Ethically Using Technology in the School Psychologist's Practice - Handout

October 10, 2015

Presented by

Dan Florell - Eastern Kentucky University

TASP 2015 Convention – San Antonio, TX

Learning Objective:

1. Participants will be able to identify ethical standards that relate to using technology.
2. Participants will be able to describe questions that should be asked prior to using particular technologies to ensure the maintenance of client confidentiality and privacy.
3. Participants will be able to describe common ethical pitfalls when using technology.

Laws and Digital Records

- Family Educational Rights and Privacy Act (FERPA)
  - FERPA was enacted in 1974 and provides certain minimum privacy protections for educational records.
  - FERPA was passed to protect the privacy of student educational records by regulating to whom and under what circumstances those records may be disclosed.
  - FERPA applies to educational agencies and institutions that receive federal funds administered by the Secretary of Education.
- The Protection of Pupil Rights Amendment (Hatch Amendment of 1978)
  - Applies to state or local education agencies that receive funding from the United States Department of Education.
  - Specifically, it ensures the rights of students and parents surrounding the collection and use of information for marketing purposes as well as information regarding certain physical exams.
- Children's Online Privacy Protection Act of 1998 (COPPA)
  - Empowers the FTC to regulate the operators of commercial websites or online services targeted to children in the collection and use of personal information obtained from children. COPPA defines "personal information" to include
    - (1) a first and last name; (2) an address; (3) an e-mail address; (4) a telephone number; (5) a Social Security number; or (6) any other identifier that the FTC may determine permits the physical or online contacting of a specific individual.
  - If a website is directed at children or the operator knowingly collects personal information from children under 13, COPPA requires that the website obtain parental notice and consent.
- Health Insurance Portability and Accountability Act (HIPAA)
  - "Covered entity," which is a health plan, healthcare clearinghouse, or any healthcare provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA.
  - A school that is not covered by FERPA may be a covered entity if it provides health services for which it transmits health information electronically, such as submitting claims for payment from a health plan.

- Health Information Technology for Economic and Clinical Health Act (HITECH) – Part D Privacy
    - Requires HIPAA covered entities to report data breaches affecting 500 or more individuals to HHS and the media, in addition to notifying the affected individuals.
    - This subtitle extends the complete Privacy and Security Provisions of HIPAA to business associates of covered entities.
    - New rules for the accounting of disclosures of a patient's health information. It extends the current accounting for disclosure requirements to information that is used to carry out treatment, payment and health care operations when an organization is using an electronic health record (EHR).
- Privacy Technical Assistance Center (PTAC) - US Dept. of Education
    - Offers guidance to school regarding the various laws regarding student privacy and confidentiality (http://ptac.ed.gov)
- Most tech ethics questions center on confidentiality and privacy and the impact it has on the client's well being.
    - Who owns the information?
    - Where is the information being stored?
    - How is the information being stored?
    - How long is that information going to be stored?
    - Who has access to the information?
    - What safeguards are in place?

Getting to This Point

- Time of Flux and Change
    - Crisis = Danger + Opportunity (Chinese)
    - Affordable Healthcare Act "goes to school"/ HIPAA & HITECH
    - Federal Funds – health care impact on school services
    - Electronic Leaks - Snowden (NSA) & Manning (Army) on electronic access and records
- Your Digital Footprint
    - Facebook – Timeline!, Online Photos – tagging, Cell phone – location, Google – Locator, Skype/VOiP, Emails, Browsing history

Basic Risk Management

- Standard of Care: Reasonable and Prudent
- Psychologist (J. Younggren, 2013)
    - Judicial: How similarly qualified practitioners would
        - have managed the patient's care under the same or similar circumstances
    - Must have and use the knowledge ordinarily possessed by members of the profession in good standing
    - Ethical**:** As used in this Ethics Code, the term
        - Reasonable means the prevailing professional judgment of psychologists engaged in similar activities in similar circumstances, given the knowledge the psychologist had or should have had at the time.

- Keys to Success
    - Informed Consent – records including electronic transmission and storage
    - Appropriate consultation with others
    - Good record keeping practices and strategies
- Risk Management
    - It can get you in trouble, if you "mess up"
    - Ignorance is not BLISS – "Standard of Care"
    - Professional ethics and technology do overlap
    - If in doubt – pause or ask a colleague
    - Grad Student v school psychologists have the same requirements with the exception of report modification by Supervisor.
    - Data management
        - Storage – cloud/CD/DVD/external hard drive
        - Lost data/computer/USB data stick
        - Password protect it – folders and files (different from encryption)
    - Copiers – may store your copies
    - E-mails are open and available to everyone
    - Master files/reports – who can access?
    - "Other files" – not protected/computer access

Tech Ethics Overview

- APA and NASP do NOT have specific guidelines for ethical use of technology.
- General APA Ethical Guidelines apply to technology as well; hard to keep up with changes but must demonstrate an effort to comply.
    - APA General Principles
        - Privacy and Security, Competence
        - Confidentiality
        - Nonmaleficence
        - Informed Consent
        - Safety (self-disclosure)
    - APA covers many different aspects including loss of data; having written policies and social media with clients (see also APA Guidelines for Telepsychology, 2013).

NASP

- NASP General Principle:
    - Data protection; testing materials updated
    - "Need to Know" provisions and electronic access
    - Be involved in developing district policies development on technology; be clear of your concerns if issues arise (paper trail)
- Issues to Consider:
    - Relationship with a client ("like"?)/be my friend
    - Learning about clients online/they learn about you online
    - Must have personal practice guidelines about disclosure
    - More training about technology is needed and keeping up to date will be a challenge

  - Policies on technology failure; accidental disclosure; e-mail, storage of information (cloud)
  - Need to define professional roles vs. personal roles in social media
- The NASP Principles in the **Preamble** state that "we must protect all students from reasonable foreseeable risk of harm."
- Principle I – **Respecting the Dignity and Rights of all Persons -** nothing here on technology
- Principle II – **Professional Competence and Responsibility**
  - Standard II, 3.2, - use assessment techniques and practices that the profession considers to be responsible, research-based practice. We have to have **up-to-date instruments and appropriate normative data**. If using **computer-assisted assessments**, computer scoring and/or interpretation programs, they must be accurate and valid.
  - Standard II.4 – **Responsible School-Based Record Keeping**,
    - Standard II. 4.1 notes: "Parents … are notified of electronic storage and transmission of personally identifiable school psychological records and the associated risks to privacy."
    - Standard II. 4.5 - release of information to outside agencies. This has typically been done with a signed release (good practice), but that does not address the HIPAA guidelines for releases.
  - Standard II.4.6 - "to the extent that school psychological records are under their control, school psychologists ensure that only those school personnel who have legitimate educational interests in a student are given access...."
  - Standard II.4.7 – protection with password or encryption. The other area that is clearly addressed is "records are not lost due to equipment failure." e.g. hard drive crash.
  - Standard II.4.9 states "school psychologists ... work to establish district policies regarding the storage and disposal of school psychological records that are consistent with law and sound professional practice."
- Standard III **— Honesty and Integrity in Professional Relationships**
  - Standard III.3.3 states that "one cannot alter a report or record of another professional without their permission. The exemption is for those supervising graduate students."
  - Standard III.4.6 speaks to having a financial interest in a product. Software is specifically mentioned.
- Standard IV — **Responsibility to Schools, Families, Communities, the Profession, and Society**
  - Standard IV.- 5.1 concerns research and methods, data collection, etc.
  - Standard IV.- 5.2 includes institutional research board (IRB) oversight. These are conditions about which graduate students are informed in their studies, but may fall behind in during field practice. Security of records, appropriate data collection, informed consent, record/protocol storage, etc. are essential under these standards.
  - Standard IV.- 5.5 concerns making research data available if needed for conclusions reported in publications or presentations. Backing up data sets to a safe place may protect you here

- Digital records include – written notes, digitized/scanned files or report, e-mail, text/SMS messages, audio files, and video files.

HIPAA - **Privacy Rule** intentional disclosure of PHI & **Security Rule** unintentional or malicious disclosure or loss of record (only electronic records). No mandated protection methods under the law. **"reasonableness"** feature under ethics.

- Examples: passwords, digital signatures, firewalls, data encryption, encryption over public networks, backup systems, and disaster recovery plan.
- Check email address before responding

Sample Language to Use

- Reference IDEA, FERPA, and HIPAA
  - HIPAA language may be optional
- Section
  - Type of Information We Collect and How We Collect It
    - Includes definition of Personally Identifiable Information
  - Effective Date and Changes to Privacy Notice
  - Outline Parent Rights re: Child Records
    - List types and location of information
    - List whom information has been shared with
    - Ask to limit what we share
    - Request communication method
    - Other use of information and withdraw of consent
    - Filing a complaint
  - Uses of records by district
  - When share information without prior consent
  - See end of handouts for sample from KY First Steps

Hot Spots for Ethical Violations

- Facebook & Timeline - yours
- Copiers – hard drive copies
- Faxes – not secure or confidential; no cover sheet
- Lost USB FOB – not password protected or encrypted
- No password protection of data; smartphone
- No firewall on computer; no anti-virus program or out of date
- Software out of date (scoring and OS)
- "Reply all"; email
- Administrative access to files; who can modify
- Electronic files & storage; cloud options
- No back-up of files
- VOIP – Skype / Google Chat / VSee
- Don't email reports / files to yourself

E-mail - Typically least protected for student confidentiality

- HIPAA Best Practice Recommendations (Oliver, Oct 2013):
  - Use only sanctioned email providers
  - Email to only one recipient at a time
  - Notify parents prior to using email
  - Recommend parent provide personal over work email
  - Verify recipient email address prior to sending
  - Include "Unintended Recipient Directions"
  - Limit confidential info to attachments only
  - Utilize password protection on documents
  - Tag email communities as "Confidential"
  - Utilize "Expiration" feature (5 days)
  - Mask personal identifiable information
- Sample e-mail confidential disclaimer
  - ***Confidentiality Warning:*** *This e-mail contains information intended only for the use of the individual or entity named above. If the reader of this e-mail is not the intended recipient or the employee or agent responsible for delivering it to the intended recipient, any dissemination, publication or copying of this e-mail is strictly prohibited. The sender does not accept any responsibility for any loss, disruption or damage to your data or computer system that may occur while using data contained in, or transmitted with, this e-mail. If you have received this e-mail in error, please immediately notify us by return e-mail. Thank you.*

"Discoverable" Information – records, text/SMS, e-mails, computer use history, personal information/profile, electronic transmissions (Skype), web sites, Twitter, blogs, social networks, and voicemail.

- Bring Your Own Device (BYOD) – have separate accounts on computer (use Administrator function to do) and have a work and personal cell phones. Otherwise devices that are work/personal are considered work.

Passwords:

- Don't be obvious
- Don't use existing online passwords
- Don't use a regular word
- Mix cases, number, and punctuation
- Change passwords regularly
- Don't share password or write down
- Create hierarchy of passwords
- Examples:
  - Aquarius Time to Crack - 9.08 minutes
  - Aquarius1 Time to Crack – 1.59 Days
  - Aquar$ius1 Time to Crack – 19.24 Years
  - Aqu57ar$iu3s Time to Crack – 17,400,000 Yrs
- Caps/case do count too; have unique password for EACH account
- Some servers do not allow symbols; insert CAPS in middle or end
- Thieves will use your "forgot password" access

- Password Sites and Storage:
    - Gibson Corp Password Haystacks – www.grc.com (Click on Services)
    - KeePass (Free) – www.keepass.info
    - LastPass (Free) – www.lastpass.com
    - SplashID – Key Safe/App

Security Questions

- Another layer of protection
- Misspell the street you grew up on or your first boy/girlfriend.
- Use street name of your best friend and you know!
- Security question hints to make it harder to guess.

Encryption - important for files, folders, and hard drives and USB/SD.

- 256 bit preferred
- HIPAA – not apply to schools
    - Personal Health Information (PHI)
    - Word processing files transmitted electronically
    - E-mail between psychologist and patient
- At least password protect it.
- Do not email file to yourself!
- Emails – Hushmail.com
- Files/Folders – Microsoft Office Suite
- Disks/Drives – TrueCrypt; BestCrypt Enterprise; PGP Whole Disk; BitLocker (Windows); BitTorrent
- Password protection is NOT encryption
    - iPhone is encrypted when locked; Android requires several steps – Password plus Security Password (not reversible) ; if locked - police cannot search without warrant (California)
    - FaceTime is secure format (iPhone)
- Dropbox – sharing
    - Viivo/PKWARE(from Dowlnoad.com) – All devices
    - Or Viivo.com
- BoxCryptor (www.boxcryptor.com) – all OS + Mobile

Archiving Data

- Focus on if data will be available in future and how can store it securely.
- Blu-Ray Disk – gold plated is best; followed by SDHC card; then SSHD, then HD, then CD
- Storage format is critical too – PDF, txt. etc.
- Check backups periodically to see if they work!
- Long term storage is an issue that requires planning

Cloud Computing

- Advantages
    - Allows access to and manipulation of files
    - Information accessed from anywhere
    - Reduces risks of files being lost or stolen
    - Allows for collaboration
    - Resource and time consciousness
- Disadvantages
    - Privacy and security of files
        - Encryption options improving
    - Who owns the data??
        - Very important – read the fine print
    - Legal liability
    - Lack of standardization
- Cloud Storage Services
    - Sample companies – Iron Mountain, Mozy, ADrive, CrashPlan & Carbonite
- Assessment – trend is to changing software and instruments to cloud platform
    - Examples include Pearson Q Local & Assess, MHS, PAR iConnect
    - Need to ask questions regarding ethical issues of scoring and storage of results.
    - These systems will also have smartphone apps associated with them.

Tech Ethics Questions to Ask

- Most tech ethics questions center on confidentiality and privacy and the impact it has on the client's well being.
    - Who owns the information?
    - Where is the information being stored?
    - How is the information being stored?
    - How long is that information going to be stored?
    - Who has access to the information?
    - What safeguards are in place?
    - Which has greater security capabilities?
    - What are the vulnerabilities of the cloud?
    - Is there incident detection/response?
    - Look at security monitoring
        - How will you exercise control over data?
        - What are potential legal concerns?
        - Does it comply with FERPA?

Cloud Assessment

- Pearson
    - Q Global – includes some assessments including WISC-V, WIAT-III, WPPSI-IV, WAIS-IV
        - Over 30 measures are available
        - Administer measures on screen
        - Scores automatically and provides a report
    - Saves time but not necessarily money
    - Increased flexibility in administration and scoring (cross battery allowed)
    - Practitioner owns the data
    - Information stored on servers in Toronto and back-ups in Vancouver
    - HIPAA and HITECH Compliant
- Hougton Mifflin – Riverside –controversy regarding storage of records indefinitely and user can't delete information.
    - Data can be used in research once de-identified
- MHS - rating scale cloud scoring and e-mail of rating scales
- PAR – iConnet administer instruments, interpret results, and examine client assessment
    - Saves time but not necessarily money
    - Increased flexibility in administration and scoring (cross-battery not allowed)
    - Practitioner owns the data
    - Information stored on servers in Tampa Bay with back-up servers elsewhere
    - Saved for 3 years from last accessed
    - HIPAA Compliant

Schools and Cloud Computing – Infinite Campus and AIMsweb examples

- Most school districts have in-house servers restricted to use only in district
- States have embraced state-wide cloud systems
    - 95% of districts rely on cloud services for data mining related to student performance, support for classroom activities, student guidance, data hosting, and special services like cafeteria payments and transportation planning
- FERPA and Cloud
    - Contractually identify cloud vendor as a "school official" under "direct control" of the education institution
    - Five principles for schools to follow:
        - Maintain control of student data
        - Expressly prohibit the mining of student data for advertising and marketing purposes
        - Enter into a comprehensive agreement covering all of the cloud services provided to the education institution
        - Consider how providers may use anonymized data
        - Conduct due diligence into the cloud service provider's practices with respect to student data

- COPPA and Schools
    - Information on children under 13 do the following:
        - Provide parental notice of their information practices
        - Obtain prior parental consent for collection, use, and/or disclosure of personal information from children
        - Empower parents, upon request, to review the personal information from their children
        - Provide a parent with the opportunity to prevent further use of personal information that has already been collected or the future collection of personal information from that child
        - Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information
    - To the extent that data analytics services collect information directly from school children or enable the tracking of school children based on their interactions with the cloud service, COPPA obligations would apply
- Fordham Law Center (2013) – findings of schools and cloud services
    - 25% of districts inform parents of their use of cloud services
    - 20% of districts fail to have policies governing the use of online services
    - 25% of the agreements specify the purpose for disclosures of student information, fewer than 7% of contracts restrict the sale or marketing of student information by vendors, many allow vendors to change the terms without notice
    - The majority of cloud service contracts do not address parental notice, consent, or access to student information
    - School district cloud service agreements generally do not provide for data security and even allow vendors to retain student information in perpetuity with alarming frequency
- School Psychologists and Cloud Computing
    - School psychologist often mandated to use school cloud services for records.
    - Many districts are violating FERPA and COPPA issues regarding student information disclosure in general.
    - What about protected populations being served?
    - School psychologists are responsible for protecting this data.

Contact the Presenters

- Dan Florell – Eastern Kentucky University
    - Dan.florell@eku.edu
    - Twitter: @schoolpsychtech
    - Facebook: "Like" MindPsi
    - Web: www.mindpsi.net
    - YouTube: School Mental Health Minute channel