



PSYCHCE

Technology in Forensic Psychological Evaluations: Ethical and Practical Guidelines



Section 1: Introduction to Technology in Forensic Psychological Evaluations	8
Introduction.....	8
Evolution of Technology in Forensic Psychology.....	9
Growth of Tele-Forensic Services	11
Benefits of Technology in Forensic Evaluations	12
Limitations and Challenges of Technology Integration	12
Impact of COVID 19 on Technology Adoption	13
Summary	14
Section 2: Overview of Technology Used in Forensic Settings	14
Telehealth and Videoconferencing Platforms.....	14
Digital Psychological Testing and Assessment Software	17
Electronic Records and Documentation Systems	18
Remote Behavioral Observation Tools.....	19
Secure Communication Platforms	20
Digital Collateral Information Collection	20
Integration of Multiple Technologies in Forensic Workflow	21
Challenges in Technology Selection and Use	22
Summary	22
Section 3: APA Guidelines and Professional Standards in Technology Mediated Forensic Evaluations	23
Introduction.....	23
APA Ethical Principles and Code of Conduct.....	24
Specialty Guidelines for Forensic Psychology	25
APA Telepsychology Guidelines	26
Continuing Education and Competence in Technology Use	27

Application of Standards in Forensic Technology Use	28
Risk Management and Professional Responsibility	28
Summary	29
Section 4: Ethical Considerations in Technology Mediated Forensic Evaluations ...	30
Introduction.....	30
Confidentiality and Privacy in Remote Forensic Practice.....	31
Informed Consent for Technology Mediated Forensic Evaluations	32
Competence in the Use of Technology	33
Data Security and Digital Protection.....	35
Identity Verification and Authenticity of Participation	36
Third Party Presence and Undue Influence	36
Recordings, Digital Evidence, and Record Keeping.....	37
Cross Jurisdictional and Regulatory Concerns	38
Equity, Access, and Fairness	39
Ethical Decision Making in Practice	39
Summary	40
Section 5: Legal and Jurisdictional Considerations in Technology Mediated Forensic Evaluations.....	41
Introduction.....	41
Legal Standards for Admissibility of Forensic Evidence	41
Impact of Technology on Legal Defensibility	42
Licensing and Cross Jurisdictional Practice.....	43
Jurisdictional Issues in Court Proceedings.....	44
Documentation and Record Keeping Requirements	45
Risk Management in Legal Contexts.....	46

Case Example.....	46
Summary	47
Section 6: Assessment Validity and Reliability in Technology Mediated Forensic Evaluations.....	48
Construct Validity	48
Criterion Validity.....	49
Performance Validity and Response Bias.....	49
Reliability in Forensic Psychology and Technology	50
Measurement Equivalence Between Remote and In-Person Assessments.....	52
Rapport and Interpersonal Dynamics.....	53
Environmental Factors and Contextual Influences	53
Identity Verification and Test Integrity	55
Technological Factors Affecting Data Quality	55
Strategies to Enhance Validity and Reliability.....	56
Case Example.....	57
Summary	57
Section 7: Digital Psychological Testing and Assessment Tools in Forensic Evaluations.....	58
Introduction.....	58
The Meaning of Digital Testing in Forensic Practice	59
Categories of Digital Assessment Tools in Forensic Settings.....	60
Digital Administration of Personality and Psychopathology Measures	61
Digital Symptom Validity and Performance Validity Assessment	63
Cognitive and Neuropsychological Testing in Digital and Remote Formats.....	64
Structured Risk Assessment and Digital Decision Support	65

Projective and Performance Based Methods in Digital Contexts	66
Test Security, Standardization, and Examinee Behavior	67
Best Practical Practices for Forensic Use of Digital Assessment Tools	68
Summary	69
Section 8: Practical Implementation and Workflow Integration in Technology Mediated Forensic Evaluations	70
Introduction.....	70
Workflow Design in Technology Mediated Forensic Practice	70
Platform Selection and Technical Considerations.....	71
Client Preparation and Technology Readiness.....	72
Managing the Remote Evaluation Session	72
Contingency Planning and Backup Procedures	73
Documentation and Workflow Consistency	74
Summary	74
Section 9: Confidentiality and Data Security Best Practices	74
Introduction.....	74
Principles of Data Security in Forensic Practice	75
Encryption and Secure Communication	75
Secure Storage and Access Control	76
Data Retention and Disposal	76
Breach Response and Risk Management.....	76
Summary	77
Section 10: Tele-Forensic Interviewing Techniques	77
Introduction.....	77
Foundations of Tele-Forensic Interviewing.....	78

Rapport Development in Remote Contexts.....	78
Structuring the Tele-Forensic Interview	79
Behavioral Observation in Tele-Forensic Interviews.....	79
Cultural and Accessibility Considerations.....	80
Summary	81
Section 11: Case Examples and Applied Decision-Making in Technology Mediated Forensic Evaluations	81
Introduction.....	81
Case 1: Competency to Stand Trial Evaluation	81
Case 2: Child Custody Evaluation.....	82
Case 3: Personal Injury Evaluation.....	82
Case 4: Disability Evaluation.....	83
Case 5: Ethical Dilemma in Remote Evaluation	83
Decision-Making Framework.....	84
Summary	84
Section 12: Artificial Intelligence and Emerging Technologies in Forensic Evaluations.....	84
Introduction.....	84
Applications of Artificial Intelligence in Forensic Psychology	85
Benefits of AI and Digital Technologies	85
Limitations and Risks	86
Ethical Considerations	86
Summary	87
Section 13: AI in the Forensic Opinion: What the Evaluator Must Be Able to Defend	87

Introduction.....	87
Daubert and the Admissibility of AI-Assisted Forensic Opinions.....	88
Cross-Examination and Methodological Accountability	89
Algorithmic Bias and Racial Disparities in Risk Assessment	91
Professional Responsibility and Forensic Judgment	92
Summary	93
Section 14: Cultural Competence, Equity, and Access in Technology-Mediated Forensic Evaluations	93
Introduction.....	93
Expanding the Definition of Culture in Digital Contexts.....	94
Language, Communication, and Interpretation.....	95
Socioeconomic Barriers and Access to Technology	95
Addressing Bias in Technology and Assessment Tools.....	96
Strategies for Promoting Equity.....	96
Case Example.....	97
Summary	97
Section 15: Documentation, Report Writing, and Testimony in Technology-Mediated Forensic Practice	97
Introduction.....	97
Comprehensive Documentation Practices	98
Report Writing in Technology-Mediated Evaluations	98
Addressing Limitations and Methodological Considerations	99
Testimony and Legal Scrutiny	99
Case Example.....	100
Summary	100

Section 16: Future Directions, Emerging Trends, and Continuing Competence ...	100
Introduction.....	100
Emerging Technologies in Forensic Practice	102
Integration of AI and Human Judgment	103
Ethical and Regulatory Developments.....	104
What Psychologists Should Do Now to Prepare	106
Case Example.....	107
Summary	108
References	109



Section 1: Introduction to Technology in Forensic Psychological Evaluations

Introduction

Technology has rapidly transformed forensic psychological practice over the past decade. Forensic psychologists increasingly rely on telehealth platforms, electronic record systems, digital testing tools, and remote data collection methods to conduct evaluations across civil, criminal, and administrative legal contexts. These technological advancements have expanded access to forensic services, improved efficiency, and created new opportunities for assessment. However, the integration of technology also introduces complex ethical, legal, and methodological considerations that must be carefully addressed to maintain validity, reliability, and defensibility in forensic evaluations. Consider three scenarios that illustrate the range of challenges this course addresses.

A forensic psychologist is retained to conduct a criminal responsibility evaluation via secure videoconferencing. Before the session begins, the defense attorney informs the psychologist that they intend to remain visible on camera throughout the entire evaluation. The psychologist must now navigate competing obligations — the attorney's legitimate interest in the process, the standardization requirements of the assessment, the examinee's candor and response style, and the objectivity that forensic practice demands. No technical failure has occurred. The ethical complexity begins before a single question is asked.

A psychologist conducting a child custody evaluation in a high-conflict divorce case uses an AI-assisted documentation tool to generate session summaries. Neither parent was informed during the consent process that AI tools would be used or

that their disclosures would be processed through a third-party platform. Opposing counsel subpoenas the documentation workflow records.

A psychologist completes a remote fitness for duty evaluation for an employee referred by their employer. Following the evaluation, the employer's legal team requests a copy of the raw session recording, citing their status as the retaining party. The psychologist must now weigh the employer's contractual claim against the examinee's privacy interests, the confidentiality of test materials visible during the session, and the professional obligations that govern record disclosure — none of which were fully anticipated in the original informed consent discussion.

None of these scenarios involve bad intentions. All three represent real practice decisions that licensed forensic psychologists face with increasing frequency and with limited formal guidance. This course provides the framework to navigate them.

Recent research indicates that the use of telepsychology and digital assessment tools in forensic settings has increased significantly, particularly following the COVID 19 pandemic, which accelerated adoption across courts, correctional systems, and private forensic practice (Bernhard et al., 2021; Skala et al., 2023; Kennedy et al., 2023). Courts, attorneys, and evaluators now routinely utilize remote technologies for competency evaluations, child custody assessments, disability evaluations, and risk assessments. This shift has fundamentally altered the practice of forensic psychology and highlights the importance of understanding best practices for technology integration.

Evolution of Technology in Forensic Psychology

Technology has long played a role in psychological assessment, but its integration into forensic psychology has accelerated significantly within the past decade. Early forms of technology use in forensic psychology primarily involved electronic

record keeping and computerized scoring of psychological tests. Over time, technological advances expanded to include videoconferencing, remote interviewing, digital behavioral monitoring, and electronic data sharing.

Recent literature indicates that technological advancements have reshaped forensic practice by allowing psychologists to conduct evaluations across geographic boundaries and provide services in previously underserved areas (Kirschstein & Singh, 2023). Telehealth technologies allow forensic psychologists to evaluate individuals in correctional facilities, hospitals, rural communities, and international settings without requiring physical travel. These developments have improved efficiency and reduced delays in legal proceedings.

The expansion of remote technology has also influenced the types of forensic evaluations conducted. For example, remote competency to stand trial evaluations have become increasingly common, particularly in jurisdictions with limited access to forensic evaluators. Studies indicate that remote competency evaluations can be conducted effectively when appropriate safeguards are implemented, including identity verification, test security measures, and environmental controls (Torres et al., 2021).

In addition to telehealth platforms, digital record review has become a standard component of forensic evaluations. Forensic psychologists frequently review electronic medical records, educational records, legal documents, and collateral information stored in digital formats. Electronic record systems allow evaluators to access large volumes of data efficiently and integrate multiple sources of information into forensic opinions.

Digital psychological testing has also expanded in forensic practice. Many commonly used forensic assessment instruments are now available in digital formats, including personality assessments, symptom validity measures, and structured risk assessment tools. Digital administration allows for automated

scoring, improved accuracy, and standardized administration procedures. However, research emphasizes that remote administration may affect test performance and must be conducted carefully to preserve validity (Palfreman, 2023).

Growth of Tele-Forensic Services

Tele-forensic services have expanded rapidly in recent years. Surveys of forensic psychologists indicate that telepsychology use increased dramatically following the COVID 19 pandemic and has remained common in many settings (Bernhard et al., 2021; Skala et al., 2023). Courts, correctional systems, and attorneys increasingly accept remote evaluations as part of routine forensic practice.

Studies also indicate that tele forensic services improve access to specialized forensic expertise. Rural and underserved areas often lack qualified forensic psychologists. Remote technology allows evaluators to provide services across jurisdictions and reduce delays in legal proceedings (Kirschstein & Singh, 2023).

For example, a rural jurisdiction may require a competency evaluation for a defendant in custody. Without remote technology, the individual might wait several weeks or months for an evaluator to travel to the facility. Telehealth platforms allow the evaluation to be conducted more quickly, reducing delays and improving legal efficiency.

Similarly, remote child custody evaluations allow evaluators to observe parents and children in home environments, which may provide additional ecological validity. However, research also highlights concerns regarding privacy, environmental distractions, and technological limitations during remote evaluations (Kennedy et al., 2023).

Benefits of Technology in Forensic Evaluations

Technology offers several benefits in forensic psychological evaluations. One of the most significant advantages is increased access to services. Remote technology allows psychologists to conduct evaluations in rural areas, correctional facilities, hospitals, and other settings that may be difficult to access in person.

Another major benefit is improved efficiency. Remote evaluations reduce travel time, scheduling difficulties, and logistical barriers. This efficiency can lead to faster completion of evaluations and reduced delays in legal proceedings.

Technology also improves documentation and data management. Digital records allow evaluators to organize information, track data, and maintain documentation more effectively. Electronic systems also facilitate collaboration with attorneys, courts, and other professionals.

Remote technology may also reduce safety risks. In some forensic settings, in person evaluations may involve individuals with histories of violence or unstable behavior. Remote evaluations allow psychologists to conduct assessments while maintaining physical safety.

Additionally, remote observation technology may enhance ecological validity in certain situations. For example, observing a parent interacting with a child in a home environment may provide valuable information that differs from office-based observations.

Limitations and Challenges of Technology Integration

Despite the benefits of technology, significant limitations and challenges must be considered. One major concern is the potential impact on assessment validity and reliability. Remote evaluations may affect rapport, behavioral observation, and

test performance. Environmental distractions, poor internet connections, and technological difficulties may influence results.

Research also indicates that remote testing may introduce additional risks, including coaching, unauthorized assistance, and compromised test security (Skala et al., 2023). Forensic psychologists must implement safeguards to reduce these risks, such as monitoring the testing environment and verifying participant identity.

Confidentiality is another major concern. Remote evaluations may be conducted in home environments where privacy cannot be fully controlled. Family members or other individuals may be present during evaluations, potentially influencing responses or compromising confidentiality.

Some individuals may have limited familiarity with technology, which may affect participation in remote evaluations. For example, older adults or individuals with cognitive impairments may struggle with videoconferencing platforms.

Connectivity issues also present challenges. Poor internet connections may disrupt interviews, reduce audio quality, and limit behavioral observation. These issues may affect the accuracy of forensic evaluations.

Legal admissibility is another consideration. Courts may question the validity of remote evaluations, particularly when assessment tools were not originally designed for remote administration. Forensic psychologists must document limitations and justify their methodology.

Impact of COVID 19 on Technology Adoption

The COVID 19 pandemic accelerated the adoption of technology in forensic psychology. Courts, correctional facilities, and forensic practitioners rapidly

transitioned to remote evaluation methods. This shift created new opportunities and challenges.

Studies indicate that many forensic psychologists adopted telehealth technology for the first time during the pandemic. Following the pandemic, many practitioners continued using remote methods due to increased efficiency and acceptance by courts (Bernhard et al., 2021). The pandemic also prompted the development of new guidelines and recommendations for remote forensic evaluations. These guidelines emphasize ethical considerations, validity concerns, and documentation requirements.

Summary

Technology has become an integral component of modern forensic psychological practice. Remote evaluations, digital testing, and electronic record systems are increasingly common. These technologies offer significant benefits, including improved access, efficiency, and safety. However, they also introduce challenges related to validity, confidentiality, and legal defensibility.

Section 2: Overview of Technology Used in Forensic Settings

Telehealth and Videoconferencing Platforms

Research indicates that videoconferencing has become a standard method for delivering forensic mental health services, particularly in correctional and rural settings (Knight et al., 2024). The primary issue in selecting a videoconferencing platform for forensic practice is whether the platform satisfies forensic-grade standards for confidentiality, data security, reliability, and defensibility in legal

proceedings. Forensic evaluations often involve highly sensitive legal information, criminal history data, competency findings, custody recommendations, or opinions regarding violence risk. As a result, psychologists must evaluate whether a platform complies with applicable privacy regulations, supports secure data transmission, and minimizes risks related to unauthorized access, recording, or interception of confidential information. The consequences of selecting an inadequate platform can be substantial, including breaches of confidentiality, compromised assessment validity, ethical complaints, exclusion of evidence, or legal challenges to the credibility of the evaluation itself.

Clinical decision-making regarding platform selection requires psychologists to conduct a systematic analysis of security, functionality, and forensic applicability. Key considerations include end-to-end encryption standards, data storage practices, authentication requirements, business associate agreements where applicable, waiting room controls, session access restrictions, and the platform's policies regarding recording or third-party data retention. Psychologists must also evaluate whether the platform allows for adequate observation of verbal and nonverbal behavior, sufficient audio and visual clarity, and stable connectivity throughout the evaluation. In forensic contexts, subtle behavioral indicators such as response latency, psychomotor agitation, affective shifts, eye movement patterns, or signs of external coaching may have substantial interpretive importance. A platform that produces lag, distortion, or intermittent connectivity may interfere with the evaluator's ability to make accurate observations and can therefore undermine the reliability of clinical conclusions.

The legal consequences of inadequate technology selection can be significant. If confidential information is exposed through insecure platforms or unauthorized recordings, psychologists may face ethical complaints, licensing board investigations, civil liability, or court scrutiny regarding professional competence. Opposing counsel may also challenge the validity of the evaluation by arguing that

technological limitations compromised behavioral observation, interfered with standardized administration procedures, or created opportunities for outside influence. For example, in competency to stand trial evaluations, failure to detect that an examinee was receiving prompts from an off-camera individual could directly affect the integrity of forensic conclusions. Similarly, poor audiovisual quality during a child custody evaluation may prevent accurate assessment of parent-child interactions, emotional reciprocity, or behavioral control. These concerns highlight why forensic psychologists must approach technology selection as a core component of assessment methodology rather than as a purely administrative or logistical decision.

Psychologists must also recognize that not all platforms marketed as “secure” are appropriate for forensic use. Some commercially available telecommunication platforms may retain metadata, permit unauthorized recording, or lack adequate encryption protections. Others may not provide sufficient control over participant access or session monitoring. Forensic evaluators are therefore ethically obligated to understand the technological limitations of the systems they use and to remain informed about evolving standards in digital privacy and cybersecurity. This responsibility is consistent with the APA Ethical Principles of Psychologists and Code of Conduct (2017), which require psychologists to practice within their boundaries of competence and to take reasonable precautions to protect confidential information. Ongoing training in tele-forensic practice, cybersecurity awareness, and digital risk management is increasingly necessary as technology becomes more deeply integrated into forensic assessment procedures.

In practice, forensic psychologists should develop standardized protocols for telehealth evaluations that include pre-session verification procedures, informed consent specific to remote assessment, environmental scans to reduce coaching or interference, contingency plans for technological disruption, and documentation of any technical limitations that may affect interpretation. These

procedures strengthen transparency and enhance the defensibility of forensic opinions. Courts increasingly expect evaluators to demonstrate not only clinical competence, but also competence in the technological systems used to conduct assessments. Accordingly, platform selection should be conceptualized as a professional judgment decision directly tied to ethical compliance, methodological rigor, and the overall integrity of the forensic evaluation process.

The integration of technology into forensic psychological practice involves a broad range of tools that support evaluation, data collection, communication, and documentation. These technologies have become essential components of modern forensic assessments, allowing psychologists to conduct evaluations remotely, manage large volumes of information, and utilize standardized testing procedures in digital formats. Understanding the types of technology used in forensic settings is critical for maintaining assessment quality, ensuring ethical compliance, and supporting defensible conclusions in legal contexts.

Recent research indicates that forensic psychologists increasingly rely on a combination of telecommunication platforms, digital assessment tools, and electronic data systems to conduct evaluations. These technologies are not limited to remote interviewing but extend to every phase of the forensic process, including intake, assessment, collateral data collection, analysis, and report preparation (Perle et al., 2025; Geraldo et al., 2024). As technology continues to evolve, psychologists must develop competency in selecting, using, and evaluating these tools in a manner consistent with professional standards.

Digital Psychological Testing and Assessment Software

Digital psychological testing tools are another key component of technology in forensic settings. These tools include computerized versions of standardized psychological assessments, automated scoring systems, and online data collection

platforms. Many widely used instruments, such as personality inventories and symptom validity tests, are now available in digital formats.

Digital testing platforms offer several advantages. They allow for standardized administration, reduce the risk of scoring errors, and facilitate efficient data collection. Automated scoring systems can generate results quickly and provide detailed reports that support clinical interpretation. Research indicates that digital administration can produce results comparable to traditional methods when appropriate procedures are followed (Giromini et al., 2024).

However, digital testing also presents challenges. Test security is a significant concern, as remote administration may increase the risk of unauthorized access to test materials or external assistance. Psychologists must implement safeguards to ensure that assessments are conducted under appropriate conditions. In addition, not all psychological tests are validated for remote administration, and the use of such tools must be supported by empirical evidence.

Electronic Records and Documentation Systems

Electronic records systems play a critical role in forensic psychological practice. These systems allow psychologists to store, organize, and retrieve information related to evaluations. Electronic records may include clinical notes, assessment results, legal documents, medical records, and collateral information.

The use of electronic records enhances efficiency by allowing psychologists to access large volumes of data quickly. It also supports accurate documentation and facilitates the integration of multiple data sources into forensic reports. Research highlights that digital record systems improve data management and support more comprehensive evaluations (Wibberly, 2024). For example, in a child custody evaluation, a psychologist may review electronic records that include school reports, medical histories, and prior legal documents. These records can be

accessed and organized within a digital system, allowing the psychologist to identify patterns and inconsistencies across sources.

Security is a critical consideration when using electronic records. Psychologists must ensure that data is stored securely and protected from unauthorized access. This includes the use of encryption, secure passwords, and compliance with privacy regulations. Proper record keeping is also essential for maintaining transparency and supporting the defensibility of forensic findings.

Remote Behavioral Observation Tools

Remote behavioral observation is an important aspect of forensic evaluations. Technology allows psychologists to observe behavior in real time through videoconferencing or through recorded sessions. In some cases, remote observation may provide unique insights that are not available in traditional settings. For example, in a child custody evaluation, a psychologist may observe parent child interactions in the home environment using a videoconferencing platform. This can provide valuable information about family dynamics, parenting practices, and the child's behavior in a natural setting. Research suggests that such observations may enhance ecological validity when conducted appropriately (Procaccia et al., 2024).

In correctional settings, remote observation tools may be used to monitor behavior during competency evaluations or risk assessments. Psychologists can observe interactions, emotional responses, and behavioral patterns without being physically present.

However, remote observation also has limitations. The psychologist's field of view may be restricted, and important contextual factors may be missed. In addition, the presence of cameras may influence behavior, and individuals may modify their

actions due to awareness of being observed. These factors must be considered when interpreting observational data.

Secure Communication Platforms

Secure communication platforms are essential for maintaining confidentiality in forensic evaluations. These platforms include encrypted email systems, secure messaging applications, and file sharing services. They allow psychologists to communicate with attorneys, courts, and other professionals while protecting sensitive information.

Secure communication is particularly important in forensic contexts, where information may have legal implications. Psychologists must ensure that all communications comply with privacy regulations and ethical standards. This includes using platforms that provide end-to-end encryption and secure data storage. For example, a forensic psychologist may use a secure file sharing system to send a report to an attorney. The system ensures that the document is protected during transmission and can only be accessed by authorized individuals. Similarly, secure messaging platforms may be used to coordinate scheduling or discuss case related information.

The use of non-secure communication methods, such as standard email or public messaging platforms, may pose risks to confidentiality. Psychologists must carefully evaluate the security features of communication tools and select those that meet professional and privacy standards.

Digital Collateral Information Collection

Collateral information is a critical component of forensic evaluations. Technology has expanded the ways in which psychologists can collect and analyze collateral

data. Digital sources may include electronic medical records, educational databases, legal documents, social media content, and other online information.

The use of digital collateral data allows psychologists to access a wide range of information quickly and efficiently. This can enhance the comprehensiveness of evaluations and support more accurate conclusions. Research indicates that digital data collection is increasingly integrated into forensic practice and contributes to more thorough assessments (Young, 2024).

There are also risks associated with digital collateral data. Information obtained from online sources may be incomplete, inaccurate, or misleading. Psychologists must evaluate the reliability and validity of such data and avoid overreliance on unverified information. Ethical considerations related to privacy and consent must also be addressed.

Integration of Multiple Technologies in Forensic Workflow

In practice, forensic psychologists typically use multiple technologies in combination rather than relying on a single tool. A comprehensive evaluation may involve videoconferencing for interviews, digital platforms for test administration, electronic systems for record review, and secure communication tools for information sharing.

For example, a forensic evaluation may begin with the review of electronic records, followed by a remote interview conducted through a videoconferencing platform. The psychologist may then administer digital assessment tools and collect additional collateral information through secure channels. Finally, the evaluation is documented using electronic record systems and shared with relevant parties.

This integrated approach allows psychologists to conduct thorough and efficient evaluations. However, it also requires careful coordination and attention to detail. Each component of the technological process must be managed in a way that supports validity, reliability, and ethical practice.

Challenges in Technology Selection and Use

Selecting appropriate technology for forensic evaluations involves several considerations. Psychologists must evaluate the functionality, security, and reliability of each tool. They must also consider the specific requirements of the evaluation, including the type of assessment, the characteristics of the examinee, and the legal context.

Research emphasizes that not all technologies are equally suitable for forensic use. Some platforms may lack necessary security features, while others may not support standardized assessment procedures (Geraldo et al., 2024). Psychologists must be able to critically evaluate available tools and select those that align with professional standards.

In addition, ongoing training is essential. Technology is constantly evolving, and psychologists must remain informed about new developments and best practices. This includes understanding updates to telehealth platforms, advancements in digital assessment tools, and changes in legal and ethical guidelines.

Summary

Technology used in forensic settings encompasses a wide range of tools, including telehealth platforms, digital testing software, electronic records systems, remote observation tools, secure communication platforms, and digital data collection methods. These technologies have transformed forensic practice by improving

access, efficiency, and data management. At the same time, each type of technology introduces specific challenges related to security, validity, and ethical use. Forensic psychologists must develop competency in selecting and using these tools while maintaining adherence to professional standards. Understanding the strengths and limitations of each technology is essential for conducting accurate and defensible evaluations.

Section 3: APA Guidelines and Professional Standards in Technology Mediated Forensic Evaluations

Introduction

The use of technology in forensic psychological evaluations requires strict adherence to established professional and ethical standards. Unlike general clinical practice, forensic psychology operates within a legal framework where the consequences of evaluation outcomes directly affect judicial decisions. As a result, the integration of telehealth, digital assessment tools, and electronic data systems must align with the American Psychological Association ethical principles, specialty forensic guidelines, and telepsychology standards.

Recent literature emphasizes that technology does not alter the fundamental ethical obligations of psychologists, but it does introduce new complexities in how those obligations are implemented (Perle et al., 2025; Sablone et al., 2024). Issues such as confidentiality, informed consent, competence, and documentation must be reconsidered in the context of remote and digital environments. Psychologists must ensure that their use of technology maintains the integrity, validity, and legal defensibility of forensic evaluations.

APA Ethical Principles and Code of Conduct

The APA Ethical Principles of Psychologists and Code of Conduct provides the foundation for ethical practice in all areas of psychology, including forensic work. Although the Ethics Code is not specific to telepsychology, its principles apply fully to technology mediated services. Key ethical principles include beneficence and nonmaleficence, fidelity and responsibility, integrity, justice, and respect for people's rights and dignity. In forensic contexts, these principles guide psychologists in maintaining objectivity, avoiding harm, and ensuring fairness.

Several specific standards are particularly relevant to technology use. Standard 2.01 requires psychologists to provide services within the boundaries of their competence. When using technology, this includes competence in telehealth platforms, digital testing tools, and data security practices. A psychologist who is unfamiliar with remote assessment procedures may risk compromising the quality of the evaluation.

Standard 3.04 addresses avoiding harm. Technology introduces risks such as breaches of confidentiality, misinterpretation of data, and reduced accuracy of observations. Psychologists must take reasonable steps to minimize these risks when conducting remote evaluations.

Standards 4.01 and 4.02 focus on confidentiality and informed consent. These standards require psychologists to protect sensitive information and ensure that individuals understand the nature and limits of the evaluation. In technology mediated contexts, this includes explaining risks related to data transmission, potential privacy limitations, and the use of digital platforms.

Standard 9.01 emphasizes the use of appropriate assessment methods. Psychologists must ensure that the tools and procedures they use are valid and reliable for the intended purpose. When using digital or remote assessments, this

requires careful evaluation of whether the method is supported by empirical evidence.

For example, if a psychologist administers a personality test remotely using an online platform, they must ensure that the test has been validated for remote use. If such validation is lacking, the psychologist must document the limitation and consider its impact on the evaluation.

Specialty Guidelines for Forensic Psychology

The Specialty Guidelines for Forensic Psychology provide additional direction specific to forensic practice. These guidelines emphasize the importance of impartiality, accuracy, and adherence to legal standards.

In the context of technology, the guidelines highlight several critical areas. One key principle is the importance of maintaining objectivity. Forensic psychologists must avoid bias and ensure that their use of technology does not introduce systematic errors. For example, differences in technology access or familiarity may affect examinee performance, potentially influencing results.

The guidelines also emphasize the importance of using appropriate methods and procedures. Psychologists must select assessment tools that are suitable for the specific forensic question and ensure that their methods are consistent with professional standards. When using technology, this includes evaluating whether remote procedures are appropriate for the type of evaluation being conducted.

Another important consideration is transparency. Forensic psychologists are expected to clearly document their methods, including any limitations associated with technology use. This documentation is essential for supporting the credibility and admissibility of forensic opinions.

For example, in a remote competency evaluation, the psychologist should document the platform used, the quality of the connection, any interruptions, and any environmental factors that may have influenced the assessment. This level of detail allows the court to evaluate the reliability of the findings.

APA Telepsychology Guidelines

The APA Guidelines for the Practice of Telepsychology provide specific guidance on the delivery of psychological services using telecommunications technologies. These guidelines are highly relevant to forensic practice, as they address issues such as competence, confidentiality, informed consent, and security.

One of the central principles of the telepsychology guidelines is the requirement for competence. Psychologists must have the necessary knowledge and skills to use technology effectively. This includes understanding how to operate telehealth platforms, manage technical issues, and adapt assessment procedures for remote delivery (Perle et al., 2025).

Confidentiality is another critical component. Telepsychology guidelines emphasize the importance of using secure platforms and implementing safeguards to protect data. Psychologists must ensure that communication is encrypted and that sensitive information is stored securely.

Informed consent in telepsychology requires additional considerations. Individuals must be informed about the nature of the technology being used, potential risks to confidentiality, and any limitations of remote assessment. This includes discussing issues such as internet security, potential interruptions, and the possibility of unauthorized access.

For example, a psychologist conducting a remote evaluation should explain to the examinee that while secure platforms are used, there is still a risk of data

breaches. The examinee should also be informed about the steps taken to minimize these risks.

The guidelines also address the importance of assessing the appropriateness of telepsychology for each case. Not all evaluations are suitable for remote delivery. Factors such as the complexity of the assessment, the characteristics of the examinee, and the availability of technology must be considered.

Continuing Education and Competence in Technology Use

APA continuing education standards emphasize the importance of maintaining professional competence through ongoing learning. In the context of technology, this includes staying informed about new tools, research findings, and best practices.

Research indicates that many psychologists received limited training in telepsychology prior to the rapid expansion of remote services (Wibberly, 2024). As a result, continuing education plays a critical role in ensuring that practitioners develop the necessary skills.

Competence in technology use involves several components. Psychologists must understand the technical aspects of the tools they use, including platform functionality and security features. They must also be able to evaluate the appropriateness of technology for specific forensic tasks.

In addition, psychologists must remain informed about evolving legal and ethical standards. As technology continues to develop, new guidelines and regulations may emerge. Continuing education ensures that practitioners remain compliant with these changes. This ongoing education supports high quality practice and reduces the risk of ethical violations.

Application of Standards in Forensic Technology Use

Applying APA standards to technology mediated forensic evaluations requires careful consideration of multiple factors. Psychologists must integrate ethical principles, forensic guidelines, and telepsychology standards into their practice.

One important application is in the area of informed consent. In a traditional in person evaluation, informed consent involves explaining the purpose of the evaluation, the limits of confidentiality, and the potential use of the results. In a remote evaluation, additional information must be provided regarding the use of technology.

Another application involves confidentiality. Psychologists must ensure that all communications and data storage methods are secure. This may involve using encrypted platforms, secure file sharing systems, and password protected devices.

Assessment validity is also a key consideration. Psychologists must evaluate whether remote methods are appropriate for the specific assessment and whether they may affect the results. If limitations are identified, they must be clearly documented.

Risk Management and Professional Responsibility

Risk management is an essential component of forensic practice. The use of technology introduces additional risks that must be addressed proactively.

One key strategy is thorough documentation. Psychologists should document all aspects of the evaluation process, including the technology used, any technical issues encountered, and any deviations from standard procedures. This documentation supports transparency and helps protect against legal challenges.

Another strategy is the use of secure technology. Psychologists should select platforms that meet established security standards and regularly update their systems to protect against vulnerabilities.

Professional responsibility also involves recognizing the limits of technology. Psychologists must be willing to modify their approach or decline to conduct a remote evaluation if it is not appropriate for the case.

Summary

APA ethical principles, forensic specialty guidelines, and telepsychology standards provide a comprehensive framework for the use of technology in forensic psychological evaluations. These standards emphasize competence, confidentiality, informed consent, and the use of appropriate assessment methods.

The integration of technology into forensic practice requires careful application of these principles. Psychologists must ensure that their use of digital tools supports valid and reliable assessments while maintaining compliance with ethical and legal standards.

Ongoing education and training are essential for developing competence in technology use. By adhering to APA guidelines and staying informed about emerging practices, forensic psychologists can effectively integrate technology into their work while maintaining the highest standards of professional practice.

Section 4: Ethical Considerations in Technology Mediated Forensic Evaluations

Introduction

Ethical practice is the core safeguard that allows technology to be used responsibly in forensic psychological evaluations. In forensic work, technology does not simply create convenience. It changes how information is gathered, how behavior is observed, how confidentiality is protected, and how professional decisions are justified. Because forensic opinions may influence liberty interests, parental rights, financial awards, competency determinations, and criminal responsibility findings, ethical errors in technology mediated practice can have serious consequences for examinees and for the legal system.

Recent scholarship consistently shows that technology use in forensic and related remote psychological services creates ethical demands in several major areas. These include confidentiality, privacy, informed consent, competence, data security, identity verification, environmental control, third party influence, record keeping, and jurisdictional practice limits (Geraldo et al., 2024; Perle et al., 2025; Young, 2024). The ethical question is not simply whether remote technology can be used. The ethical question is whether the psychologist can use it in a way that preserves fairness, accuracy, and professional integrity.

In an in person forensic evaluation, the psychologist usually controls the office environment, knows who is in the room, can monitor distractions, and can better manage privacy. In a remote setting, many of those controls are weakened. An examinee may be participating from a home, jail, hospital room, attorney's office, or other nonstandard environment. Others may be present off camera. Internet

interruptions may occur. Digital platforms may vary in security. These realities require the psychologist to think more deliberately and document more carefully.

Confidentiality and Privacy in Remote Forensic Practice

Confidentiality is one of the most important and most misunderstood issues in forensic assessment. In forensic work, confidentiality is already more limited than in treatment contexts because information is often intended for courts, attorneys, agencies, or other retaining parties. Technology adds another layer of complexity because privacy can be threatened both by the legal nature of the evaluation and by the method of communication.

In a remote evaluation, confidentiality can be compromised in multiple ways. The platform itself may be insecure. The examinee may be in a shared environment. Family members, correctional staff, attorneys, or others may be able to hear or influence the interaction. Sessions may be recorded without the evaluator's knowledge. Files may be stored on unsecured devices or transmitted through vulnerable systems. Research and professional guidance consistently identify these risks as central ethical concerns in telepsychology and remote forensic work (Geraldo et al., 2024; Sablone et al., 2024).

Forensic psychologists must therefore distinguish clearly between confidentiality and privacy. Confidentiality refers to the professional handling of information. Privacy refers to the conditions under which the communication occurs. A psychologist may correctly explain the legal limits of confidentiality, yet still conduct an ethically problematic evaluation if the examinee is speaking from a room where others can overhear sensitive material.

For example, consider a remote parenting capacity evaluation in which a parent joins from home while a new partner is in the next room. Even if that partner never appears on camera, the possibility that the parent's responses are being

influenced by that person affects privacy, candor, and the integrity of the evaluation. Similarly, in a correctional setting, a competency examinee may be interviewed via video in a space where officers are nearby. That arrangement may be unavoidable in some institutions, but it must be recognized as a limitation and addressed in the report.

Ethically sound practice requires psychologists to assess privacy before and during the session. This can include asking the examinee to scan the room with the camera, asking who is present, requiring use of headphones when feasible, and instructing the examinee to notify the evaluator if anyone enters the space. The psychologist should also explain that privacy cannot be assumed and that any concerns should be raised immediately. If privacy is clearly inadequate and cannot be improved, the psychologist should consider postponing or limiting the evaluation.

Informed Consent for Technology Mediated Forensic Evaluations

Informed consent is not a one time formality. In forensic telepractice, it is an active ethical process that must address both the general forensic nature of the evaluation and the specific risks created by technology. Research and current professional guidance emphasize that informed consent in remote practice should include clear explanation of technological risks, privacy limits, data handling procedures, possible interruptions, and procedures if the connection fails (Perle et al., 2025; Young, 2024).

In forensic settings, informed consent also requires careful explanation of role and purpose. Examinees must understand that the psychologist is acting as a forensic evaluator rather than a treating therapist, that the evaluation may not be confidential in the ordinary therapeutic sense, that findings may be disclosed to a retaining party or tribunal, and that the psychologist may not be providing

treatment recommendations in a therapeutic relationship. Technology does not replace these explanations. It increases the need for clarity because remote interactions can feel less formal and may create false assumptions about the nature of the relationship.

A proper informed consent discussion for a remote forensic evaluation should generally include the purpose of the evaluation, the party requesting the evaluation, who will receive the report, the limits of confidentiality, the technology being used, known risks to privacy and data security, expectations about the physical environment, procedures for confirming identity, policies regarding recording, and contingency plans for technical disruption.

In a remote criminal responsibility evaluation, the psychologist should explain that if the video connection fails during a critical portion of the interview, the interruption may affect the continuity of the assessment and may require rescheduling. The psychologist should also explain whether digital materials will be displayed on screen, how any test responses will be stored, and whether the examinee may or may not have anyone else present.

When the examinee has limited cognitive ability, low literacy, severe mental illness, or limited English proficiency, informed consent becomes even more ethically significant. Remote communication may make comprehension more difficult. The psychologist should use simple language, ask the examinee to explain their understanding in their own words, and document the steps taken to ensure meaningful understanding.

Competence in the Use of Technology

The ethical requirement of competence applies directly to the use of technology. A psychologist may be highly experienced in forensic evaluation yet still be insufficiently competent to conduct a technology mediated assessment if they do

not understand the platform, the security procedures, the limits of remote observation, or the validation status of remotely administered tools.

Current literature repeatedly emphasizes that competence in telepsychology is not just technical familiarity. It includes the ability to select appropriate technology, understand its limitations, assess the suitability of remote methods for a given referral question, manage privacy risks, and adapt procedures while preserving validity (Geraldo et al., 2024; Perle et al., 2025). In forensic contexts, competence also includes awareness of how remote procedures may affect legal defensibility.

A psychologist who knows how to start a video session but does not know whether the platform meets institutional privacy standards is not fully competent. A psychologist who administers a measure remotely without knowing whether remote administration changes interpretation is not fully competent. A psychologist who cannot detect when a remote examinee may be receiving off camera coaching is not fully competent for that task.

Competence also involves case selection. Not every case is appropriate for remote forensic assessment. Some examinees may have severe paranoia, profound cognitive impairment, acute psychosis, sensory limitations, or language needs that make remote evaluation inadequate or unfair. Ethical competence includes recognizing when technology is not the right method. An examinee with significant disorganization and intermittent responding may appear more impaired over unstable video than they would in person, or the opposite may occur if environmental distractions are hidden from the evaluator's view. A competent evaluator should be able to identify such risks and decide whether the method should be modified or abandoned.

Data Security and Digital Protection

Data security is one of the most concrete ethical issues in technology mediated forensic practice. Remote evaluations generate digital trails at nearly every step. Appointment links, digital forms, emails, text messages, audio or video streams, assessment data, and reports may all exist electronically. Each point of storage or transmission creates risk.

Professional guidance and recent literature emphasize the need for secure platforms, encryption, access controls, device protection, and clear policies about storage and transmission (Perle et al., 2025; Sablone et al., 2024). The evaluator must know where the data travels, where it is stored, who can access it, and how long it will be retained.

Ethical practice requires more than assuming that a platform is secure because it is popular. Psychologists should verify whether the platform offers appropriate encryption, whether institutional contracts or business associate agreements are required in the relevant setting, whether recordings are automatically created, and whether chat functions or cloud storage create additional risk.

Consider a civil forensic evaluator who conducts remote interviews and stores reports on a personal laptop without encryption. Even if the interviews themselves are competently conducted, the storage method creates serious ethical risk if the device is lost, hacked, or shared. Similarly, sending a forensic report through ordinary unsecured email may expose highly sensitive information. The legal and professional consequences of such breaches can be substantial.

Psychologists should also address security with examinees. They may need to instruct examinees not to use public Wi Fi, not to participate in a shared workspace, and not to record or screenshot assessment materials. These instructions should be part of informed consent and repeated when needed.

Identity Verification and Authenticity of Participation

One ethical challenge that is especially important in remote forensic work is confirming who is actually participating. Identity verification is essential because forensic opinions depend on accurate attribution of information. If the evaluator cannot be confident that the correct individual is present, the integrity of the evaluation is undermined.

Identity verification can involve visual confirmation of government issued identification, verification through institutional staff, cross checking demographic information, and documenting the steps used. In correctional or hospital settings, staff assistance may support identity confirmation. In private civil matters, additional caution may be needed.

Authenticity of participation goes beyond identity. The psychologist must consider whether the examinee is receiving assistance, consulting notes, reading prepared statements, or being coached by another person off camera. Remote environments make these possibilities more difficult to detect. Ethical practice requires active monitoring, direct questioning, and willingness to stop the evaluation if authenticity is in doubt. If an examinee repeatedly looks off screen before answering straightforward questions, whispers to someone nearby, or changes speaking style when the camera angle shifts, the evaluator should address these concerns directly. It may be appropriate to request a room scan, restate participation rules, or terminate the session if the integrity of the assessment cannot be preserved.

Third Party Presence and Undue Influence

Third party presence is a longstanding issue in forensic assessment, but technology has made it more common and more difficult to control. In remote settings, third parties may be visibly present, silently off camera, or involved

through technology itself. Family members may help the examinee connect. Attorneys may remain nearby. Institutional staff may monitor the interaction. Interpreters may join the session. Each additional person changes the ethical landscape.

The presence of a third party may affect candor, response style, emotional expression, and the examinee's sense of safety. It may also compromise standardization. In some circumstances, a third party may be necessary. An interpreter may be essential. A correctional staff member may be required for security. A support person may be necessary for an examinee with severe disability. Ethical practice does not demand a zero third party rule in every case. It demands careful analysis, disclosure, and documentation.

The evaluator should establish clear participation rules in advance and document any third party presence, including who was present, why, for how long, and how the presence may have affected the evaluation.

Recordings, Digital Evidence, and Record Keeping

Recording is an especially sensitive ethical issue in remote forensic practice. Many digital platforms make recording easy, automatic, or difficult to detect. Some participants assume that because the interaction is online, recording is acceptable. In forensic work, unauthorized recording can threaten confidentiality, expose test materials, and alter the behavior of participants.

The evaluator should have a clear policy on recording and communicate it explicitly during informed consent. If recording is not permitted, that rule should be stated plainly. If recording is required by court order, institutional policy, or other legal authority, the evaluator should address the implications for privacy, data security, and test integrity.

Record keeping must also reflect the realities of remote practice. Notes should include the technology platform used, date and time, participants present, identity verification steps, environmental observations, interruptions, privacy concerns, connection quality, and any deviations from typical procedure. This is not merely administrative detail. It is part of the ethical duty to be transparent and accurate.

Cross Jurisdictional and Regulatory Concerns

Technology often makes it easier to practice across geographic boundaries, but ethical permissibility does not automatically follow technological capability. A psychologist may be physically located in one jurisdiction while the examinee is in another. Laws, licensing requirements, and court expectations may differ. Ethical practice requires the psychologist to understand and comply with applicable jurisdictional rules.

Recent literature continues to identify cross jurisdictional practice as a major concern in telepsychology and forensic work (Perle et al., 2025; Sablone et al., 2024). The ethical problem is not only licensure. Different jurisdictions may vary in rules about privilege, mandated reporting, consent, minor participation, electronic records, and admissibility.

The evaluator must consider whether practice is legally authorized where the parent is located, whether additional permissions are needed, and whether the court's acceptance of the evaluation resolves or does not resolve professional regulatory obligations. Ethical practice requires not assumptions, but verification.

The same issue can arise in federal, military, correctional, or international settings. Technology broadens access, but it also broadens the need for regulatory diligence.

Equity, Access, and Fairness

Ethical forensic practice requires attention to fairness. Technology can improve access, but it can also produce inequity. Not all examinees have equal internet access, equal device quality, equal digital literacy, equal privacy in the home, or equal comfort with remote communication. These disparities can influence the evaluation process in ways that may be mistaken for psychological differences.

An examinee with unstable internet may appear distractible or disengaged when the issue is actually connectivity. An individual with limited experience using computers may perform poorly on digital tasks for reasons unrelated to the referral question. A person living in a crowded home may have less privacy and thus disclose less. Ethical practice requires the evaluator to recognize these contextual factors and avoid overinterpreting them as personal traits.

Psychologists should therefore assess technology access and literacy early, provide clear instructions, and document barriers that may affect performance. Equity is not achieved by using the same remote procedure for everyone. It is achieved by considering whether the procedure gives each examinee a fair opportunity to participate meaningfully.

Ethical Decision Making in Practice

Technology mediated forensic work often requires rapid ethical judgment. A strong ethical approach involves identifying the issue, reviewing relevant standards, considering alternatives, evaluating risks to fairness and validity, consulting when necessary, and documenting the rationale for the decision.

Suppose a psychologist begins a remote competency evaluation and suspects that correctional staff are intermittently listening outside the interview room. The ethical issue includes privacy, candor, and data quality. The psychologist should

address the concern in real time if possible, determine whether the setting can be improved, weigh whether the interview can continue, and document the circumstances and any limitations that resulted.

Or consider a parenting evaluation in which a parent requests that the session continue by phone only after the video fails. The ethical response depends on the referral question, the need for behavioral observation, the quality of information already obtained, and the significance of losing visual data. There is no automatic answer. Ethical decision making requires methodical reasoning, not convenience.

Summary

Ethical considerations in technology mediated forensic evaluations extend far beyond general telehealth etiquette. They shape whether an evaluation is fair, valid, secure, and professionally defensible. The major ethical domains include confidentiality, privacy, informed consent, competence, data security, identity verification, third party influence, record keeping, cross jurisdictional practice, and equitable access.

The responsible forensic psychologist does not treat technology as ethically neutral. Instead, the psychologist evaluates how each technological choice affects the examinee, the data, and the legal use of the final opinion. Strong ethical practice requires advance planning, active monitoring during the evaluation, clear documentation, and willingness to limit or discontinue remote procedures when the integrity of the evaluation cannot be maintained.

As technology becomes more common in forensic work, ethical discipline becomes more important, not less. The psychologist who can explain both the advantages and the limits of remote practice, and who documents those considerations carefully, is better positioned to protect examinees, inform courts accurately, and uphold professional standards.

Section 5: Legal and Jurisdictional Considerations in Technology Mediated Forensic Evaluations

Introduction

The integration of technology into forensic psychological evaluations introduces complex legal and jurisdictional considerations that extend beyond traditional in person practice. Forensic psychologists must ensure that their work not only meets professional and ethical standards but also satisfies legal requirements for admissibility, licensure, and procedural fairness. Because forensic evaluations are often scrutinized in court, any deviation from accepted legal standards can undermine the credibility and utility of the evaluation.

Technology mediated evaluations raise important legal questions regarding admissibility of evidence, cross jurisdictional practice, licensing requirements, and documentation standards. Courts increasingly accept remote evaluations, but acceptance is not automatic. Instead, admissibility depends on whether the evaluation methods meet established legal criteria and whether the psychologist can demonstrate that the use of technology did not compromise reliability or fairness (Young, 2024; Perle et al., 2025).

Legal Standards for Admissibility of Forensic Evidence

One of the most critical legal considerations in forensic psychology is whether an evaluation will be admitted as evidence in court. In many jurisdictions, admissibility is governed by standards such as the Daubert standard or related evidentiary rules. These standards require that expert testimony be based on reliable methods, sufficient data, and sound scientific principles.

Under the Daubert framework, courts evaluate several factors, including whether the method has been tested, whether it has been subjected to peer review, its known error rate, and its general acceptance within the relevant professional community. Technology mediated forensic evaluations must meet these same criteria.

The use of remote assessment methods introduces additional scrutiny. Courts may question whether videoconferencing, digital testing, or remote observation affects the reliability of the evaluation. Research indicates that while many remote methods are comparable to in person procedures, the psychologist must be prepared to justify their use and explain any limitations (Eddy, 2025; Young et al., 2025).

For example, if a psychologist conducts a criminal responsibility evaluation using videoconferencing, opposing counsel may challenge whether the method allowed for adequate observation of the defendant's behavior. The psychologist must be able to explain how the technology was used, why it was appropriate, and how any limitations were addressed.

Similarly, the use of digital psychological tests may be challenged if the test has not been validated for remote administration. In such cases, the psychologist must either provide evidence supporting the method or acknowledge limitations and explain how they affect interpretation.

Impact of Technology on Legal Defensibility

Legal defensibility refers to the ability of a forensic evaluation to withstand scrutiny in legal proceedings. Technology can both enhance and undermine defensibility depending on how it is used.

On one hand, digital tools can improve documentation, provide accurate records, and allow for efficient data management. On the other hand, technological limitations may introduce uncertainty regarding the accuracy and completeness of the evaluation.

Courts often examine whether the evaluation process was conducted in a manner consistent with professional standards. This includes evaluating whether the psychologist used appropriate methods, maintained objectivity, and documented procedures adequately. When technology is involved, additional factors may be considered, such as the quality of the video connection, the security of the platform, and the conditions under which the evaluation was conducted.

Research suggests that transparency is a key factor in maintaining legal defensibility. Psychologists who clearly document their methods, acknowledge limitations, and provide rationale for their decisions are more likely to produce defensible evaluations (Perle et al., 2025).

Licensing and Cross Jurisdictional Practice

Technology enables forensic psychologists to conduct evaluations across geographic boundaries, but legal authority to practice does not automatically extend across jurisdictions. Licensing laws vary by state, region, and country, and psychologists must comply with the regulations of the jurisdiction in which the examinee is located.

Cross jurisdictional practice is one of the most complex legal issues in teleforensic work. In many cases, psychologists must be licensed in the jurisdiction where the examinee resides, even if the psychologist is physically located elsewhere. Some jurisdictions have temporary practice provisions, reciprocity agreements, or telehealth specific regulations, but these vary widely.

Failure to comply with licensing requirements can have serious consequences, including legal sanctions, exclusion of testimony, and professional discipline. Therefore, psychologists must verify their authority to practice before conducting remote evaluations.

For example, a psychologist licensed in one state may be asked to conduct a remote disability evaluation for an individual located in another state. Before proceeding, the psychologist must determine whether their license permits practice in that jurisdiction or whether additional authorization is required. Simply being retained by an attorney or court does not override licensing requirements.

International evaluations introduce additional complexity. Laws governing psychological practice, data protection, and expert testimony may differ significantly between countries. Psychologists must ensure compliance with all relevant regulations when conducting cross border evaluations.

Jurisdictional Issues in Court Proceedings

In addition to licensing, jurisdictional issues may arise in relation to court authority and procedural rules. Different courts may have varying requirements for expert testimony, documentation, and admissibility of remote evaluations.

Some courts have specific rules regarding the use of videoconferencing for testimony or evaluation. Others may require in person assessments for certain types of cases. Psychologists must be familiar with the rules governing the specific court in which their evaluation will be used.

Jurisdictional differences may also affect confidentiality and privilege. The extent to which forensic evaluation data is protected from disclosure may vary depending on the legal context and location. Psychologists must understand these differences and explain them to examinees during informed consent.

Documentation and Record Keeping Requirements

Documentation is a critical component of legal compliance in forensic evaluations. Technology mediated assessments require additional documentation to address the unique aspects of remote practice.

Psychologists should document the type of technology used, including the platform and any relevant security features. They should record the date, time, and duration of sessions, as well as the identity verification process.

Environmental conditions, such as the presence of other individuals or potential distractions, should also be noted.

Technical issues must be documented in detail. This includes interruptions, connectivity problems, and any steps taken to address them. Such documentation is essential for demonstrating that the evaluation was conducted responsibly and for explaining any limitations.

For instance, if a videoconferencing session was interrupted multiple times due to internet instability, the psychologist should document how this affected the evaluation and whether any portions were repeated or omitted. Failure to document such issues may lead to challenges regarding the reliability of the findings.

Digital record keeping also raises legal considerations regarding data storage and retention. Psychologists must comply with applicable laws and regulations regarding how long records must be kept and how they must be protected. Secure storage and controlled access are essential to prevent unauthorized disclosure.

Risk Management in Legal Contexts

Risk management involves identifying and addressing potential legal vulnerabilities in forensic practice. Technology introduces new risks that must be managed proactively.

One key strategy is the use of clear and detailed informed consent procedures. By informing examinees of the nature and limitations of remote evaluations, psychologists reduce the risk of misunderstandings and legal disputes.

Another strategy is adherence to established guidelines and best practices. Psychologists who follow recognized standards are better positioned to defend their methods in court. This includes using validated assessment tools, maintaining secure data practices, and documenting procedures thoroughly.

Consultation is also an important risk management tool. When facing complex legal or technological issues, psychologists may benefit from consulting with colleagues, legal professionals, or regulatory boards.

Case Example

Consider a forensic psychologist conducting a remote competency to stand trial evaluation for a defendant in a different state. The psychologist uses a videoconferencing platform to conduct interviews and administers a cognitive screening tool digitally.

During the evaluation, the connection becomes unstable, and several portions of the interview must be repeated. The defendant is located in a correctional facility where staff are present nearby. The psychologist completes the evaluation and submits a report without documenting these issues.

In court, the evaluation is challenged. The opposing party argues that the unstable connection may have affected the accuracy of the assessment and that the presence of staff may have influenced the defendant's responses. Additionally, questions are raised about whether the psychologist was authorized to practice in the defendant's state.

This scenario illustrates multiple legal vulnerabilities. The lack of documentation undermines the credibility of the evaluation. The potential licensing issue raises questions about the legality of the practice. The environmental factors and technical issues affect reliability. A more defensible approach would have included verifying licensure, documenting all conditions, and clearly explaining limitations in the report.

Summary

Legal and jurisdictional considerations are central to the use of technology in forensic psychological evaluations. Psychologists must ensure that their methods meet standards for admissibility, comply with licensing requirements, and align with court procedures. Technology does not eliminate these requirements but adds new layers of complexity.

Adherence to legal standards requires careful planning, thorough documentation, and ongoing awareness of regulatory requirements. By understanding and addressing these considerations, forensic psychologists can produce evaluations that are both ethically sound and legally defensible.

Section 6: Assessment Validity and Reliability in Technology Mediated Forensic Evaluations

Validity and reliability concerns emerge immediately when forensic assessments are conducted remotely because technology fundamentally changes the conditions under which psychological data are obtained. In traditional in person evaluations, psychologists have greater control over the testing environment, behavioral observation, rapport development, and administration procedures. Remote administration introduces variables that can directly affect the accuracy, consistency, and interpretability of forensic findings. As a result, psychologists must evaluate not simply whether a test can be administered remotely, but whether the technological conditions alter the meaning or defensibility of the results. In forensic contexts, where evaluations may influence criminal responsibility determinations, competency findings, custody decisions, disability claims, or risk assessments, even subtle threats to validity can carry substantial legal consequences.

Construct Validity

Remote administration challenges construct validity by potentially altering the psychological processes being measured. For example, a cognitive assessment administered through videoconferencing may unintentionally measure technological familiarity, internet stability, or environmental distraction in addition to the intended cognitive construct. Examinees with limited digital literacy, sensory impairments, or unstable internet access may perform differently for reasons unrelated to actual psychological functioning. Similarly, personality or symptom-based assessments administered remotely may be influenced by diminished rapport, reduced behavioral containment, or increased opportunity for impression management. In forensic settings, where response style and credibility

are often central issues, these factors can significantly complicate interpretation. Psychologists must therefore consider whether remote conditions introduce construct-irrelevant variance that weakens confidence in the conclusions drawn from assessment data.

Criterion Validity

Criterion validity may also be affected when remote assessment conditions differ substantially from the contexts in which instruments were originally validated. Many forensic assessment tools were standardized using in person administration procedures under controlled conditions. When administered remotely, it is not always clear whether the predictive relationships established in validation studies remain equivalent. For example, a violence risk assessment tool validated through structured in person interviewing may not function identically when administered through videoconferencing if important behavioral indicators are more difficult to observe. Delays in audio transmission, restricted camera angles, reduced visibility of psychomotor behavior, or inability to fully assess environmental context may weaken the evaluator's ability to gather clinically relevant information. Consequently, psychologists must critically examine whether remote administration alters the predictive utility or interpretive framework of the instruments being used.

Performance Validity and Response Bias

Performance validity and response bias are critical concerns in forensic assessment. Psychologists must evaluate whether the examinee is putting forth adequate effort and providing accurate information. Technology mediated assessments introduce additional challenges in this area. Research indicates that symptom validity tests and performance validity tests can be administered

remotely, but their interpretation may be affected by contextual factors (Shura et al., 2024; Giromini et al., 2024). For example, distractions, technical difficulties, or misunderstanding of instructions may influence performance in ways that mimic poor effort.

In forensic contexts, misinterpreting such factors can have serious consequences. An examinee may be incorrectly classified as malingering due to low performance caused by environmental factors or technological issues. Conversely, actual malingering may go undetected if monitoring is insufficient. To address these challenges, psychologists should use multiple validity measures, consider contextual factors, and interpret results cautiously. They should also document any factors that may have influenced performance.

Reliability in Forensic Psychology and Technology

Reliability is similarly vulnerable to technological disruption and procedural inconsistency. Test-retest reliability may be affected if internet instability, device differences, or changing environmental conditions alter examinee performance across administrations. Interrater reliability may also be compromised when evaluators have inconsistent access to behavioral information due to differences in camera quality, screen resolution, or audiovisual clarity. Internal consistency can be affected if examinees become distracted, fatigued, or disengaged during lengthy remote procedures. In forensic settings, where evaluators are often expected to defend the methodological integrity of their conclusions under legal scrutiny, these reliability concerns become particularly important. Opposing counsel may challenge whether technological conditions undermined consistency or introduced uncontrolled error into the assessment process.

Remote administration also increases concerns regarding standardization and procedural control. Traditional forensic assessment relies heavily on standardized

administration procedures to preserve psychometric integrity. Remote testing environments make it more difficult to ensure that instructions are delivered consistently, that examinees are free from external assistance, or that testing materials remain secure. For example, an examinee completing cognitive tasks remotely may have access to notes, internet resources, calculators, or off-camera coaching without the evaluator's knowledge. Even subtle deviations from standardized administration can affect score interpretation and weaken legal defensibility. Accordingly, psychologists must implement safeguards such as environmental scans, explicit instructions regarding testing conditions, continuous behavioral monitoring, and detailed documentation of any irregularities that occur during the evaluation process.

Research increasingly suggests that some remotely administered forensic procedures can approximate traditional administration when appropriate safeguards are used, but equivalence cannot be assumed automatically across all instruments or populations (Alva et al., 2025; Giromini et al., 2024). Psychologists must therefore evaluate each assessment method individually, considering empirical support for remote use, characteristics of the examinee, technological limitations, and the specific forensic referral question. Ethical forensic practice requires psychologists to recognize that validity and reliability are not static properties of a test alone but are influenced by the conditions under which assessment occurs. As tele-forensic practice continues to expand, ongoing research, training, and methodological scrutiny will remain essential for preserving the scientific integrity and legal defensibility of forensic psychological evaluations.

Technology mediated assessments may influence these properties by altering how data are collected, how examinees respond, and how psychologists interpret results. Research emphasizes that remote methods must be evaluated carefully to

determine whether they maintain equivalence with traditional administration procedures (Alva et al., 2025; Giromini et al., 2024).

Measurement Equivalence Between Remote and In-Person Assessments

A central question in tele-forensic assessment is whether remote administration produces results equivalent to in person methods. Measurement equivalence is critical because forensic conclusions often rely on standardized norms derived from in person testing conditions.

Recent research suggests that many psychological measures show comparable results across remote and in person formats, particularly for structured interviews and certain self-report instruments (Sperling et al., 2024). However, equivalence is not universal. Some assessments, particularly those involving complex cognitive tasks, timed responses, or detailed behavioral observation, may be more sensitive to changes in administration conditions.

Neuropsychological tests that require precise timing or manipulation of physical materials may produce different results when administered remotely. Similarly, projective measures or performance based assessments may be affected by changes in visual presentation or examiner interaction (Ales et al., 2023).

In forensic settings, even small differences in measurement can have significant implications. A slight variation in cognitive test performance could influence determinations of competency, intellectual functioning, or impairment. Therefore, psychologists must evaluate whether the specific tools they use have been validated for remote administration. When validation data are limited or absent, psychologists must proceed with caution. This may involve supplementing remote data with collateral information, using multiple assessment methods, and clearly documenting limitations.

Rapport and Interpersonal Dynamics

Rapport is a critical component of forensic assessment. It influences the examinee's willingness to engage, provide accurate information, and respond honestly. Technology mediated evaluations can affect rapport in both positive and negative ways. On one hand, some individuals may feel more comfortable in their own environment and may be more willing to disclose sensitive information. On the other hand, the lack of physical presence may reduce the psychologist's ability to establish trust and read subtle interpersonal cues.

Research indicates that videoconferencing can support adequate rapport in many cases, but it may limit the observation of nonverbal behavior, such as body language, eye contact, and subtle emotional expressions (Procaccia et al., 2024). These limitations can affect both data collection and interpretation.

In a criminal responsibility evaluation, the psychologist must assess emotional responsiveness, affective expression, and interpersonal behavior. If video quality is poor or the camera frame is limited, important cues may be missed. This can reduce the validity of conclusions regarding emotional functioning. To mitigate these challenges, psychologists can use strategies such as maintaining consistent eye contact through the camera, using clear and structured communication, and allowing additional time for interaction. They should also acknowledge the limitations of remote observation in their reports.

Environmental Factors and Contextual Influences

One of the most significant threats to validity in remote assessments is the lack of control over the evaluation environment. In traditional settings, psychologists can standardize conditions by controlling noise, lighting, interruptions, and access to materials. In remote settings, these factors are often outside the psychologist's control.

Environmental distractions can affect attention, memory, and overall performance. Background noise, interruptions by family members, or competing demands can reduce concentration and lead to inconsistent responses. Research highlights that uncontrolled environments are a major source of variability in remote assessment data (Yıldırım et al., 2024). For example, an examinee completing a cognitive task at home may be interrupted by a phone call or distracted by other activities. These disruptions may result in lower performance scores that do not accurately reflect the individual's true abilities.

Ecological validity presents a more complex issue in remote forensic assessment. In some situations, remote evaluations may enhance ecological validity by allowing psychologists to observe individuals within more naturalistic environments. For example, a child custody evaluator conducting remote parent-child observations within the home may obtain information about family interactions that would not emerge in a clinical office. However, uncontrolled environments also create substantial interpretive challenges. External interruptions, presence of off-camera individuals, environmental distractions, and variability in testing conditions can all influence behavior in ways that are difficult to standardize or interpret. The psychologist may be unable to determine whether observed behaviors reflect genuine psychological functioning or reactions to environmental variables unique to the remote setting. These limitations must be carefully documented and considered when formulating forensic opinions.

In forensic contexts, such variability can lead to misinterpretation. A psychologist might attribute poor performance to cognitive impairment when it is due to environmental distraction. To address this issue, psychologists should assess the environment at the beginning of the session, provide instructions to minimize distractions, and document any interruptions.

Identity Verification and Test Integrity

Ensuring that the correct individual is participating in the evaluation is essential for validity. In remote settings, identity verification can be more challenging than in person. If identity is not confirmed, the entire assessment may be invalid.

In addition to identity verification, psychologists must ensure that the examinee is completing the assessment independently. Remote environments create opportunities for coaching, consultation, or use of unauthorized materials. These factors can compromise test integrity and lead to inaccurate results.

Research emphasizes the importance of implementing safeguards such as visual monitoring, environmental scans, and clear instructions regarding independent participation (Perle et al., 2025). Psychologists should also be attentive to behavioral indicators of potential interference, such as inconsistent responses, unusual pauses, or frequent off screen attention.

Technological Factors Affecting Data Quality

Technology itself can influence the quality of assessment data. Factors such as internet connectivity, audio quality, video resolution, and device functionality can all affect communication and observation.

Poor connectivity may result in delays, interruptions, or loss of information. Audio issues may make it difficult to hear responses accurately. Video limitations may obscure facial expressions or gestures. These factors can reduce both reliability and validity. If an examinee's responses are frequently interrupted by connection issues, the psychologist may miss important information or misinterpret incomplete responses. Similarly, if video quality is insufficient, subtle behavioral cues may not be observable.

Psychologists should assess technological quality at the beginning of the session and address any issues promptly. If technological limitations significantly interfere with the evaluation, alternative arrangements should be considered.

Strategies to Enhance Validity and Reliability

Maintaining validity and reliability in technology mediated forensic evaluations requires deliberate planning and implementation of best practices. Several strategies are supported by research and professional guidelines.

First, psychologists should select assessment tools that have evidence supporting their use in remote contexts. When such evidence is limited, multiple methods should be used to corroborate findings.

Second, environmental conditions should be optimized as much as possible. This includes providing clear instructions to examinees, minimizing distractions, and verifying privacy.

Third, identity verification and monitoring procedures should be implemented to ensure authenticity of participation. This may include checking identification, conducting environmental scans, and observing behavior throughout the session.

Fourth, psychologists should document all relevant factors, including technological issues, environmental conditions, and deviations from standard procedures. This documentation supports transparency and allows for appropriate interpretation of results.

Finally, psychologists should interpret findings cautiously and consider alternative explanations for observed results. This includes considering the potential impact of technology related factors on performance.

Case Example

Consider a remote disability evaluation in which an examinee completes a cognitive screening test via videoconferencing. During the assessment, the internet connection becomes unstable, and the examinee appears distracted by background noise. The psychologist observes inconsistent performance and concludes that the examinee has significant cognitive impairment.

Upon further review, it becomes apparent that the examinee was experiencing multiple interruptions and had difficulty hearing instructions due to audio issues. In this case, the observed performance may not reflect true cognitive ability but rather the impact of environmental and technological factors.

A more appropriate approach would involve documenting these issues, repeating the assessment under improved conditions if possible, and considering collateral data before reaching conclusions.

Summary

Validity and reliability are central to the integrity of forensic psychological evaluations. Technology mediated assessments introduce new variables that can influence measurement accuracy, consistency, and interpretation. While research supports the use of remote methods in many contexts, limitations must be carefully managed.

Key factors affecting validity and reliability include measurement equivalence, rapport, environmental conditions, identity verification, performance validity, and technological quality. Psychologists must implement strategies to minimize bias, ensure accurate data collection, and maintain transparency.

By understanding and addressing these challenges, forensic psychologists can use technology effectively while preserving the scientific and legal integrity of their evaluations.

Section 7: Digital Psychological Testing and Assessment Tools in Forensic Evaluations

Introduction

Digital psychological testing and assessment tools are now a routine part of contemporary forensic practice. What was once limited to computerized scoring or electronic storage of test responses has evolved into a broader ecosystem that includes remote administration platforms, online symptom inventories, digital performance validity measures, computerized cognitive screening, tele neuropsychological procedures, and app supported assessment workflows. In forensic settings, these tools are used in criminal, civil, family, correctional, disability, and administrative evaluations. Their growing use reflects practical advantages such as improved access, efficient scoring, more streamlined data management, and the ability to conduct assessments when in person contact is not feasible.

At the same time, forensic use of digital assessment tools requires a higher level of caution than many nonforensic uses. In clinical practice, a digital screening result may guide treatment planning and later be revised with additional information. In forensic work, however, digital test results may influence legal conclusions about competency, credibility, damages, parenting capacity, violence risk, impairment, or response style. That means the psychologist must evaluate whether the digital format preserves standardization, validity, reliability, security, fairness, and interpretive accuracy. The ethical and scientific question is not

whether a tool is available in digital form. The question is whether it can be used in a particular forensic referral with adequate confidence.

Recent scholarship shows that digital testing can be appropriate in selected contexts, but also emphasizes that not all tools are equally suited to remote or technology mediated administration (Giromini et al., 2024; Perle et al., 2025; Young, 2024). Some self report instruments appear relatively adaptable to secure digital delivery. Other measures, especially those involving timing, complex instructions, physical manipulatives, nuanced behavior observation, or strong test security concerns, require far more caution. This section reviews the main categories of digital psychological testing used in forensic work, their advantages and risks, and best practices for their defensible use.

The Meaning of Digital Testing in Forensic Practice

Digital testing refers broadly to the use of electronic platforms, devices, or software to administer, score, transmit, store, or interpret assessment data. In forensic work, digital testing does not always mean fully remote assessment. It may include in person testing using tablets or computers, hybrid methods in which interviews occur by video but testing is supervised in a controlled location, or asynchronous data collection followed by synchronous review.

The forensic psychologist must distinguish among several levels of digital use. One level involves simple electronic scoring of a measure administered in traditional fashion. Another involves remote delivery of a self-report inventory through a secure platform. A more complex level involves remote supervision of performance based or cognitive tasks through video. The legal and psychometric risks are different at each level. A measure that is acceptable when taken on a secure tablet in a controlled clinic room may not be equally acceptable when taken on an unsupervised home computer.

In practical terms, digital assessment tools are not a single class of instruments. They include personality inventories, symptom checklists, structured interview supports, risk assessment software, cognitive screening measures, response validity tools, projective system supports, and emerging mobile or app-based tools. Each must be evaluated on its own evidentiary and forensic merits.

Categories of Digital Assessment Tools in Forensic Settings

Digital tools used in forensic settings can be grouped into several broad categories. The first category is self-report inventories, including personality and psychopathology measures. These are often among the easiest to move into digital environments because the core task involves reading items and selecting responses. Many platforms now support secure online administration and automated scoring of broad band measures frequently considered in forensic practice.

The second category is symptom validity and performance validity assessment. These tools are especially important in forensic work because referral contexts often involve incentives to exaggerate, minimize, or distort symptoms. Recent research on remote administration of symptom validity measures suggests that some measures may function reasonably in person and remote formats, but interpretation still requires careful attention to context, supervision, and environmental conditions (Shura et al., 2024; Giromini et al., 2024).

The third category is cognitive and neuropsychological assessment. This area is more complex. Certain brief screening procedures and some structured tele neuropsychological methods have demonstrated promise, but the literature continues to caution against assuming equivalence across all instruments and populations. Remote cognitive testing may be affected by connection quality,

screen size, device differences, timing precision, and environmental distractions (Sperling et al., 2024; Yıldırım et al., 2024).

The fourth category includes structured professional judgment and risk related tools that may be digitized for scoring, documentation, or decision support. These tools may improve consistency in data entry and record keeping, but they do not eliminate the psychologist's responsibility for careful judgment. A digital format does not transform a structured professional judgment method into a purely actuarial or self-executing conclusion.

The fifth category includes projective and performance-based methods supported by digital tools. This is a particularly sensitive area in forensic practice because these methods often depend on careful standardization, controlled presentation, and detailed observation of examinee behavior. Some work has explored digital adaptation, but the literature generally recommends strong caution and method specific justification (Ales et al., 2023).

Digital Administration of Personality and Psychopathology Measures

Personality and psychopathology measures are among the most common digital tools in forensic work. These measures are often relevant to civil damages evaluations, disability matters, criminal responsibility assessments, parental functioning questions, and credibility analysis. Their digital appeal is obvious. They can be administered efficiently, scored automatically, and integrated into larger forensic workflows.

The main advantages of digital administration in this area are efficiency, standardization of item presentation, reduction of hand scoring errors, and easier record management. Forensic psychologists can also benefit from rapid report generation, which may support more consistent interpretation when used

responsibly. Digital administration can improve access for individuals who cannot easily travel to an office or institution.

However, these strengths do not remove the need for psychometric caution. A digital personality inventory must still be interpreted within the limits of its remote administration evidence. The evaluator should know whether the measure has evidence supporting remote use, whether instructions can be delivered clearly, whether item visibility is adequate across devices, and whether the examinee can complete the measure independently. In forensic settings, the possibility of consulting outside materials, discussing items with others, or responding under external influence is not trivial.

Recent research on remote administration formats for certain measures and validity indicators suggests encouraging but not universal findings. Giromini et al. (2024) reported data relevant to in person and remote administration formats involving the MMPI 2 RF, IOP 29, IOP M, and FIT in a simulation study on feigned mild traumatic brain injury. Forensic psychologists should treat such findings as informative rather than blanket permission for all remote use. The specific referral question, examinee characteristics, supervision level, and environmental conditions still matter.

As an example, consider a remote personal injury evaluation in which the examinee completes a broad psychopathology inventory from home. If the psychologist has verified identity, reviewed the testing environment, used a secure platform, and monitored completion in real time, the resulting data may be substantially more interpretable than if the same measure were simply emailed for unsupervised completion. The digital tool is the same, but the forensic quality of the procedure is very different.

Digital Symptom Validity and Performance Validity Assessment

Validity assessment is indispensable in forensic work. Because many forensic referrals involve secondary gain, contested claims, or legal incentives, psychologists must evaluate whether reported symptoms and observed performance are credible. Digital delivery of symptom validity and performance validity tools therefore raises especially important questions.

Remote conditions can affect validity testing in two opposite ways. They may create additional opportunities for distortion, such as off camera coaching or access to notes. They may also create false positives if distractions, poor audio, unstable connections, or misunderstandings reduce performance or alter response style. The psychologist must therefore interpret digital validity data with more contextual awareness than might be needed in a tightly controlled in person setting.

Shura et al. (2024) evaluated telehealth administration of MMPI symptom validity scales and highlighted the need to consider factors that may reduce reliability and validity in remote formats. Similarly, Giromini et al. (2024) addressed the functioning of validity related tools across remote and in person formats. These studies support cautious, informed use rather than unquestioning equivalence.

Best practice in forensic digital validity assessment generally includes using multiple indicators rather than relying on a single score, maintaining real time supervision when possible, documenting environmental conditions, and integrating validity findings with interview behavior, collateral information, and contextual evidence. A remote validity score should not be interpreted in isolation from how the testing occurred.

For instance, in a disability claim evaluation, an examinee may show patterns suggesting exaggeration on a remotely administered inventory. Before drawing

strong conclusions, the evaluator should consider whether the examinee was alone, whether instructions were understood, whether the connection disrupted item presentation, whether literacy or language factors complicated responses, and whether additional validity indicators converge. A defensible forensic opinion comes from the integrated pattern, not from one digital output.

Cognitive and Neuropsychological Testing in Digital and Remote Formats

Cognitive and neuropsychological assessment presents some of the most difficult challenges in digital forensic work. These evaluations are often central to questions involving competency, traumatic brain injury, neurocognitive impairment, intellectual functioning, and functional capacity. Yet many cognitive measures were developed under controlled in person conditions and may be sensitive to administration changes.

Recent tele-neuropsychology literature suggests that certain remote procedures can generate useful data, especially when built around validated methods, appropriate case selection, and careful control of conditions (Alva et al., 2025; Sperling et al., 2024). However, the literature also makes clear that not all neuropsychological tasks transfer cleanly to remote formats. Timing precision, screen lag, audio quality, device variation, and limited behavioral observation can all affect performance.

Yıldırım et al. (2024) noted that some assessment types, including certain forensic applications, may have lower reliability in remote conditions and require heightened caution. This is especially relevant in legal contexts where small score differences can matter. A digit span task performed over unstable video, for example, may not reflect the same construct with the same precision as a directly administered in person task. A visuospatial task may be altered by screen size or

camera angle. Processing speed tasks may be distorted by software delays or input device differences.

Forensic psychologists should therefore avoid overgeneralization. It is not enough to say that tele neuropsychology exists. The question is whether this specific test, with this specific examinee, can answer this specific forensic referral question adequately. Sometimes the answer will be yes. Sometimes a limited cognitive screening is appropriate, but a full diagnostic interpretation is not. Sometimes the answer will be no and an in-person assessment will be necessary.

As an example, a court may request evaluation of an older adult's decisional capacity where travel is difficult. A remote interview and selective cognitive screening may provide useful preliminary information, especially if corroborated by records and collateral interviews. However, if the case turns on fine distinctions in executive functioning and memory with significant financial implications, a more controlled in person evaluation may be more defensible.

Structured Risk Assessment and Digital Decision Support

Digital tools are also increasingly used to support structured risk assessment and forensic decision making. These tools may help psychologists organize data, calculate actuarial scores, generate structured summaries, and track case information across multiple evaluations. They can improve consistency and reduce clerical error, which is valuable in high volume or institution-based practice.

Gowensmith et al. (2022) discussed use of a mobile app to identify base rates and monitor bias in forensic evaluation. This illustrates an important point. Digital systems can support forensic reasoning, but they should not be mistaken for autonomous reasoning. A well-designed tool can prompt attention to relevant variables or base rate considerations, yet the evaluator remains responsible for determining whether the entered information is accurate, whether the case fits

the tool's intended population, and whether the output is interpreted appropriately.

In risk assessment, digital tools can sometimes create a false sense of precision. A numerically generated result may appear more objective than it truly is. In forensic practice, psychologists must resist the temptation to equate computerized scoring with infallibility. The tool's legal value depends on the quality of the underlying model, the appropriateness of the data entered, and the evaluator's transparent explanation of how the result was used.

For example, in a violence risk evaluation, a digital scoring platform may streamline data entry for a structured tool. That can be helpful. But if the evaluator inputs incomplete history, misunderstands variable definitions, or uses the instrument outside its validated population, the digital convenience does not preserve forensic quality. The resulting opinion may still be flawed.

Projective and Performance Based Methods in Digital Contexts

Projective and performance-based methods require particular caution in digital forensic practice. These methods often depend on standardized presentation, careful monitoring of response process, high quality observation, and strict control of test materials. Remote adaptation can therefore pose significant methodological and legal concerns.

Ales et al. (2023) reviewed options for remote administration of the Rorschach and reported pilot work involving an R PAS app. Their article is especially useful because it does not treat digital adaptation as a simple substitution. Instead, it highlights the need to consider reliability, validity, utility, response process, and practical administration issues. In forensic settings, where these methods may already attract scrutiny, digital adaptation requires an especially strong justification.

The core forensic question is whether the digital format preserves the meaning of the task. If visual details, card handling, response timing, or spontaneous behavioral features change in important ways, then interpretive continuity may be weakened. In many cases, the most defensible approach may be to reserve such methods for controlled in person settings or to use them digitally only in a limited, well justified, and clearly documented manner.

If a forensic psychologist chooses to use a performance-based method in a digital context, the report should explain the procedure in detail, identify any deviations from usual administration, describe supporting literature, and discuss the implications of the format for interpretation. Without that transparency, the assessment may be vulnerable to legal challenge.

Test Security, Standardization, and Examinee Behavior

A major issue across all digital assessment formats is test security. In forensic work, unauthorized exposure of materials does not just threaten future administrations. It may contaminate ongoing cases, undermine fairness, and raise admissibility concerns. Digital delivery creates risks such as screenshots, recordings, unauthorized printing, item sharing, and AI assisted response coaching.

Standardization is equally important. Even if the content of a measure remains the same, digital differences in screen size, input method, device type, internet speed, and environmental context may alter the examinee's experience. In forensic settings, the psychologist should think of digital testing as a procedural system, not just an instrument. Every part of the system influences interpretability.

Examinee behavior also matters. Looking off screen, delayed responding, inconsistent engagement, reading from notes, or apparent interaction with unseen others can all affect the meaning of digital data. The psychologist should

monitor these behaviors actively and document them. In some cases, the data may remain interpretable with caution. In others, the administration should be discontinued.

For example, if an examinee in a custody evaluation repeatedly turns away from the camera and appears to consult a phone while completing a digital inventory, the psychologist cannot assume the responses reflect an unassisted self-report. That observation becomes part of the forensic data and may influence whether the test can be interpreted at all.

Best Practical Practices for Forensic Use of Digital Assessment Tools

The best forensic use of digital tools begins before test administration. The psychologist should first determine whether the referral question can be answered adequately using digital methods. Next, the evaluator should confirm whether the selected tools have evidence supporting the intended format and population. The psychologist should then establish secure platform procedures, verify examinee identity, assess digital literacy, and review environmental expectations.

During administration, real time supervision is often preferable to unsupervised completion, especially in contested or high stakes matters. The evaluator should monitor privacy, minimize interruptions, observe behavior, and note any deviations from standard conditions. After administration, interpretation should integrate test data with interview findings, collateral records, and contextual factors.

Reports should state that digital methods were used and describe how they were implemented. If evidence supporting the format is limited, that limitation should

be stated directly. If the digital procedure likely improved access but reduced control over conditions, both sides of that balance should be discussed.

A useful example is a remote employment related fitness for duty evaluation in which the psychologist uses a secure digital platform for a personality inventory, conducts an extended video interview, reviews employment records electronically, and documents that the examinee was alone, identity verified, and continuously monitored. Such a procedure may be reasonably strong if the tools are suitable and the report explains the method carefully. By contrast, an unsupervised emailed battery completed under unknown conditions would be far less defensible.

Summary

Digital psychological testing and assessment tools can play an important role in forensic evaluations, but their value depends on more than availability or convenience. In forensic work, digital methods must be judged by whether they preserve validity, reliability, security, fairness, and legal defensibility. Self-report inventories, validity measures, cognitive tools, structured decision supports, and selected performance-based methods may all have a place in digital forensic practice, but only when used thoughtfully and with attention to the evidence base.

The strongest forensic use of digital tools combines method specific knowledge, careful supervision, attention to environmental and technological factors, active monitoring of examinee behavior, and transparent reporting. Digital tools should support forensic reasoning, not replace it. A psychologist who understands both the possibilities and the limits of digital assessment is better equipped to produce accurate, ethical, and defensible forensic opinions.

Section 8: Practical Implementation and Workflow Integration in Technology Mediated Forensic Evaluations

Introduction

The successful integration of technology into forensic psychological evaluations requires more than knowledge of tools and ethical standards. It requires a structured and intentional workflow that ensures consistency, accuracy, and legal defensibility across all phases of the evaluation. Technology affects every step of the forensic process, including referral intake, scheduling, informed consent, data collection, testing, collateral review, documentation, and report preparation. Without a well-designed workflow, the use of technology can introduce inefficiencies, inconsistencies, and risks that undermine the quality of the evaluation.

Research emphasizes that structured implementation and clear procedural planning improve both the reliability of forensic assessments and the evaluator's ability to manage technological challenges (Abascal et al., 2024; Perle et al., 2025). This section provides a comprehensive overview of how to integrate technology into forensic workflows, including platform selection, client preparation, session management, and contingency planning.

Workflow Design in Technology Mediated Forensic Practice

A well-structured workflow begins with referral clarification. The psychologist must determine the legal question, the scope of the evaluation, and whether technology mediated methods are appropriate. Not all cases are suitable for remote assessment, and this determination should be made before scheduling.

Once the case is accepted, the workflow should include standardized procedures for scheduling and communication. This may involve sending secure appointment links, providing written instructions for accessing the platform, and confirming technological readiness. Consistency in these steps reduces the likelihood of technical disruptions and ensures that all examinees receive the same information.

The evaluation itself should follow a structured sequence. This typically includes identity verification, informed consent, environmental assessment, clinical interview, psychological testing, and collateral data collection. Each step should be adapted for remote delivery while maintaining alignment with standard forensic procedures.

For example, in a remote competency evaluation, the workflow may include a pre-session technology check, verification of the examinee's identity through institutional staff, a structured informed consent discussion addressing telehealth risks, a clinical interview conducted via videoconferencing, and administration of selected assessment tools. Each step should be documented clearly.

Platform Selection and Technical Considerations

Selecting appropriate technology platforms is a critical component of workflow integration. Platforms should be evaluated based on security, reliability, functionality, and compliance with applicable regulations. Secure videoconferencing systems with encryption and privacy protections are essential for forensic work.

In addition to security, functionality is important. Platforms should support features such as screen sharing, stable video and audio quality, and compatibility with different devices. These features facilitate effective communication and allow for the administration of certain assessment tools.

Reliability is also a key factor. Frequent disconnections or poor-quality connections can disrupt the evaluation and affect data quality. Psychologists should test platforms in advance and be prepared to troubleshoot common issues.

Client Preparation and Technology Readiness

Preparing the examinee for a technology mediated evaluation is essential for ensuring valid and reliable results. This preparation includes providing clear instructions about how to access the platform, what to expect during the session, and how to prepare the environment.

Examinees should be instructed to use a private, quiet space with minimal distractions. They should be informed about the importance of maintaining confidentiality and avoiding the presence of others during the evaluation. Instructions should also include guidance on device use, such as ensuring that the camera and microphone are functioning properly.

Technology readiness should be assessed prior to the evaluation. This may involve a brief pre session check to confirm that the examinee can access the platform and use its features. Addressing technical issues in advance reduces the likelihood of disruptions during the evaluation.

Managing the Remote Evaluation Session

Effective management of remote forensic evaluation sessions requires a structured approach to maintain assessment integrity. At the beginning of the session, the psychologist should verify the examinee's identity, confirm that no unauthorized individuals are present, and evaluate the environment for privacy and potential distractions. Establishing these conditions helps support accurate data collection. Throughout the session, the psychologist must continue to

monitor environmental factors, such as interruptions or background noise, as well as observe behavioral cues that may influence interpretation. Ongoing awareness is especially important in remote settings where control over the environment is limited.

Clear and organized communication is essential to ensure the evaluation proceeds effectively. The psychologist should provide instructions in a structured manner and check for understanding, adjusting as needed to account for potential communication barriers. When technical issues arise, such as poor audio or video quality, they should be addressed promptly. If disruptions interfere with critical portions of the evaluation, the psychologist may need to pause, repeat information, or determine whether rescheduling is necessary to maintain the validity and reliability of the assessment.

Contingency Planning and Backup Procedures

Technology mediated evaluations require contingency planning to address potential disruptions. Psychologists should develop backup procedures for common issues such as connectivity problems, platform failures, and device malfunctions.

Backup plans may include alternative communication methods, such as switching to a different secure platform or using telephone contact for coordination. However, the use of alternative methods should be evaluated carefully, as they may affect the quality of the assessment. If a videoconferencing platform fails during a session, the psychologist may attempt to reconnect or switch to a backup platform. If video cannot be restored, the psychologist must determine whether continuing by audio only is appropriate for the evaluation. Contingency planning should be communicated to the examinee during informed consent. This ensures that both parties understand how disruptions will be handled.

Documentation and Workflow Consistency

Consistent documentation is essential for maintaining the integrity of technology mediated workflows. Psychologists should document each step of the process, including platform use, identity verification, environmental conditions, and any deviations from standard procedures. Standardized documentation templates can support consistency across cases. These templates may include sections for recording technological details, session conditions, and any issues encountered.

For example, a documentation template may include fields for noting the platform used, connection quality, presence of others, and any interruptions. This information supports transparency and legal defensibility.

Summary

Effective workflow integration is essential for the successful use of technology in forensic evaluations. Structured procedures, appropriate platform selection, thorough client preparation, and careful session management all contribute to the quality and reliability of the evaluation. By implementing consistent workflows and contingency plans, psychologists can minimize risks and enhance the defensibility of their work.

Section 9: Confidentiality and Data Security Best Practices

Introduction

Confidentiality and data security are fundamental responsibilities in forensic psychological practice. The use of technology introduces additional risks related to

data transmission, storage, and access. Forensic psychologists must ensure that sensitive information is protected at all stages of the evaluation process.

Research highlights that data breaches, unauthorized access, and insecure communication methods are among the most significant risks in telepsychology (Geraldo et al., 2024; Perle et al., 2025). In forensic contexts, these risks are particularly serious because evaluation data may include highly sensitive personal, medical, and legal information.

Principles of Data Security in Forensic Practice

Data security involves protecting information from unauthorized access, disclosure, or loss. Key principles include confidentiality, integrity, and availability. Confidentiality ensures that information is accessible only to authorized individuals. Integrity ensures that data is accurate and not altered improperly. Availability ensures that data can be accessed when needed. In forensic practice, these principles must be applied to all aspects of technology use, including communication, data storage, and record keeping.

Encryption and Secure Communication

Encryption is a critical component of data security. It ensures that information transmitted between the psychologist and the examinee cannot be intercepted or accessed by unauthorized parties. Secure telehealth platforms typically include encryption features that protect video and audio communication.

Psychologists should use platforms that provide strong encryption and avoid using unsecured communication methods. This includes avoiding standard email for transmitting sensitive information unless additional security measures are in place. For example, a forensic psychologist sending a report to an attorney should

use a secure file transfer system rather than standard email. This reduces the risk of unauthorized access.

Secure Storage and Access Control

Data storage must be managed carefully to prevent unauthorized access.

Electronic records should be stored on secure systems with appropriate access controls, such as password protection and user authentication.

Psychologists should also consider the physical security of devices used to store data. Laptops, tablets, and external drives should be protected against theft or loss. Regular updates and security patches should be applied to protect against vulnerabilities. Storing forensic reports on an encrypted hard drive with restricted access helps ensure that only authorized individuals can access the data.

Data Retention and Disposal

Forensic psychologists must comply with legal and professional requirements regarding data retention. Records must be retained for specified periods and disposed of securely when no longer needed.

Secure disposal methods include deleting electronic files using methods that prevent recovery and destroying physical media when applicable. Improper disposal can result in data breaches and ethical violations.

Breach Response and Risk Management

Despite best efforts, data breaches may occur. Psychologists must have a plan for responding to such incidents. This includes identifying the breach, assessing its impact, notifying affected parties if required, and taking steps to prevent future

occurrences. For example, if a laptop containing forensic data is lost, the psychologist should assess whether the data was encrypted and determine whether notification is required. Prompt response and documentation are essential.

Summary

Maintaining confidentiality and data security is a critical aspect of technology mediated forensic practice. By implementing encryption, secure storage, and effective risk management strategies, psychologists can protect sensitive information and uphold professional standards.

Section 10: Tele-Forensic Interviewing Techniques

Introduction

Interviewing is a central and often determinative component of forensic psychological evaluations. While psychological testing and record review contribute important data, the forensic interview frequently provides the primary foundation for understanding mental status, credibility, behavioral patterns, and functional abilities. The transition to tele-forensic interviewing requires psychologists to adapt traditional interviewing methods to a technology mediated environment while preserving validity, neutrality, and legal defensibility.

Recent research indicates that videoconferencing can support effective forensic interviewing, but it also introduces measurable differences in communication dynamics, rapport formation, and behavioral observation (Procaccia et al., 2024; Shahvaroughi et al., 2022). These differences do not render tele-interviews invalid,

but they require deliberate modification of technique and increased awareness of potential limitations.

Foundations of Tele-Forensic Interviewing

Tele-forensic interviewing retains the same core goals as in person interviewing. These include gathering accurate information, assessing psychological functioning, evaluating credibility, and addressing specific legal questions. However, the medium of communication changes how these goals are achieved.

Videoconferencing reduces access to certain nonverbal cues and may alter conversational flow. Research suggests that remote interviews can affect turn taking, response latency, and perceived interpersonal connection (Shahvaroughi et al., 2022). These factors can influence both the content and quality of information obtained. A slight delay in audio transmission may lead to interruptions or overlapping speech, which can disrupt the natural flow of conversation. The psychologist must adjust pacing and allow additional time for responses.

Rapport Development in Remote Contexts

Rapport is essential in forensic interviewing because it influences cooperation, disclosure, and the overall quality of information obtained. In remote settings, rapport may be more difficult to establish due to physical distance and reduced social cues.

Research indicates that rapport can still be effectively developed through videoconferencing when deliberate strategies are used (Abascal et al., 2024). These strategies include maintaining consistent eye contact with the camera, using clear and supportive language, and demonstrating attentiveness through verbal feedback. For example, in a criminal responsibility evaluation, the

psychologist may begin by explaining the process in a calm and structured manner, acknowledging the unusual nature of remote interaction, and inviting questions. This approach can reduce anxiety and increase engagement.

Building of rapport may also require additional time in remote settings.

Psychologists should allow for brief informal interaction at the beginning of the session to establish comfort. However, they must also maintain professional boundaries and neutrality.

Structuring the Tele-Forensic Interview

Structure is particularly important in remote interviews because it helps compensate for potential communication disruptions. A well-structured interview ensures that all relevant topics are addressed and that the evaluation remains focused on the referral question.

Psychologists should use clear transitions between topics and provide explicit instructions. This includes explaining when the interview is moving from general background information to more specific or sensitive topics. For example, in a competency evaluation, the psychologist may clearly indicate when the discussion is shifting from personal history to understanding of legal proceedings. This helps the examinee follow the structure and reduces confusion.

Structured interviewing also supports reliability. Using standardized questions or interview frameworks can help ensure consistency across cases and reduce the influence of technological variability.

Behavioral Observation in Tele-Forensic Interviews

Behavioral observation is a key component of forensic assessment. In remote settings, observation is limited by camera angle, video quality, and environmental

factors. Psychologists must adapt their observational strategies to account for these limitations.

Visual observation should focus on facial expressions, eye contact, and visible motor behavior. Auditory observation should include tone of voice, speech patterns, and response latency. Research indicates that some nonverbal cues, such as subtle gestures, may be less detectable in videoconferencing environments (Johnstone et al., 2024). For example, in a child custody evaluation, the psychologist may observe the parent's facial expressions and tone while discussing the child. However, body language below the camera frame may not be visible, limiting interpretation.

Psychologists should also document observational limitations. If video quality prevents clear observation of certain behaviors, this should be noted in the report.

Cultural and Accessibility Considerations

Cultural competence is essential in forensic interviewing, and technology adds additional layers of complexity. Differences in language, communication style, and familiarity with technology can affect participation.

Psychologists should assess whether the examinee has adequate access to technology and the ability to use it effectively. Accommodations may be necessary for individuals with disabilities, language barriers, or limited digital literacy. For example, an interpreter may be required for a non-English speaking examinee. In remote settings, this requires coordination to ensure that all parties can communicate effectively through the platform.

Summary

Tele-forensic interviewing requires adaptation of traditional techniques to a technology mediated environment. Key considerations include rapport development, structured communication, behavioral observation, and management of challenging situations. By applying evidence-based strategies and maintaining awareness of limitations, psychologists can conduct effective and defensible remote interviews.

Section 11: Case Examples and Applied Decision-Making in Technology Mediated Forensic Evaluations

Introduction

Case based learning is a critical component of professional competence in forensic psychology. Research consistently demonstrates that scenario-based training enhances clinical judgment, ethical decision making, and practical skill development (Abascal et al., 2024). In the context of technology mediated forensic evaluations, case examples provide an opportunity to apply theoretical knowledge to real world situations.

Case 1: Competency to Stand Trial Evaluation

A forensic psychologist is retained to conduct a competency evaluation for a defendant housed in a rural correctional facility. Due to logistical constraints, the evaluation is conducted via videoconferencing.

During the interview, the psychologist observes that the defendant is able to describe the roles of courtroom personnel but struggles to understand plea

bargaining. The connection is stable, and the environment is quiet, although correctional staff are present nearby.

The psychologist documents the presence of staff and considers its potential impact on responses. The evaluation includes a structured interview and review of records. The psychologist concludes that the defendant has partial understanding but requires further education. This case demonstrates appropriate use of tele-forensic methods with attention to environmental factors and documentation.

Case 2: Child Custody Evaluation

A psychologist conducts a remote child custody evaluation involving two parents in different locations. Interviews and parent child observations are conducted via videoconferencing.

During one session, the psychologist notices that a parent frequently looks off screen and appears to receive prompts. The psychologist pauses the session and asks whether anyone else is present. The parent initially denies this but later acknowledges that a relative is in the room.

The psychologist documents the incident and considers its impact on the reliability of the data. Additional sessions are conducted with stricter environmental controls. This case illustrates the importance of monitoring for third party influence and maintaining test integrity.

Case 3: Personal Injury Evaluation

A plaintiff in a personal injury case completes psychological testing remotely. The results indicate elevated symptom reporting and possible exaggeration.

The psychologist reviews the testing conditions and notes that the assessment was completed without real time supervision. The psychologist considers the possibility that external factors may have influenced responses.

To address this, the psychologist conducts additional interviews and uses multiple validity measures. The final report reflects a cautious interpretation of the test results. This case highlights the importance of considering context and using multiple data sources.

Case 4: Disability Evaluation

A psychologist conducts a remote disability evaluation for an individual with limited technological experience. During cognitive testing, the examinee struggles to navigate the platform and becomes frustrated.

The psychologist recognizes that performance may be affected by technological difficulties rather than cognitive impairment. The evaluation is adjusted to include simpler tasks and additional support. The psychologist documents these issues and interprets results cautiously. This case demonstrates the need to consider technology literacy and its impact on assessment.

Case 5: Ethical Dilemma in Remote Evaluation

A psychologist is asked to conduct a remote evaluation across state lines. Upon review, the psychologist realizes that they are not licensed in the examinee's jurisdiction.

The psychologist consults relevant regulations and determines that conducting the evaluation would violate licensing requirements. The referral is declined, and the psychologist provides recommendations for local evaluators. This case illustrates the importance of legal compliance and ethical decision making.

Decision-Making Framework

Effective decision making in tele-forensic evaluations involves several steps. First, the psychologist identifies the issue, such as a technical problem, ethical concern, or validity question. Second, relevant guidelines and research are reviewed. Third, alternative actions are considered. Fourth, the psychologist selects the most appropriate course of action and documents the rationale. This structured approach supports consistency and defensibility.

Summary

Case examples provide valuable insight into the application of technology in forensic evaluations. They highlight the importance of ethical awareness, careful observation, and informed decision making. By analyzing real world scenarios, psychologists can develop the skills needed to navigate the complexities of tele-forensic practice.

Section 12: Artificial Intelligence and Emerging Technologies in Forensic Evaluations

Introduction

The rapid development of artificial intelligence and related digital technologies is reshaping many areas of psychology, including forensic evaluation. These technologies include machine learning algorithms, natural language processing systems, digital phenotyping tools, and predictive analytics platforms. While these innovations offer potential benefits such as increased efficiency, improved data integration, and enhanced predictive capabilities, they also introduce significant ethical, legal, and scientific challenges.

Recent literature emphasizes that AI is not a replacement for forensic judgment but rather a tool that must be used cautiously and within established professional standards (Kennedy et al., 2023; Villarreal et al., 2025). In forensic contexts, where decisions have legal consequences, misuse or overreliance on AI can lead to serious errors and injustices.

Applications of Artificial Intelligence in Forensic Psychology

Artificial intelligence is increasingly being applied in areas such as risk assessment, behavioral prediction, and data analysis. Machine learning models can analyze large datasets to identify patterns that may not be apparent through traditional methods.

Digital phenotyping is another emerging application. This involves the use of data collected from digital devices, such as smartphones, to assess behavioral patterns. These data may include activity levels, communication patterns, and other indicators of functioning (Babu & Joseph, 2025).

While these applications offer potential benefits, they must be used with caution. The accuracy and validity of AI models depend on the quality of the data and the assumptions underlying the algorithms.

Benefits of AI and Digital Technologies

AI and digital technologies can enhance forensic practice in several ways. They can improve efficiency by automating data analysis and reducing administrative burden. They can also support consistency by applying standardized procedures across cases.

In addition, AI can assist in identifying patterns and relationships that may not be evident through manual analysis. For example, predictive models may help

identify risk factors associated with violence or recidivism. These tools may also support access to services by enabling remote monitoring and assessment. This is particularly relevant in underserved or rural areas.

Limitations and Risks

Despite their potential benefits, AI technologies have significant limitations. One major concern is algorithmic bias. If the data used to train an AI system are biased, the resulting predictions may also be biased. This can lead to unfair or discriminatory outcomes (Perlin et al., 2025).

Another limitation is the lack of transparency in some AI systems. Complex models may function as “black boxes,” making it difficult to understand how decisions are made. This lack of transparency can undermine legal defensibility.

AI systems also lack human judgment and ethical reasoning. They cannot fully account for context, nuance, or individual differences in the way that a trained forensic psychologist can.

Ethical Considerations

The use of AI in forensic psychology raises important ethical questions. Psychologists must ensure that the use of technology aligns with principles of beneficence, nonmaleficence, and justice.

Informed consent is a key consideration. Examinees should be informed if AI tools are being used and how their data will be processed. Privacy and data security are also critical, particularly when using digital phenotyping tools that collect continuous data.

Professional competence is another issue. Psychologists must have sufficient understanding of AI tools to use them appropriately. This includes understanding their limitations and potential sources of error.

Summary

Artificial intelligence and emerging technologies offer significant opportunities for advancing forensic psychology, but they also present substantial challenges. Psychologists must use these tools responsibly, with careful attention to validity, ethics, and legal standards.

Section 13: AI in the Forensic Opinion: What the Evaluator Must Be Able to Defend

Introduction

As artificial intelligence becomes increasingly integrated into forensic psychology, the central issue is no longer simply whether AI tools can assist with assessment or prediction, but whether the forensic evaluator can scientifically and ethically defend the use of those tools under legal scrutiny. In forensic contexts, any methodology contributing to an expert opinion may become the subject of judicial review, cross-examination, and evidentiary challenge. Unlike administrative or purely clinical applications of technology, forensic evaluations occur within adversarial legal systems in which methodological weaknesses can directly affect liberty interests, parental rights, sentencing outcomes, or civil commitment decisions. Accordingly, psychologists who incorporate AI-assisted tools into forensic work must be prepared to explain not only what the technology does, but

how it works, what limitations it carries, and whether its outputs satisfy accepted scientific and legal standards.

The use of AI in forensic psychology introduces a fundamental tension between technological efficiency and legal defensibility. Machine learning systems can process large datasets rapidly and identify statistical relationships beyond human analytical capacity. However, courts do not admit evidence simply because it is technologically advanced. Under legal standards governing expert testimony, forensic psychologists remain personally responsible for the opinions they present, regardless of whether portions of their analysis were assisted by algorithmic systems. This means that psychologists cannot defer responsibility to software developers, proprietary systems, or automated outputs. The evaluator must independently assess whether the AI-assisted methodology is scientifically reliable, appropriately applied, and sufficiently transparent to withstand judicial scrutiny.

Daubert and the Admissibility of AI-Assisted Forensic Opinions

The Daubert standard presents one of the most significant legal challenges for AI-assisted forensic practice. Under *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (1993), judges serve as gatekeepers responsible for determining whether expert testimony is based on scientifically valid reasoning and methodology. Courts evaluating expert evidence may consider factors such as testability, peer review, known or potential error rates, standards controlling operation of the technique, and general acceptance within the relevant scientific community. These criteria create substantial complications when AI-generated outputs contribute to forensic opinions, particularly when machine learning systems operate through opaque or proprietary processes.

Forensic psychologists using AI-assisted tools must therefore be prepared to explain how the underlying system generates conclusions. It is insufficient to state that an algorithm identified a risk pattern or produced a predictive classification. The evaluator must understand the methodological foundations of the tool well enough to articulate its training procedures, validation research, known limitations, and appropriate scope of application. If an evaluator cannot explain how the AI system arrived at its conclusions, the testimony may be vulnerable to exclusion or impeachment. Courts are increasingly skeptical of “black box” methodologies in which experts rely on outputs they cannot independently interpret or evaluate. In forensic contexts, this concern is especially pronounced because legal decision makers require transparency regarding how conclusions were formed.

The issue becomes more complicated when AI systems rely on proprietary algorithms that are not publicly disclosed. Some commercial risk assessment systems restrict access to their underlying computational models, citing intellectual property protections. However, forensic psychologists remain ethically responsible for understanding the tools they use. Reliance on proprietary systems that cannot be meaningfully explained may create conflicts with professional obligations related to competence, transparency, and scientific integrity. An evaluator who cannot answer methodological questions during cross-examination may appear to be offering conclusions based on technological authority rather than independent professional judgment.

Cross-Examination and Methodological Accountability

Cross-examination involving AI-assisted forensic opinions is likely to focus heavily on methodological transparency and reliability. Opposing counsel may question whether the psychologist understands the system’s design, whether the model

has been independently validated, whether error rates are known, and whether the tool has been validated for the specific population being evaluated. The evaluator must therefore be capable of articulating the scientific basis for using the technology in the specific forensic context at issue.

For example, if an AI-assisted violence risk tool contributes to a sentencing recommendation, the psychologist may be asked whether the model was validated across racial, socioeconomic, or psychiatric subgroups comparable to the examinee. Counsel may also inquire whether the algorithm has been peer reviewed, whether independent replication studies exist, and whether alternative explanations for the findings were considered. If the evaluator responds with generalized statements such as “the software calculated the risk score,” this may substantially undermine the credibility of the testimony. Courts expect forensic experts to demonstrate mastery of the methods underlying their opinions, not merely familiarity with the resulting outputs.

Additionally, psychologists must be prepared to explain how AI-generated findings were integrated into broader forensic reasoning. AI tools should not function as autonomous decision makers within forensic evaluations. Rather, they may serve as one source of information within a larger assessment framework that includes clinical interviews, behavioral observations, collateral data, record review, and psychological testing. The evaluator must be able to explain why the AI-assisted findings were considered relevant, how contradictory information was weighed, and why independent professional judgment ultimately guided the forensic opinion. Failure to demonstrate this analytical process may create the appearance that the evaluator abdicated professional responsibility to automated systems.

Algorithmic Bias and Racial Disparities in Risk Assessment

One of the most serious concerns involving AI in forensic psychology is the potential for algorithmic bias, particularly in risk assessment contexts involving documented racial disparities. Machine learning systems are only as reliable as the data on which they are trained. If historical datasets reflect systemic inequities within policing, sentencing, incarceration, or mental health systems, AI models may reproduce or amplify those inequities in future predictions. This problem is especially concerning in forensic contexts because risk assessment tools may influence decisions involving bail, sentencing, parole, civil commitment, or supervision intensity.

Research has demonstrated that some algorithmic risk assessment systems produce disproportionately elevated risk classifications for Black individuals compared to White individuals with similar behavioral histories. These disparities may emerge because historical criminal justice data are themselves shaped by unequal surveillance, arrest patterns, socioeconomic inequality, and systemic bias. As a result, AI systems trained on such data may interpret historically biased outcomes as predictive indicators of future risk. The algorithm may appear statistically sophisticated while still perpetuating structural inequities embedded within the training data.

Forensic psychologists must therefore critically evaluate whether AI-assisted tools have been assessed for demographic fairness, subgroup validity, and disparate impact. It is not enough to know that a tool predicts recidivism at an acceptable aggregate level. The evaluator must consider whether predictive accuracy varies across racial or ethnic groups, whether false positive rates differ substantially, and whether the model may reinforce existing disparities within the legal system. Ethical forensic practice requires psychologists to recognize that technological

neutrality cannot be assumed merely because decisions are generated algorithmically.

Importantly, algorithmic bias cannot be solved solely through technical adjustments. Even systems designed to remove explicitly racial variables may still produce biased outcomes if correlated variables function as indirect proxies for race or structural disadvantage. Factors such as neighborhood characteristics, employment instability, educational history, or prior justice system contact may reflect broader systemic inequalities rather than purely individual risk characteristics. Psychologists must therefore approach AI-assisted risk assessment with substantial caution and avoid overstating the objectivity of algorithmic outputs.

Professional Responsibility and Forensic Judgment

Ultimately, the forensic evaluator remains fully responsible for any opinion presented to the court, regardless of whether AI-assisted tools contributed to the analysis. The psychologist's role is not to serve as a conduit for algorithmic conclusions, but to critically evaluate all available information through scientifically grounded professional judgment. AI systems may assist with pattern recognition, data organization, or probabilistic analysis, but they cannot independently evaluate credibility, contextual nuance, developmental history, cultural variables, or ethical implications in the manner required for forensic decision making.

Psychologists using AI-assisted technologies must therefore maintain ongoing competence in both forensic methodology and technological literacy. This includes understanding the strengths and limitations of machine learning systems, remaining informed about emerging legal standards, and documenting how technological tools were used within the evaluation process. Courts increasingly

expect experts to justify the scientific basis of all methodologies contributing to forensic opinions, including digital and algorithmic tools. Accordingly, evaluators must be prepared not only to use technology competently, but also to defend its use rigorously under adversarial scrutiny.

Summary

Artificial intelligence is likely to remain an expanding feature of forensic psychological practice, particularly in areas involving predictive analytics, behavioral classification, and risk assessment. However, the legal and ethical responsibilities associated with AI-assisted evaluations are substantial. Under Daubert, psychologists must be able to explain the methodological foundations, validation research, limitations, and error potential of any AI tool contributing to forensic opinions. They must also address concerns related to algorithmic bias, demographic fairness, and the risk of reinforcing systemic inequities. Most importantly, psychologists must recognize that forensic responsibility cannot be delegated to automated systems. Regardless of technological sophistication, the evaluator remains accountable for ensuring that opinions are scientifically defensible, ethically grounded, and consistent with professional standards of forensic practice.

Section 14: Cultural Competence, Equity, and Access in Technology-Mediated Forensic Evaluations

Introduction

Cultural competence is a foundational requirement in forensic psychological practice and is explicitly tied to ethical obligations under the APA Ethics Code,

including standards related to competence, fairness, and avoidance of harm. In technology-mediated forensic evaluations, cultural competence extends beyond traditional considerations such as race, ethnicity, and language to include digital access, technological literacy, disability, and socioeconomic disparities. These additional variables can directly affect assessment validity, participation, and legal fairness.

Recent research emphasizes that digital mental health technologies, including telehealth and AI-supported systems, can both reduce and exacerbate disparities depending on how they are implemented (Babu & Joseph, 2025; Sheperis & Annan-Coultas, 2025). Forensic psychologists must therefore approach remote evaluations with an equity-informed framework that accounts for systemic and individual differences.

Expanding the Definition of Culture in Digital Contexts

In technology-mediated forensic work, culture must be understood broadly. In addition to traditional cultural variables, psychologists must consider “digital culture,” which includes familiarity with technology, attitudes toward remote communication, and access to digital resources.

For example, individuals from underserved communities may have limited experience with videoconferencing platforms, which can affect comfort, engagement, and performance. Similarly, older adults or individuals with cognitive impairments may struggle with digital interfaces, which can influence test results or interview responses.

Research on digital mental health highlights that unequal access to technology can create systematic biases in assessment outcomes (Sheperis & Annan-Coultas, 2025). These disparities must be addressed proactively to ensure fairness.

Language, Communication, and Interpretation

Language differences are a well-established challenge in forensic evaluation, and these challenges are amplified in remote settings. Telehealth platforms may introduce delays, reduce audio clarity, or complicate turn-taking, all of which can affect communication accuracy.

The use of interpreters in tele-forensic evaluations requires careful coordination. Interpreters must be qualified, impartial, and familiar with forensic contexts. The psychologist must also ensure that technology supports clear communication among all parties.

For example, in an immigration-related forensic evaluation conducted remotely, the psychologist may need to work with an interpreter across three separate locations. Ensuring stable connections and clear communication is essential to maintaining validity.

Psychologists should document the use of interpreters, the method of communication, and any limitations that may affect interpretation.

Socioeconomic Barriers and Access to Technology

Access to technology is not evenly distributed. Factors such as income, geographic location, and education level can influence access to reliable internet, appropriate devices, and private spaces for evaluation.

These barriers can affect both participation and performance. For example, an examinee completing a remote assessment in a crowded household may experience distractions that reduce concentration and affect results. Similarly, limited bandwidth may result in poor video or audio quality, affecting communication and observation.

Research on digital phenotyping and telehealth indicates that disparities in access can lead to biased data and inequitable outcomes if not addressed (Babu & Joseph, 2025). Forensic psychologists must assess these factors during the initial stages of evaluation and consider alternative arrangements when necessary.

Addressing Bias in Technology and Assessment Tools

Technology can introduce new forms of bias, particularly in AI-assisted tools and digital assessment platforms. Algorithmic bias may arise when training data do not adequately represent diverse populations, leading to inaccurate or unfair predictions.

An AI-based risk assessment tool trained on data from a specific population may not generalize to individuals from different cultural or socioeconomic backgrounds. This can result in overestimation or underestimation of risk.

Psychologists must critically evaluate the tools they use and avoid overreliance on automated outputs. Human judgment, informed by cultural competence and contextual understanding, remains essential.

Strategies for Promoting Equity

Promoting equity in tele-forensic evaluations requires intentional strategies. Psychologists should assess technological access and literacy prior to the evaluation and provide support as needed. This may include offering practice sessions, providing clear instructions, or arranging for alternative settings.

Assessment tools should be selected with consideration of cultural validity. When appropriate tools are not available, psychologists should acknowledge limitations and interpret results cautiously.

Documentation is also critical. Reports should include discussion of cultural and contextual factors that may influence findings.

Case Example

A forensic psychologist conducts a remote disability evaluation with an individual from a rural area with limited internet access. During testing, the connection is unstable, and the examinee appears frustrated and distracted.

The psychologist recognizes that these factors may affect performance and decides to supplement the evaluation with collateral information and reschedule portions of the assessment in a more stable environment. The report includes detailed documentation of these issues. This example illustrates how attention to equity and context supports more accurate and defensible conclusions.

Summary

Cultural competence in technology-mediated forensic evaluations requires an expanded framework that includes digital access, literacy, and systemic disparities. By addressing these factors, psychologists can enhance the fairness, validity, and ethical integrity of their evaluations.

Section 15: Documentation, Report Writing, and Testimony in Technology-Mediated Forensic Practice

Introduction

Documentation and report writing are central to forensic psychological practice and are essential for meeting APA continuing education and ethical standards. In

technology-mediated evaluations, documentation must include additional details that address the role of technology in the assessment process. These details are critical for ensuring transparency, supporting validity, and maintaining legal defensibility.

Forensic reports must clearly communicate methods, findings, and limitations in a manner that can be understood by legal professionals. When technology is used, the psychologist must explicitly address how it was implemented and how it may have influenced the evaluation.

Comprehensive Documentation Practices

Documentation in tele-forensic evaluations should include all standard elements of forensic assessment as well as technology-specific information. This includes the type of platform used, security features, date and time of sessions, identity verification procedures, and environmental conditions.

Psychologists should also document any deviations from standard procedures. For example, if a test was administered remotely rather than in person, this should be noted along with any supporting evidence for its use. Technical issues must be recorded in detail. This includes interruptions, connectivity problems, and any adjustments made during the session. Research emphasizes that thorough documentation enhances legal defensibility and supports the psychologist's ability to explain and justify their methods (Perle et al., 2025).

Report Writing in Technology-Mediated Evaluations

Forensic reports must adhere to APA guidelines, including clarity, objectivity, and reliance on evidence-based methods. When technology is involved, the report should include a dedicated section describing the use of technology. For example,

a report may include a statement such as: “The evaluation was conducted via secure videoconferencing due to logistical constraints. Identity was verified, and the examinee was observed to be alone in a private environment. Minor connectivity disruptions occurred and are noted in the behavioral observations section.” Such transparency allows the court to evaluate the credibility of the findings.

Addressing Limitations and Methodological Considerations

Acknowledging limitations is a critical component of forensic reporting.

Technology-mediated evaluations may involve limitations related to observation, environmental control, and test administration.

Psychologists should discuss how these limitations may affect interpretation and whether additional data sources were used to mitigate their impact. For example, if a cognitive test was administered remotely without full standardization, the psychologist should explain how this affects the interpretation of scores and whether conclusions are tentative.

Testimony and Legal Scrutiny

Forensic psychologists must be prepared to testify about their methods and conclusions. In cases involving technology, this includes explaining the rationale for using remote methods and addressing potential challenges.

Opposing counsel may question the validity of remote assessments, the reliability of digital tools, or the adequacy of observation. The psychologist must be able to provide evidence-based responses and demonstrate adherence to professional standards. For example, a psychologist may cite research supporting the use of

telehealth in forensic contexts while also acknowledging limitations and explaining how they were addressed.

Preparation for testimony should include review of documentation, familiarity with relevant research, and ability to communicate complex concepts clearly.

Case Example

A psychologist conducts a remote personal injury evaluation and prepares a report that includes detailed documentation of the technology used, testing conditions, and observed limitations. During testimony, the psychologist was questioned about the reliability of remote testing. Because the report includes comprehensive documentation and references supporting research, the psychologist can defend the methodology effectively.

Summary

Thorough documentation and clear reporting are essential for maintaining the integrity and defensibility of technology-mediated forensic evaluations. By providing detailed descriptions of methods and limitations, psychologists support transparency and credibility in legal contexts.

Section 16: Future Directions, Emerging Trends, and Continuing Competence

Introduction

The field of forensic psychology is entering a period of rapid transformation as courts, correctional systems, attorneys, healthcare systems, and public agencies

increasingly rely on digital technology, artificial intelligence, remote assessment platforms, electronic records, wearable devices, and large-scale data systems. These developments are reshaping how forensic psychologists collect information, conduct evaluations, interpret behavioral data, communicate findings, and defend opinions in legal settings. While these tools may improve efficiency, expand access, and support more systematic data integration, they also introduce significant risks related to privacy, validity, algorithmic bias, procedural fairness, and professional competence. For forensic psychologists, the central question is not simply whether emerging technology is useful, but whether it can be ethically, scientifically, and legally defended when used in evaluations that may affect situations such as liberty, parental rights, sentencing, civil commitment, disability determinations, or institutional placement.

Continuing competence is especially important because technology often evolves faster than professional guidelines, case law, and regulatory systems. Psychologists cannot assume that tools are appropriate for forensic use simply because they are commercially available, widely adopted, or marketed as evidence-based. The evaluator must understand how a tool works, what population it was validated on, what limitations apply, what forms of bias may be present, and whether its use is consistent with the referral question and legal standard. This expectation is consistent with the APA Ethical Principles of Psychologists and Code of Conduct, which requires psychologists to practice within the boundaries of competence, use assessment techniques appropriately, protect confidentiality, and avoid misrepresentation of findings (American Psychological Association, 2017). It is also consistent with the Specialty Guidelines for Forensic Psychology, which emphasize objectivity, transparency, adequate data, and awareness of the limits of forensic opinions (American Psychological Association, 2013).

Emerging Technologies in Forensic Practice

Emerging technologies in forensic psychology include artificial intelligence, machine learning, natural language processing, digital phenotyping, remote behavioral observation, wearable sensors, electronic records analysis, automated scoring platforms, and predictive analytics. These technologies may assist psychologists in organizing large volumes of data, identifying patterns in records, monitoring behavior over time, or supplementing traditional assessment methods. For example, AI-assisted document review may help identify inconsistencies across thousands of pages of records. Digital phenotyping tools may collect information about sleep, movement, communication patterns, or activity levels through smartphones or wearable devices. Remote platforms may permit access to examinees in rural areas, correctional settings, or hospitals where in-person evaluation is difficult.

However, forensic psychologists must avoid treating technological data as inherently more objective than traditional clinical data. Digital information is still shaped by context, measurement limitations, missing data, user behavior, device access, and interpretation. A wearable device may record reduced activity, but the meaning of that data depends on medical status, environmental restrictions, depression, pain, incarceration conditions, motivation, or device nonuse. Smartphone communication patterns may suggest social withdrawal, but they may also reflect poverty, restricted phone access, safety concerns, or legal advice not to communicate. In forensic settings, where conclusions must be defensible under cross-examination, psychologists must be prepared to explain not only what digital data show, but what they do not show.

Integration of AI and Human Judgment

The integration of AI and human judgment will be one of the most important future directions in forensic psychology. AI systems may be able to process large datasets and identify statistical patterns, but they cannot replace the evaluator's professional responsibility to interpret findings within the legal, clinical, cultural, developmental, and ethical context of a case. Forensic opinions require more than prediction. They require reasoning, explanation, attention to referral questions, consideration of alternative hypotheses, and acknowledgment of uncertainty. A risk score, algorithmic classification, or AI-generated summary cannot independently determine competence, criminal responsibility, parental capacity, mitigation, or violence risk.

Psychologists using AI-assisted tools must understand the difference between decision support and decision substitution. Decision support means that AI contributes one source of information that the psychologist evaluates alongside interviews, psychological testing, collateral records, behavioral observations, and legal criteria. Decision substitution occurs when the evaluator allows the algorithmic output to drive the conclusion without adequate independent analysis. The latter is ethically and legally problematic. Courts rely on expert witnesses because they possess specialized knowledge and can explain their reasoning. If a psychologist cannot explain how an AI tool contributed to an opinion, why it was appropriate for the case, or how limitations were addressed, the opinion may be vulnerable to challenge.

AI integration also requires attention to automation bias, which occurs when professionals overvalue algorithmic outputs because they appear objective, mathematical, or technologically sophisticated. In forensic contexts, automation bias can be especially dangerous because legal decision makers may also give undue weight to quantitative scores. Psychologists must therefore guard against

presenting AI-generated outputs as neutral facts. Instead, they should describe them as data points produced by a specific model, trained on specific data, with specific assumptions and limitations. The evaluator must remain responsible for determining whether the output is clinically meaningful and legally relevant.

A defensible integration model should include several steps. First, the psychologist should determine whether the AI tool is relevant to the referral question. Second, the psychologist should evaluate whether the tool has empirical support for the population and setting involved. Third, the psychologist should consider whether the tool has been tested for bias, subgroup validity, and error rates. Fourth, the psychologist should compare AI-generated information with other data sources. Fifth, the psychologist should document how the tool was used and what weight it was given. This approach helps preserve professional judgment while allowing technology to contribute appropriately to the evaluation.

Ethical and Regulatory Developments

Ethical and regulatory developments are likely to shape forensic technology use more aggressively in the coming years. Although professional guidelines currently provide broad principles regarding competence, confidentiality, informed consent, assessment validity, and data protection, AI-specific regulation is still developing. Forensic psychologists should anticipate increased scrutiny from courts, licensing boards, legislatures, and agencies regarding algorithmic tools used in legal decision-making. This is particularly true in criminal justice contexts, where AI-based risk assessment, predictive policing, pretrial decision tools, and correctional classification systems have raised concerns about transparency, racial disparities, and due process.

State-level AI legislation is emerging across the United States, with many proposals focused on algorithmic accountability, automated decision systems,

data privacy, and discrimination. Some legislative efforts seek to require agencies to inventory automated decision tools, conduct impact assessments, disclose when AI is used, evaluate disparate impact, and provide mechanisms for human review. Although laws vary by jurisdiction, the direction is clear: professionals using AI in high-stakes contexts will increasingly be expected to understand, document, and justify how automated systems influence decisions. Forensic psychologists should not wait for every jurisdiction to enact detailed rules before adapting their practice. Instead, they should begin building documentation habits and competency practices now.

Algorithmic accountability proposals are especially relevant to forensic psychology because many legal decisions depend on assessments of risk, credibility, capacity, dangerousness, or treatment need. These constructs are already complex when evaluated by humans. When AI systems are added, the potential for error becomes harder to detect unless evaluators understand the model's training data, validation studies, and limitations. Accountability frameworks often emphasize transparency, explainability, auditability, and fairness. Forensic psychologists should incorporate these concepts into their own practice by asking whether a tool has been independently validated, whether its error rates are known, whether it performs similarly across demographic groups, and whether its outputs can be explained in language understandable to legal decision makers.

Privacy regulation is another major future direction. Digital phenotyping, wearable monitoring, and mobile health tools may collect continuous or passive data, including location, activity, sleep, communication patterns, and physiological indicators. In forensic contexts, such data may become discoverable, subpoenaed, or used beyond the original purpose of collection. Psychologists must ensure that examinees understand what data are being collected, who will access the data, how long data will be retained, whether third-party vendors are involved, and whether the information may be disclosed in legal proceedings. Standard

informed consent language is often insufficient for these technologies. Consent must be specific, understandable, and tailored to the forensic context.

What Psychologists Should Do Now to Prepare

Forensic psychologists should take proactive steps to prepare for the technological and regulatory future of the field. First, psychologists should develop a technology competence plan. This plan should identify the digital tools used in practice, the purpose of each tool, the evidence supporting its use, known limitations, security features, and any training completed. This type of self-audit is consistent with continuing competence expectations and can help psychologists identify areas where additional training or consultation is needed.

Second, psychologists should create documentation templates for technology-assisted evaluations. Reports should specify when AI tools, digital platforms, remote procedures, or digital collateral sources were used. The report should explain why the tool was appropriate, what limitations were present, and how findings were integrated with other data. If technological problems occurred, such as internet disruption, audio delay, restricted camera view, or missing digital data, these limitations should be documented. In forensic settings, failure to document technological limitations may create vulnerabilities during cross-examination.

Third, psychologists should evaluate vendors carefully. Vendor selection should not be treated as an administrative task. Psychologists should ask whether the vendor provides information about validation, data security, encryption, data retention, third-party access, breach notification, and use of client data for model training. If a vendor cannot answer basic questions about data handling or validation, the tool may not be appropriate for forensic use. Psychologists should also avoid assuming that institutional approval automatically resolves ethical concerns. The individual evaluator remains responsible for competent use.

Fourth, psychologists should prepare for cross-examination involving technology. Attorneys may ask whether the psychologist understands the AI tool's methodology, whether the tool has known error rates, whether it has been independently validated, whether it has been tested across demographic groups, whether the examinee had equal access to the technology, and whether any technical problems affected the evaluation. Psychologists should be able to answer these questions clearly and without overstating science. If the evaluator cannot explain the tool, the evaluator should not rely heavily on it.

Fifth, forensic psychologists should participate in continuing education focused on AI, teleassessment, cybersecurity, digital ethics, and forensic technology. Continuing education should not be limited to general technology awareness. It should include applied forensic topics such as Daubert challenges to algorithmic evidence, digital data admissibility, privacy in remote evaluations, bias in risk assessment, and report writing for technology-assisted evaluations. Consultation with legal professionals, data scientists, and experienced forensic colleagues may also be necessary.

Case Example

A forensic psychologist begins using a digital phenotyping tool to supplement evaluations. Recognizing the novelty of the technology, the psychologist completes specialized training, reviews current research, and consults with colleagues.

The psychologist uses the tool cautiously, integrates its findings with traditional assessment methods, and clearly documents its use and limitations in reports. This example demonstrates responsible adoption of new technology.

Summary

The future of forensic psychology will be shaped by technological innovation. By engaging in continuous learning, maintaining ethical awareness, and integrating new tools thoughtfully, psychologists can adapt to these changes while preserving the integrity of their work.



References

- Abascal, A. M., Lillard, C. M., & Law, K. B. (2024). Curriculum development for competencies in forensic telemental health evaluations. *Journal of Technology in Behavioral Science*.
- Ales, F., Meyer, G. J., Mihura, J. L., & Loia, A. C. (2023). Can the Rorschach be administered remotely? A review of options and a pilot study using a newly developed R-PAS app. *Psychological Injury and Law*, 16, 217–235.
- Alva, J. I., Brewster, R. C., & Mahmood, Z. (2025). Are tele-neuropsychology and in-person assessment scores meaningfully different? A systematic review and meta-analysis. *The Clinical Neuropsychologist*.
- Babu, A., & Joseph, A. P. (2025). Repositioning intellectual disability in the ethics of digital mental health technologies. *Frontiers in Psychiatry*.
- Frederick, R. I., Mikesell, J. W., & Otto, R. K. (2024). Ethical considerations for demands for evidence in forensic examinations. *Journal of Forensic Psychology Practice*. Advance online publication.
- Geraldo, A., Dorés, A. R., & Mendes-Santos, C. (2024). Guidelines for the provision of remote psychological services. *European Psychologist*.
- Giromini, L., Pignolo, C., Zennaro, A., & Sellbom, M. (2024). Using the MMPI-2-RF, IOP-29, IOP-M, and FIT in in-person and remote administration formats: A simulation study on feigned mild traumatic brain injury. *Assessment*.
- Gowensmith, W. N., & McCallum, K. (2024). Using a mobile app to identify base rates and monitor bias in forensic evaluation. *Journal of Forensic Psychology Research and Practice*, 24(1), 35–52.

- Johnstone, K. L., Martin, C., & Blades, M. (2024). The digital witness: Exploring gestural misinformation in tele-forensic interviews with children. *Journal of Nonverbal Behavior*.
- Karachaliou, E., Douzenis, P., & Martinaki, S. (2024). A systematic literature review on the application of telepsychiatry in correctional facilities: Necessity and modern challenges. *Journal of Technology in Behavioral Science*.
- Kennedy, T. D., Woods, S., Anillo, I., & Caggiano, C. (2023). Child and adolescent forensic evaluations: Challenges amid scientific and technological advancements. *Practice Innovations*.
- Kirschstein, M. A., & Singh, J. P. (2023). International survey on the use of emerging technologies among forensic and correctional mental health professionals. *Criminal Justice and Behavior*, 50(4), 567–589.
- Knight, V., Ross, S., & Wood, M. (2024). Digitalising corrections: Telepsychology and videoconferencing in justice settings. *Journal of Criminology*.
- Neal, T. M. S., & Brodsky, S. L. (2016). Forensic psychologists' perceptions of bias and potential correction strategies in forensic mental health evaluations. *Psychology, Public Policy, and Law*, 22(1), 58–76.
- Perle, J. G., Smucker-Barnwell, S., & Morland, L. A. (2025). A compendium for the 2024 APA guidelines for the practice of telepsychology: Guideline applications and resources. *American Psychologist*.
- Perlin, M., Ellis Cucolo, H., & Kulesza, J. (2025). Artificial intelligence, algorithmic bias, and mental disability law: Ethical challenges and regulatory solutions.
- Procaccia, R., Verde, A., & La Via, V. (2024). Forensic assessment via videoconferences in family law proceedings: From pandemic experience to future practice.

- Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, 1(5), 206–215.
- Sablone, S., Bellino, M., & Lagona, V. (2024). Telepsychology revolution in mental health care delivery: Clinical and legal issues. *Forensic Sciences Research*, 9(3), owae008.
- Shahvaroughi, A., Bahrami Ehsan, H., & Hatami, J. (2022). The cognitive interview: Comparing face-to-face and video-mediated interviews. *Journal of Criminal Psychology*, 12(4), 74–90.
- Shura, R. D., Sapp, A., Ingram, P. B., et al. (2024). Evaluation of telehealth administration of MMPI symptom validity scales. *Journal of Clinical and Experimental Neuropsychology*.
- Sheperis, C. J., & Annan-Coultas, D. L. (2025). Reimagining the counseling profession: Preparing counselors for AI and digital health integration. *Journal of Counselor Preparation and Supervision*.
- Skala, J., Chavez, J. X., & Anderson, K. (2023). Examiners' perceptions of forensic mental health assessments conducted via videoconferencing. *Behavioral Sciences and the Law*, 41(6), 913–930.
- Sperling, S. A., Acheson, S. K., & Fox-Fuller, J. (2024). Tele-neuropsychology: From science to policy to practice. *Archives of Clinical Neuropsychology*, 39(2), 227–240.
- Villarreal, R. I., Singhal, S., & Dempsey, A. G. (2025). The future of digital mental health: A literature review. *Psychiatric Clinics of North America*.

- Voultsiou, E., & Moussiades, L. (2026). A systematic review of large language models in mental health: Opportunities, challenges, and future directions. *Electronics*, 15(3), 524.
- Wibberly, K. H. (2024). Preparing mental health providers for the future: Integrating telehealth training into professional education. *Frontiers in Psychology*.
- Yıldırım, E., Büyükişcan, E. S., Kalem, Ş. A., & Yıldız, M. (2024). Remote neuropsychological assessment: Teleneuropsychology. *Archives of Neuropsychiatry*, 61(2), 167–174.
- Young, G. (2024). Remote neuropsychological assessment: Forensics, research, and ethics. *Psychological Injury and Law*.
- Young, G., Rogers, R., Giromini, L., & Erdodi, L. (2025). Invalid response set and malingering in the field of psychological injury and law II: New topics. In *Handbook of Psychological Injury and Law*. Springer.





The material contained herein was created by EdCompass, LLC ("EdCompass") for the purpose of preparing users for course examinations on websites owned by EdCompass, and is intended for use only by users for those exams. The material is owned or licensed by EdCompass and is protected under the copyright laws of the United States and under applicable international treaties and conventions. Copyright 2026 EdCompass. All rights reserved. Any reproduction, retransmission, or republication of all or part of this material is expressly prohibited, unless specifically authorized by EdCompass in writing.