PRACTICE RESOURCE

Google Glass and Health Care: Initial Legal and Ethical Questions

Nicolas P. Terry, Chad S. Priest, Paul P. Szotek

Nicolas P. Terry is Professor of Law at Indiana University Robert H. McKinney School of Law. He serves as Co-Director of the Hall Center of Law and Health. Contact him via email at npterry@iupui.edu or on Twitter @nicolasterry.

Chad S. Priest, JD, MSN, RN is Assistant Dean for Operations & Community Partnerships at Indiana University School of Nursing. Contact him via email at cspriest@iu.edu or on Twitter @ChadSPriest.

Paul P. Szotek, MD is Associate Professor of Surgery at Indiana University School of Medicine, Indiana University Health. Contact him via email at pszotek@gmail.com or on Twitter @PaulSzotekMD.

Terry, Priest, and Szotek: Google Glass

CONTENTS

Introduction .................................................................................................................. 95
Data and Image Display .............................................................................................. 96
The Limited Relevance of FDA Device Regulation .............................................. 100
Recording and Transmitting .................................................................................... 102
Data Storage ............................................................................................................... 103
Risk Management Strategies .................................................................................... 106
Risk Management Checklist ...................................................................................... 107
Conclusion .................................................................................................................. 108
Introduction

Google Glass (Glass) is a multi-functional, augmented reality device that can be used as a camera, video recorder, audio recorder, telephone, conferencing platform, or vehicle to run any number of applications currently under development. The immediate uses of Glass in the medical context are simultaneously modest and extraordinary: modest because relatively few medical apps have been released for Glass and extraordinary because surgeons and other health care professionals seem to perceive great value in Glass, a positive reaction they seldom display for traditional health information technologies.1

One of Glass’s unique features is its ability to overlay text or pictures over the wearer’s field of vision. Current medical uses include displaying patient-specific information (for example, a scan or electronic health record) during a diagnosis, treatment, or surgery. As currently configured, Glass’s other major feature is a camera that photographs or video records interventions and, because it is connected to the Internet, also serves as a teaching or mentoring conduit (for example, monitoring a resident’s surgery).

The use of Glass has the potential to yield several positives in the health care environment. For example, using images overlaid on the surgical site should result in greater accuracy and margins. In the future, a combination of radiologic images with wearable technology may provide a type of guidance system, allowing for more precise tumor resection and minimizing the occurrence of incomplete resections and multiple surgeries. Image overlay aside, Glass

and other wearables show potential for medical education, mentoring, first responders, and mass casualty scenarios.

Although physicians and some hospitals have exhibited considerable enthusiasm for the implementation of Google Glass in the health care environment, current uses for data display, recording and transmitting, or data storage pose several challenging ethical and legal questions. In addition, some of those uses may raise as yet unmeasured risks, such as distraction. More concretely, Glass users face informed consent requirements and legal and ethical limits on recording patients even for educational purposes. Most seriously, Glass is not yet compliant with the Health Insurance Portability and Accountability Act (HIPAA), although some apps developed for it are. Some uses of Glass will be subject to privacy and security constraints. This Practice Resource previews some of the legal and ethical issues involved in the use of Glass for data and image display, recording and transmitting, and data storage and provides risk management strategies for health care entities considering early adoption of this technology.

**Data and Image Display**

The most obvious medical use of Glass is to allow a care provider to display patient data or images in the field of vision during assessment, treatment, or procedure.\(^2\) For example, one emergency department has adopted Glass for accessing patient records by scanning Quick Response (QR) codes posted on the outside of

---

patient rooms. Other potential uses include rapid diagnostic tests and internet searches for codes and terminologies.

The technologies and components built into Glass are quite conventional and derived from those commonly found in mobile phones, but introducing any new technology into the health care environment carries some risk. New technologies may be unreliable or have poor battery life (a specific problem with early versions of Glass), suggesting the need for backup processes in the event of failure.

In general, clinical innovation involves little legal risk. As one court noted, “Therapeutic innovation has long been recognized as permissible to avoid serious consequences . . . [and a] physician is presumed to have the knowledge and skill necessary to use some innovation to fit the peculiar circumstances of each case.” Innovation may come, however, at the cost of enhanced risk disclosure.

Although early adopters apparently are using Glass to increase the user’s concentration on the task at hand, it is possible the technology may prove to be a distraction when used more broadly. Multi-tasking creates risk. Recall for example Halamka’s case study involving a resident who failed to complete a drug order in a computerized physician order entry application because he was

---

3 See e.g., Callum Borchers, Google Glass Embraced at Beth Israel Deaconess, BOSTON GLOBE, Apr. 9, 2014, available at www.bostonglobe.com/business/2014/04/08/beth-israel-use-google-glass-throughout-emergency-room/WhlXcVzkpn7MOCAhKuRJZL/story.html [hereinafter Google Glass Embraced at Beth Israel Deaconess].


distracted by a smartphone text. In addition, current research indicates that some health information technologies may be stressors, such as “alert fatigue” caused by decision support alerts.

Even when a wearable device is not being used to change a diagnostic method or surgical process, as may be the case with videotaping or photographing a case, wearing the device and the mere presence of a new image in the physician’s field of vision could be a distraction that leads to negative consequences. Indeed, several recent malpractice actions claim cell phones and mobile devices distracted medical personnel in the operating room.

While the potential positive benefits of heads-up displays in the surgical environment may outweigh the risks of distraction, the informed consent process arguably should include an appraisal of potential risks associated with use of the new device, including a candid discussion of how wearing the device will alter surgical and other workflows.

While the law varies slightly from state to state, the doctrine of informed consent generally “imposes on a physician a duty to disclose material information that ‘a physician knows, or ought to know would be significant to a reasonable person in the patient’s position in deciding whether or not to submit to a particular medical treatment or procedure.’” Importantly (especially considering the broad array of risks faced by patients in modern health

care environments), not every risk is required to be disclosed to patients. Only material risks that are likely to influence a patient’s decision to undergo a specific intervention must be disclosed.\footnote{The Rhode Island Supreme Court identified two factors to determine materiality of risk: (1) “severity of the risk” and (2) “likelihood of its occurrence.” Wilkinson v. Vesey, 295 A.2d 676, 689 (R.I. 1972).}

There is a good argument that using Glass during diagnosis or surgery may not pose a material risk that requires any additional informed consent. First, in contrast to the major innovations that occur daily in the health care industry, Glass may seem a relatively modest addition. Second, Glass could replace a potentially unsafe technique, such as walking away from the patient to view an image on a computer screen or a light table, with a less risky one. The use of any new technology in the operating room (OR) as a surgical adjunct (e.g., the use of a new surgical technique) may, however, require additional risk disclosure. Another argument could be made: that using a wearable device for any purpose in the OR has the potential to transform a procedure, process, or workflow so significantly that it creates the potential for outcomes or risks that should be communicated to a patient to secure informed consent. In practical terms, this issue will reduce to the persuasiveness of expert testimony on the materiality of the risk of using Glass,\footnote{Jaskoviak v. Gruver, 638 N.W.2d 1, 9 (N.D. 2002).} whether the jurisdiction follows the patient expectations test or the customary standard for reasonable disclosure.\footnote{See generally Largey v. Rothman, 540 A.2d 504 (N.J. 1988).}

Expert medical testimony is generally necessary to identify the risks of treatment, their gravity, likelihood of occurrence, and reasonable alternatives . . . . The necessity for expert testimony is particularly so when such information is outside the common knowledge of laymen. \[\text{[^]}\] Expert testimony may be necessary under the lay standard, at least to establish the existence of a risk, its likelihood of occurrence, and the type of harm in question; after that, however, expert evidence may not be required. \[\text{[^]}\] However, experts may be required to show both that material information existed and that the defendant should reasonably have known about it.
Courts have held consistently that the physician, not the health care institution, owes the patient the duty of informed consent\textsuperscript{16} despite cogent arguments that this duty should have migrated to the institution.\textsuperscript{17} An area of weakness, however, may be where the institution has better information about risks than the physician, which could be the case if the institution adopted and implemented an experimental program, such as equipping a department’s professional staff with Glass. For example, an appellate court in Utah recently held that a hospital had an independent duty to obtain a patient’s consent because it was in the best position to prevent injury by an experimental ventilator. The court stated, “It does not create an undue imposition to require that when a hospital . . . allows the use of equipment that is not part of the hospital’s usual inventory, the hospital has an independent duty to obtain informed consent.”\textsuperscript{18}

The Limited Relevance of FDA Device Regulation

Google has positioned Glass as a consumer device, rather than a professional device.\textsuperscript{19} The Food and Drug Administration (FDA) regulates medical devices, which may be subject to pre-marketing and post-marketing (surveillance) regulatory controls. In its current form, Glass is unlikely to attract such regulation. In a 2013

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{19} Vidya Viswanathan, Is There a Place for Google Glass in Hospitals?, Atlantic, July 21 2014, available at www.theatlantic.com/health/archive/2014/07/is-there-a-place-for-google-glass-in-hospitals/374153/ (quoting Google spokesperson that Google is “very focused on making Glass a consumer device”).
\end{itemize}
\end{footnotesize}
Guidance to mobile app and platform manufacturers, the FDA said the agency did not consider “Manufacturers or distributors of mobile platforms who solely distribute or market their platform and do not intend (by marketing claims–e.g., labeling claims or advertising material) the platform to be used for medical device functions” to be mobile medical app manufacturers.\(^{20}\)

Some Glass apps may be subject to device regulation, however, if the app converts the platform (Glass) into a medical device,\(^ {21}\) such as when an app provides the Glass user with remote display of alarms from bedside monitors or when the app is integrated with robotic surgery.\(^ {22}\)

Applying for FDA device approval is the manufacturer’s obligation, not the physician’s or hospital’s. Nevertheless, the experimental or novel use of devices has been viewed as relevant in some informed consent cases. The case law surrounding the physician’s duty to obtain informed consent about unapproved or off-label uses is mixed, but many courts allow the jury to consider attendant liability risks.\(^ {23}\) For example, one state’s informed


\(^{21}\) MOBILE MEDICAL APPLICATIONS.

\(^{22}\) Id. at 14.

\(^{23}\) See e.g., DeNeui v. Wellman, No. 07-4172-KES (D. S.D. 2009) (collecting authorities and holding case presented a genuine issue of material fact as to whether a reasonable person would have attached significance to a doctor’s off-label use of a bone protein prior to consenting to surgery). See also Corrigan v. Methodist Hosp., 869 F.Supp. 1208 (E.D. Pa. 1994) (material fact issues existed as to patient’s claims for use of unapproved screws in surgery on theory that hospital should have had policies regarding informed consent). Cf. Shannon (trial court did not abuse its discretion in excluding evidence related to FDA approval status of drug).
consent statute requires a physician to obtain informed consent if “[a]dministering an experimental medication, using an experimental device or using an approved medication or device in an experimental manner.”

Recording and Transmitting

Glass has the capacity to bring “outside observers” into the examination room or the operating suite, either in real-time or through recorded photos and videos. When used for teaching, Glass may further the democratization of surgical education. While it is widely accepted as both ethical and appropriate to film and/or broadcast medical procedures to advance legitimate educational objectives, important ethical and legal constraints must be followed.

In the health care domain, the contributions of the common law of privacy have been modest. Notwithstanding, the courts have been clear in their rulings about unauthorized photography of patients. Ethical constraints are equally well-defined. For example, the American Medical Association’s (AMA’s) ethics opinions

require “the patient’s explicit agreement” for the presence of outside observers who themselves are required to agree in advance to maintain confidentiality. Patient consent should be given only after the physician provides “an explanation of the educational purpose of film, potential benefits and harms (such as breaches of privacy and confidentiality), as well as a clear statement that participation in filming is voluntary and that the decision will not affect the medical care the patient receives.” If the audience is not limited to health care professionals and their students, an additional explicit consent will be required.

In most cases, a simple photographic consent/release form should be sufficient to educate the patient about the procedure that will be used to obtain the photos, their intended use, and what rights, if any, the patient may have to any images or videos taken.

Data Storage

In some states, a picture or video of a patient taken with Glass will be considered part of the patient’s record. The implication is that the health care provider must curate such images as stipulated by the applicable record retention statute. In most cases, a

30 Id.
31 E.g., 49 Pa. Code § 16.95(c) “Clinical information pertaining to the patient which has been accumulated by the physician, either by himself or through his agents, shall be incorporated in the patient’s medical record.”
A video recording of a patient encounter or surgery will be admissible in a malpractice case.\textsuperscript{33} Further, destruction of such potential evidence may result in adverse repercussions based on spoliation of evidence.\textsuperscript{34}

The greatest number of risks regarding Glass-generated data storage relate to federal regulations on health privacy and security. When a physician uses Glass to record an image or video of a patient, the data being acquired and stored implicate HIPAA’s regulation of data uses and disclosures. A HIPAA-covered provider is subject to regulatory duties as to non-disclosure of collected data (including images and videos), security standards, and breach notification.

If the data acquired are stored only on hospital secure servers (or on a HIPAA-compliant “cloud”) and accessed for “treatment, payment, and health care operations” (TPO), a HIPAA problem is unlikely to arise.\textsuperscript{35} Transmitting the image or other patient data to Google, however, would fall outside of TPO and create serious HIPAA privacy and security issues. Typically, where a third party service provider is involved, a covered entity complies with HIPAA by entering into a Business Associate Agreement (BAA) with the third-party that will have access to such protected health information.\textsuperscript{36} Currently, however, Google does not offer a publicly available BAA for Glass, which still uses unencrypted data transmission and non-compliant storage. Complicating matters, some apps...

\textsuperscript{33} Aikman v. Kanda, 975 A.2d 152 (D.C. Ct. App. 2009)
\textsuperscript{35} 45 C.F.R. § 164.501, \textit{id.} § 164.506.
\textsuperscript{36} \textit{id.} § 164.504.
developed for Glass modify the device by, for example, encrypting video transmission to render some features HIPAA-compliant.\textsuperscript{37}

Under HIPAA, an individual patient may authorize otherwise prohibited data use, but the process is highly regulated and cumbersome and does not scale well to multiple procedures or large numbers of patients.\textsuperscript{38} If use or disclosure is for the purposes of research, individual authorizations could be waived. For example, an Institutional Review Board (IRB) may waive the requirement when approving a research protocol. The criteria for such a waiver are particularly stringent.\textsuperscript{39} One report suggests that an IRB did grant such a waiver.\textsuperscript{40} Most IRBs, however, probably would focus on the regulatory requirements of minimal risk and restricted disclosure regarding subject identifiers,\textsuperscript{41} which would be difficult to satisfy given the data transmission and storage employed by Glass.

The security rule implications of Glass for hospitals will be particularly serious during the device’s early adoption phase. Early adopter-physicians may use their own devices, tether them to smartphones, and entirely bypass the hospital’s network. As such, Glass adds to a hospital’s existing “Bring Your Own Devices” (BYOD) challenge. The HIPAA security rule includes requirements for administrative safeguards such as risk management,\textsuperscript{42} physical safeguards such as workstation security or policies regarding portability of data-containing devices,\textsuperscript{43} and technical safeguards such

\begin{footnotesize}
\begin{itemize}
    \item[38] 45 C.F.R. § 164.508.
    \item[39] Id. § 164.512 (i).
    \item[41] 45 C.F.R. § 164.512 (i)(2).
    \item[42] Id. § 164.308 (a)(1)(ii)(B).
    \item[43] Id. §§ 164.310(c)–(d).
\end{itemize}
\end{footnotesize}
as access control and audits. Hospitals find these requirements difficult—if not impossible—to apply to BYOD technologies.

Gradually, Glass will be formally adopted by institutions and integrated into security and privacy protocols. In the meantime, hospitals have reason to be wary of unapproved devices with network access.

**Risk Management Strategies**

Technological innovation in the health care context presents a polarity that requires careful management. On the one hand, technological innovations, by their definition, represent something new, create novel risks, and threaten outcomes. On the other hand, failure to adopt new technologies in health care carries risks. Generally, the health care industry operates on the presumption that the status quo is safer, or at least less risky, than a new technology. While that may be true, a process or procedure consistently performed is not necessarily consistently performed well. Nor will adherence to current practices stop the relentless march of innovative, even disruptive, technologies entering the health care space.

A clearer picture of the risk-benefit proposition will materialize as medical uses of Glass multiply and more data emerges. In the interim, providers and hospitals should consider several risk management and related strategies. At the very least, health care institutions will need to review how security and privacy policies apply to physician-owned BYOD devices, including Glass. Physicians considering using such devices should engage in a dialogue with the institution’s privacy officer, risk management, and compliance counsel. Detailed suggestions are listed in the Risk Management Checklist below.

---

44 Id. § 164.312.
45 See e.g., Google Glass Embraced at Beth Israel Deaconess.
Risk Management Checklist

✔ Update security and privacy policies for BYOD devices used in patient settings to factor in use of Glass.

✔ Review social media policies because of the integration of Glass with Google+.

✔ Engage in a dialogue with the institution’s privacy officer, risk management, and compliance counsel about the use(s) of Glass.

  ✔ Specifically discuss the language to be used in any HIPAA individual authorizations or informed consent documents, with particular emphasis on making the extent of data sharing understandable for the patient.

✔ Establish a working group to report on detailed issues such as:

  ✔ HIPAA-compliant communications;

  ✔ whether the camera should be disabled;

  ✔ approval processes for apps;

  ✔ whether use should be restricted to Glass devices modified to be HIPAA-compliant;

  ✔ Google policies for the availability of a Glass BAA; and

  ✔ the use of delayed broadcast to prevent the inadvertent transmission of unconsented-to processes, complications, or negative outcomes.
Conclusion

Mobile health wearables and their associated apps will redefine patients’ involvement in wellness and condition management.46 The digital health revolution likely will favor more products like Glass and a rapidly iterating world of apps. Full electronic health record integration is becoming available, 47 as is the ability to use Glass to document encounters,48 while other developers are looking to bring real-time patient data and alerts into the surgeon’s field of vision.49 Better care coordination is possible as Glass is adopted not only by surgeons but also by other members of the surgical team or paramedics in the field.50 In the future, Glass also may be joined by virtual reality products that until now have been viewed as more valuable for gaming than surgery.51

As providers and hospitals manage the integration of such technologies into workflows and regulatory or risk management models, it is crucial to appreciate that Glass and other first generation wearables are “very early, crude prototypes for much more interesting and useful devices that will be widely used by 2025.”52 The legal and ethical structures within which they operate will also similarly continue to evolve.

46 See generally Nicolas Terry, mHealth: Assessing the Barriers, (forthcoming CHEST, 2015).