed during the commission of the crime), the copy with the witness marking becomes a new Exhibit. If the evidence was used without any annotations, the clerk’s copy can be uploaded to the case management system.

The court retains and files evidence. If the court has a case management or document management system that includes file attachment capabilities, evidence should be attached to the case file.

In courts that require hardcopy, originals utilized during the hearing may need to be delivered to the court following the hearing. Parties and attorneys retain copies in case of appeal. The judge retains his/her virtual notes.

### **Instead of a Hearing**

In some instances, a public-facing digital evidence submission mechanism may resolve some kinds of issues making a hearing unnecessary. For example, a chatbot<sup>8</sup> could be used to streamline the submission of documents and evidence for “fix it” traffic tickets and other simple cases, making it possible for the public to easily submit a photo of a license plate tag to resolve a tag infraction or a PDF of the vehicle owner’s insurance ID card or proof of insurance document.

## **Platforms and Mechanisms for Sharing**

Mechanisms for sharing evidence in a virtual hearing are as varied as the methods for creating, sharing, and storing any digital content. However, some methods provide a

---

<sup>8</sup> For more information about court uses for chatbots, see JTC publication [Getting Started with a Chatbot](#).

much higher level of security than others. Convenience may, of necessity, have been the highest priority as pandemic-related closures forced courts to rapidly implement virtual hearings. As courts settle into longer term use of virtual hearings and adapt to the use of digital evidence for in-person hearings, greater priority should be given to the long-term risks and benefits of various evidence management methods.

Where possible, evidence submission mechanisms should permit submission via smartphone, since pro se litigants may not have access to traditional “office equipment” including computers and scanners.

### **Evidence Management Systems**

While many courts are handling evidence with technologies designed for other purposes, some courts have evidence management systems implemented prior to the pandemic and the widespread transition to virtual hearings. Courts without evidence-specific systems may wish to consider the costs and benefits of a system designed specifically for that purpose, especially in light of the likelihood of long-term use in both virtual and in-person hearings. Evidence management systems can streamline the evidence management process as well as enhance security, making virtual hearings in particular easier to manage.

Electronic filing systems support the submission of electronic documents to the court. It is not uncommon for a litigant to use e-filing to submit an exhibit. However, limitations on the file size and formats accepted by most e-filing systems prevent the e-filing of many forms of digital evidentiary materials (e.g., large video files). The task is best handled by evidence management systems built specifically for this purpose.

Most case management systems have some mechanism for integration with other court business functions reflected in the Court Component Model.<sup>9</sup> In most instances, an evidence management system can be deployed alongside an existing CMS. Some case management system vendors offer a specific evidence management module. Courts should select the tool with the best mix of features, functionality, and integration when selecting an evidence and exhibit management system.

Evidence and Exhibit Management systems are widely available and offer the most robust range of features of all the options discussed in this paper. Cloud-based systems can be deployed fairly quickly and with few upfront capital costs. Reducing the labor cost of storing and managing case files can yield cost benefits. Considering that systems may pay for themselves and will improve the management of evidence in virtual hearings, courts may wish to prioritize the implementation of an evidence management system. For a list of evidence

---

<sup>9</sup> See the JTC Resource Bulletin (2017), [Introduction to the Next-Generation Court Technology Standards Application Component Model](#), p.6 for the Application Component Model.



management products available currently, see the [IJIS Technology Provider Directory](#).

### **Cloud Storage**

Consumer cloud storage platforms (Box, DropBox, OneDrive, iCloud, etc.) offer convenient access but may not meet federal guidelines for security and privacy. Some do not adequately protect metadata that may be necessary to demonstrate the origin or provenance of digital evidence. State and local courts can utilize product and vendor ratings by the Federal Risk and Authorization Management Program (FedRAMP)<sup>10</sup> to help select a secure cloud storage platform.

### **Conferencing Platform**

Courts are using a variety of conferencing platforms: GoToMeeting, Microsoft Teams, Cisco WebEx, Zoom, and more. Not only do these platforms effectively facilitate the audio and video aspects of virtual hearings, they also offer superior file transfer mechanisms. Documents, spreadsheets, PDFs, SMS text, audio, video, image and other digital files can be shared during a hearing either by sending the file through the court's preferred conferencing platform or by screen sharing.

Using the platform's recording features, evidence that exists on personal devices can be incorporated into the court record without witnesses having to relinquish their devices. During a hearing, conferencing platforms are particularly well-suited to working with the kinds of evidence contained in social media posts, "feed" activity, text messages, and videos.

Generally speaking, a conferencing platform would not be the best mechanism for submitting evidence in advance of a hearing.

### **Physical Media**

Thumb drive, DVD, and external hard drives are sometimes used to transfer evidence, particularly if there is a lot of material to be shared. However, thumb drives and external hard drives should be handled as potential sources of malware/ransomware that can lead to a cybersecurity breach. The court's IT staff should provide a screening process to ensure devices do not introduce viruses that would compromise the court's data and networks.

### **Email**

Email may be the least secure method of submitting evidence, but possibly also the most widely used. Courts may choose to receive evidence by email to a specific court staff member. Some courts use a generic email account set up to receive only evidence messages. This approach ensures that a staff member's illness, vacation or termination does not impact the court's ability to function.

---

<sup>10</sup> See [FedRAMP Marketplace](#) for a list of vendors and products that meet Federal Information Security Management Act (FISMA) IT security requirements.

Evidence can be circulated to all appropriate parties via email. Email inbox “rules” can be used to automate the distribution of incoming email. This approach is only feasible when the quantity and size of files to be shared is small and security/privacy is not a concern.

## **Obstacles and Opportunities**

In many jurisdictions, paper is the court’s official record and wet signatures are still required. However, even many of these courts are operating under temporary rules that allow for digital processes. Identify points in the digital hearing process where document/process rule barriers exist. Then work toward permanent rule changes.

Some courts that were on a path to embracing or enhancing digital processes have been able to accelerate their efforts and adapt more quickly and comfortably to virtual hearings. Courts that still operate using paper are struggling with more than the burden of storing and moving documents, they are now dealing with very real safety concerns for the staff who must handle paper filings and evidence, as well as interface with the public directly. Some courts have only been able to address emergency matters during the pandemic, while more tech-savvy courts have been able to continue in new normal, albeit virtual, operations.

Courts can reduce the quantity of Personal Protective Equipment required to conduct operations safely while improving the court’s efficiency and public service by adopting digital processes. The pandemic presents a compelling case for the advantages of digital processes and an urgency for adopting current technologies and moving permanently away from handling paper.

## **Conclusion**

As courts look at long term evidence management solutions, consideration should be given to the needs of SRLs, data security and privacy, authentication, and methods for protecting the integrity of submissions. The court’s ability and willingness to support users in submitting evidence digitally, as well as the court’s official record and signature requirements are additional considerations.

Widely available technology tools and platforms are being used successfully to share digital evidence and facilitate virtual hearings. Best practices are emerging. Courts are not merely enduring the COVID-19 pandemic crisis; many are embracing the technologies and processes commonly used in other sectors both public and private. Courts are continuing to function during challenging circumstances, and are finding virtual processes not only manageable, but increasingly advantageous.

For more information, contact NCSC at [technology@ncsc.org](mailto:technology@ncsc.org).



## Appendix A - Resources

The following virtual hearing resources include information on evidence management that may be useful for discussion.

Michigan Law Help	<a href="#">What to expect at a virtual hearing</a>
Texas Judicial Branch	<a href="#">Court Coronavirus Information</a>
Texas Access to Justice Commission	<a href="#">Best Practices for Courts in Zoom Hearings Involving Self Represented Litigants</a>
Michigan Courts	<a href="#">Resources for Self-Represented Litigants</a>
Florida Supreme Court	<a href="#">Management of Evidence in Remote Hearings in Civil and Family Cases</a>
Florida Supreme Court	<a href="#">Best Practices: Facilitating Remote Appearance Technology For The Court And The Litigants In The Domestic Relations Divisions</a>
Library of Congress Law Library	<a href="#">Virtual Civil Trials</a>
Illinois, 17th Judicial Circuit	<a href="#">Procedure for Virtual Hearings - Family Division</a>
Louisiana State Bar Association	<a href="#">Virtual Court Hearings - Best Practices for Self-Represented Litigants</a>
District Court, Pueblo County (CO)	<a href="#">Webex Procedures – Pueblo County District Court Div. 501</a>
Supreme Court of Victoria (Australia)	<a href="#">Virtual Hearings - Tips and Tricks for Practitioners<sup>11</sup></a>
New York State Court System	<a href="#">Resources and Help for Litigants, Attorneys &amp; Agencies</a>

---

<sup>11</sup> Note that this court's information is clearly available in audio form to make it easily accessible for those who are visually impaired or have other disabilities.

# Appendix B - Sample Notice of Filing, Use and Submission of Exhibits for Virtual Hearing

## SUPERIOR COURT OF NEW JERSEY PASSAIC VICINAGE

CHAMBERS OF  
HON. SOHAIL MOHAMMED, J.S.C.



Passaic County Courthouse  
77 Hamilton Street  
Paterson, NJ 07505  
Office: (973) 653-2910 ext. 24555

April 8, 2020

### NOTICE

#### **FILING, USE AND/OR SUBMISSION OF EXHIBITS FOR JUDGE MOHAMMED'S VIRTUAL COURTROOM SESSION**

In order to ensure that the Court, court staff, counsel, and other parties have access to electronically filed and/or submitted exhibits, the following requirements apply to their filing, submission and use in a Virtual Courtroom proceeding before the Hon. Sohail Mohammed, J.S.C.

#### **1. Protocol for Pre-Hearing Submission of Evidentiary Exhibits**

- a. The submission of the Electronic evidence files should normally occur after the parties are reasonably sure that the lists are complete to avoid a piecemeal submission of files to the Court.
- b. Counsel or moving party must pre-mark all Evidentiary exhibits – documentary, audio, video – using the following naming convention. State Exhibit: S-1; Defense Exhibit: D-1; Joint Exhibit: J-1; Court Exhibit: C-1.
- c. File Type Requirements - All Electronic exhibits are to be submitted only in these formats

Exhibit Types	Allowable File Types
Documents	.pdf
Images, Pictures	.jpg, gif, .png, .pdf
Audio Recordings	.avi, .mpg, .mp3, .mp4
Video Recordings	.avi, .mpg, .mp3, .mp4

- d. Exhibit files are not to be encoded with any proprietary software, and they must be readable by computers running Microsoft Windows software without the need to install any additional proprietary tools.