# legal notes

By Daniel Pollack

Legal Benefits of Mobile Digital Documentation for Human Services Agencies

Documentation is one of the most crucial aspects of proof that workers meet their required legal standard of care. Many of the advantages of digital documentation over paper documentation are self-evident. Digital documents:

- can be edited.
- are instantly accessible.
- lend themselves to audit and compliance inspection.
- are less likely to be lost.
- are easily duplicated.
- are easily stored.
- ensure a consistency and conformance of reporting style.
- are easily retrieved.
- are secure.
- are usually searchable.
- can be easily shared.
- are cost-effective.
- are accessible to many workers simultaneously.
- are environmentally friendly.
- can be seamlessly integrated with back-office systems.

With all the above advantages, is there room for improvement? One of the most important concerns is the need to allow workers to record narrative notes without being bound by their office computer.

During the busiest part of the day a residential group home worker on a field trip realized that the medicine he was supposed to administer to a client had run out. He called his supervisor for assistance. The supervisor said she'd take care of getting more medicine and would ensure that the client received it. In the rush of the day's activity the supervisor forgot to follow up and the worker never
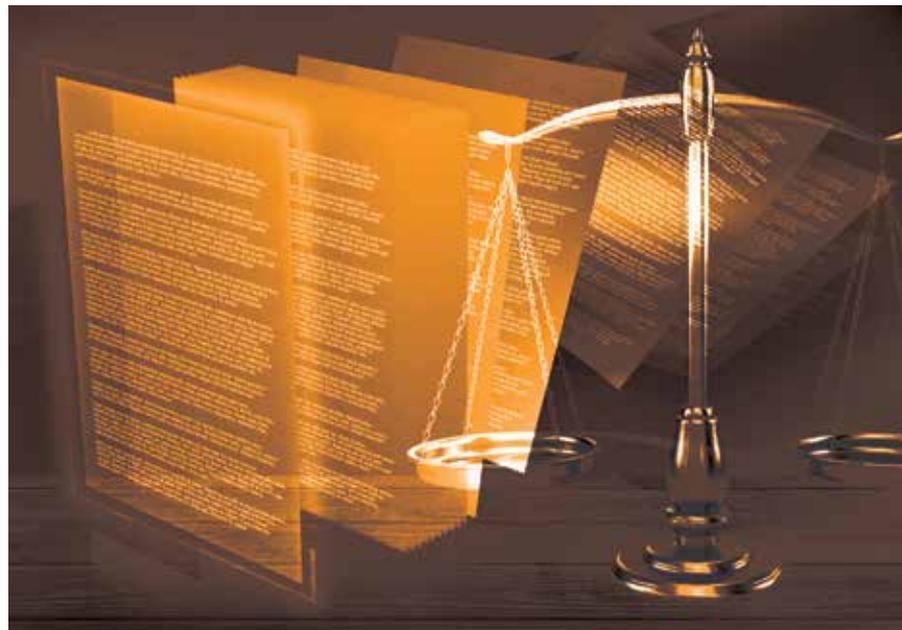
documented the phone call. When the client subsequently sustained lasting medical damage and a lawsuit was filed, the digital record was no help to the worker. The worker had recorded his conversation on paper but had never transferred it to the digital record. The supervisor had not recorded the incident at all. A contemporaneous verbal note via mobile technology to the electronic file by the worker would have been the crucial piece of evidence to provide legal cover for him.

The recent headline, "Arizona Department of Child Safety going mobile" should not really be news.[1] With the ubiquitous availability of mobile technology via smartphones and tablets, human services agencies need to ensure that client records can be easily accessed while workers are in transit. Yes, there are barriers to moving to this technology—cost, education, and training—but financial barriers are coming down, and education and training are as much a matter of commitment as anything.

Failures in internal and external communication come up as a major factor in lawsuits against human services agencies and their employees. Cloud technology allows agencies to share information instantaneously from any location. No delays. Few additional costs. Even official signatures can be obtained through eSignature platforms.

Missouri attorney Rebecca Randles observes, "Lawsuits are supposed to hold providers accountable, ensuring quality client and patient care. For a lawsuit to go forward, something terribly wrong must have happened.

Illustration by Chris Campbell

measures and using procedures to effectively manage identities. As with all forms of cybercrime, however, the criminals continue to evolve and find new methods of defrauding these systems; putting the onus back on these programs to develop stronger protections and stay ahead of the criminals.

Currently, agencies may access the Federal Hub to verify identities; the hub provides Remote Identity Proofing using information from one of the credit bureaus. This is a step in the right direction, but has limitations: for example, individuals with limited credit histories, identity theft victims, immigrants, and non-English speaking citizens all would have problems with identity verification. Additionally, if someone were to steal a credit report, they would essentially have a cheat sheet to pass authentication. So while this is a good step, it just isn't enough.

Effective identity management is more than simply verifying a name or Social Security number (SSN). Looking at identity as a comprehensive network of data points, both current and historical, provides a much more robust basis upon which to build a strong identity management system. Using an identity repository that includes demographics (name, date of birth, SSN, address history, and so on), asset information (homes, vehicles, boats, bank information, etc.) and legal information (such as criminal records, liens, and court judgments) provides an evolutionary record of how an individual's identity has changed over time. LexisNexis Risk Solutions uses information from more than 10,000 different data sources to build a comprehensive, ongoing view of an individual's identity from which to build multi-faceted solutions that meet clients' identity management needs—all while maintaining a positive user experience for the majority of non-fraudulent applicants.

Using this kind of multi-layered approach to identity authentication serves a much broader patient base, because it provides verifications for identities at risk of not being verified by using older, traditional methods… and does it with stronger protections and lower false positives. And, while it steps up fraud prevention and deterrence, it has the even larger benefit of facilitating greater system efficiencies and much more positive user experiences.

All stakeholders in the government health care ecosystem bear financial and non-monetary costs of identity theft—some to a greater degree than others. The health of every patient is at risk and we need to protect that. Finding better ways to verify the authenticity of members' identities while delivering services more cost effectively promises long-term relief, better outcomes for your members, and, overall, much stronger programs that your constituents can rely on. ▣

Justin Hyde is the Director of Market Planning, Health and Human Services, for LexisNexis Risk Solutions.

Reference Notes
1. See *http://www.kff.org/medicaid/state-indicator/total-medicaid-spending/?currentTimeframe=0&sortModel=%7B%22colId%22:%22Location%22,%22sort%22:%22asc%22%7D*
2. See *https://www.hhs.gov/sites/default/files/fy-2016-hhs-agency-financial-report.pdf*
3. See *https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/*
4. See *https://www.usatoday.com/story/money/personalfinance/2015/03/28/the-new-kind-of-identity-theft-you-havent-heard-of/25091257/*
5. See *http://www.idtheftcenter.org/images/breach/2017Breaches/DataBreachReport_2017.pdf*
6. See *http://sonorannews.com/new/2017/05/09/arizona-department-child-safety-going-mobile/*
7. See *http://sonorannews.com/new/2017/05/09/arizona-department-child-safety-going-mobile/*
8. See *http://sonorannews.com/new/2017/05/09/arizona-department-child-safety-going-mobile/*
9. See *http://sonorannews.com/new/2017/05/09/arizona-department-child-safety-going-mobile/*
10. See *http://sonorannews.com/new/2017/05/09/arizona-department-child-safety-going-mobile/*

Cloud technology has the capacity for increasing the quality of care and making it more difficult for negligence to occur. We had a case in which a defendant mental health technician assigned to regular 15-minute watches did not make his rounds. Nonetheless, he initialed his forms, photocopied them and put each one in the appropriate patient record. Our client died when the defendant was off unit. With real-time communication and the supporting metadata, this kind of malfeasance would be more easily caught and, likely, our client would have lived. Mobile technology allows for proactive solutions that can truly save lives."

Consumers are demanding a digital world that is accessible on demand, versatile, and customizable. That kind of mobile technology is here. The convergence of cloud technology and social media have spurred innovations in computer documentation today that have the potential to renew and reshape human services tomorrow. The end result will be an improved quality of life for our clients. ▣

Daniel Pollack is a professor at Yeshiva University's School of Social Work in New York City. He can be reached at dpollack@yu.edu; (212) 960-0836.

Reference Note
1. See *http://sonorannews.com/new/2017/05/09/arizona-department-child-safety-going-mobile/*