Breathing New Life into HIPAA's UHID - Is the FDA's Green Light to the Verichip the Prince Charming Sleeping Beauty Has Been Waiting For?

Crystal Spivey

Follow this and additional works at: https://via.library.depaul.edu/jhcl

Recommended Citation
Crystal Spivey, Breathing New Life into HIPAA's UHID - Is the FDA's Green Light to the Verichip the Prince Charming Sleeping Beauty Has Been Waiting For?, 9 DePaul J. Health Care L. 1317 (2006)
Available at: https://via.library.depaul.edu/jhcl/vol9/iss3/7

This Article is brought to you for free and open access by the College of Law at Via Sapientiae. It has been accepted for inclusion in DePaul Journal of Health Care Law by an authorized editor of Via Sapientiae. For more information, please contact wsulliv6@depaul.edu, c.mcclure@depaul.edu.
BREATHING NEW LIFE INTO HIPAA’S UHID – IS THE FDA’S GREEN LIGHT TO THE VERICHIP™ THE PRINCE CHARMING SLEEPING BEAUTY HAS BEEN WAITING FOR?

Crystal Spivey*

SYNOPSIS: Given the tendency for our society to continually accept and move forward with any technological device aimed at ease and efficiency, the FDA’s approval of the Verichip™, President Bush’s initiative to have medical records transferred to electronic media within the next ten years, and HIPAA’s requirement for a UHID, it seems inevitable that the Verichip™, a new technology, is on the brink of huge success and will eventually become mainstream in our healthcare facilities. As a result, most people will be convinced, in the name of efficiency, to consent to having the chip implanted in their bodies. The acceptance of the technology by medical professionals and society will also work to create a dependency, and therefore, disadvantage those individuals who either will not consent to the chip or do not have the funds available to do so. This article primarily examines President Bush’s plan, HIPAA, and the Verichip™. However, because of danger inherent in the proliferation of the device, this article urges caution in the distribution of the Verichip™ and calls upon legislators to ensure that the Verichip™ does not deprive individuals of their ability to acquire medical services or infringe upon privacy rights.

THE STAGE IS SET. On October 13, 2004, the Federal Drug Administration (FDA) approved the Verichip™, an implantable computer chip, for marketing to hospitals and other medical health facilities for use in electronic medical record-keeping.1 From the left stage, enter gasping privacy experts and advocates; from the right, enter hailing supporters, such as Verichip’s™ producer, Applied Digital and CEO Michael Silverman,2 as well as President Bush and his plan to have all medical records changed over to electronic media within the

---

* Ms. Spivey would like to thank her family for teaching her the value and integrity in hard work; her friends for sharing their contagious optimism and confidence; and her fiancé for his unwavering support and encouragement.

2 Applied Digital Solutions, Inc., 1690 S. Congress Av. #200, Delray Beach, FL 33445-6386 (Scott R. Silverman, CEO).
next ten years.\textsuperscript{3} As a backdrop to the set, The Health Insurance Portability and Accountability Act\textsuperscript{`} of 1996 (HIPAA)\textsuperscript{4} looms in the distance. And let the story begin …

In the wake of the FDA’s recent approval of the Verichip\textsuperscript{TM} implant, and in light of President Bush’s push for electronic medical records in his second term in office, it is imperative to examine the implications of these possible coalescing events and predict the consequences of the success of both. In the past, electronic storage of medical records and implantable chip technology were thought to be inventions of science fiction, pondered largely in books, such as Aldous Huxley’s \textit{Brave New World}\textsuperscript{5} and George Orwell’s \textit{1984},\textsuperscript{6} and movies, such as \textit{The Manchurian Candidate}\textsuperscript{7} and \textit{The Bourne Identity},\textsuperscript{8} but today, as science continues to advance, we live in the shadow of the impending proliferation of such devices. In fact, as some argue, the march toward mainstream use of this device has put not just Americans, but all, on a veritable fast track toward the fictional extremes revealed in popular science fiction.

\textsuperscript{3} The president announced on April 26, 2004 his goal of assuring that most Americans have electronic health records within the next ten years. See GOP.com, Transforming Health Care: The President’s Health Information Technology Plan, http://www.gop.com/News/Read.aspx?ID=4140 (last visited Jan. 9, 2006) (highlighting the president’s plan, challenging the current system, and proposing electronic medical records as the solution) [hereinafter Transforming Health Care].

\textsuperscript{4} Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C.) [hereinafter HIPAA]. HIPAA was enacted on August 21, 1996 to “improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.” Id.

\textsuperscript{5} ALDOUS HUXLEY, \textit{BRAVE NEW WORLD} (1932).

\textsuperscript{6} GEORGE ORWELL, \textit{1984} (1949).

\textsuperscript{7} Originally a novel by Richard Condon in 1956, \textit{The Manchurian Candidate} has twice been made into a movie. In 1962, it was directed by John Frankenheimer. THE MANCHURIAN CANDIDATE (United Artists 1962). More recently, Jonathan Demme directed another movie in 2004. THE MANCHURIAN CANDIDATE (Paramount Pictures 1962). In the 2004 movie, the main character, a former American military soldier, was brainwashed and implanted with a computer chip. Id.

\textsuperscript{8} The \textit{Bourne Identity} was originally a book written by Robert Ludlum. ROBERT LUDLUM, \textit{THE BOURNE IDENTITY} (Bantam Books 1984). In 2002, a movie, loosely based on the book, was directed by Tom Gilroy. \textit{THE BOURNE IDENTITY} (Universal Pictures 2002). \textit{The Bourne Identity} was followed by a sequel with \textit{The Bourne Supremacy} in 2004. \textit{THE BOURNE SUPREMACY} (Universal Pictures 2002).
This article is divided into three main sections. The first section will examine the politics behind electronic medical records. Both the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requirement for a Unique Health Identifier ("UHID") for all Americans and President George W. Bush's plan to have most records turned over to electronic media within the next ten years will be examined. The second section will introduce and explain the Verichip™ technology, its capabilities, and its uses. Relevant fears and concerns from the Verichip's™ opponents will also be discussed. In addition, that section will speculate as to whether the Verichip™ could be the technology in which HIPAA's UHID and Bush's plan will be implemented. A final section will discuss relevant issues concerning mainstream implantation of the Verichip™. Specifically, will the Verichip™ remain on a "consent-only" basis as its proponents suggest? Will "non-chipped" patients be disadvantaged in acquiring medical services if it becomes mainstream? A call upon legislators to preemptively handle such issues concludes this article.

PART I: ELECTRONIC MEDICAL RECORDS AND POLITICS

The Past and The Current Push

Increasing access to healthcare in America and simplifying procedures have been points of contention for the last decade. In 1993, President Clinton proposed issuing national health identification cards to provide every "American health security, health care that can never be taken away, health care that is always there." Clinton's cards were to be linked to a health identifier for each individual that could be used in a national healthcare database. Mocked by the public and media,
however, Clinton abandoned the plan without ever having made progress on the health identifier. After Clinton's unsuccessful attempt, the idea of a national database of electronic medical records remained lifeless, until HIPAA was enacted in 1996. Again, the national health identifier came to the forefront of the debate. HIPAA's main purpose was to eliminate health care fraud and facilitate administrative convenience, primarily by making all health information electronically available, although it also addresses other health care issues. The Act was passed to "improve portability and continuity of health insurance coverage in the group and individual markets." Although HIPAA passed with relative ease, certain portions garnered wide controversy post-enactment, including a provision which mandated assignment of a universal individual health identifier (UHID) to each American for use in a national healthcare record database.

---


13 HIPAA, supra note 4.


16 "The sample UHID consists of a sixteen (16) digit sequential identifier, a (period) that serves as a delimiter, a six (6) digit check-digit and a six (6) digit encryption scheme. Altogether, it consists of 28 numeric digits and a period." HIPAA.net.com, Sample Universal Health Identifier, http://www.hipaanet.com/upin7-2.htm (last visited Jan. 9, 2006).

17 See Netter, supra note 9, at 172-73.

HIPAA required the Secretary of HHS to recommend privacy standards for health information to Congress twelve months after its enactment. If Congress did not enact the privacy legislation within three years of enactment, the Secretary was to promulgate privacy regulations for individually identifiable electronic health information. Congress missed the three-year deadline, and on November 3, 1999, the Secretary promulgated the regulations, known as the Privacy Rule to compel most health plans and health care providers, by April 2003, to meet standards for confidentiality, consent, and access to private individual medical information. The Rule's adoption opens the door for the UHID.

Id. See Myra Moran et al., Living with the HIPAA Privacy Rule, 32 J.L. MED. & ETHICS 73, 73 (2004) (providing more information on the Privacy
HIPAA directs the Secretary of Health and Human Services (HHS) to "adopt standards providing for a standard unique health identifier for each individual ... for use in the health care system."\(^{18}\) Title II of HIPAA, subtitle F, is titled, "Administrative Simplification," and states as its purpose the improvement of 'the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishments of standards and requirements for the electronic transmission of certain health information.'\(^{19}\)

An UHID achieves the goal of "administrative simplification" by eliminating patient identity confusion, unnecessary delay for the patient in going from one provider to another, and difficulties in bill collection and in mergers between health care providers.\(^{20}\) Thus, according to at least one source, the UHID, offering the benefit of a "lifetime health record, logically containing data from all sources, when authorized by the patient, is key to delivering high quality, cost-effective care".\(^{21}\) By using a UHID, a patient would not have to worry whether his records would be transferred from one doctor to another.\(^{22}\) Instead, the patient’s entire record would always be in one central database, accessible only through the use of his unique number.\(^{23}\)

As posted on the HIPAA website, the current proposal for the UHID is still being considered and is currently on hold pending


\(^{19}\) See Buckman, supra note 14, at 147-48.

\(^{20}\) Netter, supra note 9, at 168-69.


\(^{22}\) Id.

\(^{23}\) Id.
Although HIPAA and the privacy standards set forth by the Health and Human Services have been legally challenged for

---

24 See HIPAA.net.com, Tentative Schedule for Publication of HIPAA Administrative Simplification Regulations, http://www.hipaanet.com/asmiles.htm (last visited Jan. 9, 2006) (commenting that "reaction to discussion of individual identifier in absence of privacy protection prompted administration to put this standard development on hold"). Also, implementation of the individual health identifier is listed as "on hold pending privacy legislation and/or regulations." Id.


In light of this envisioned computerization and increased electronic transmission of health information, and recognizing the concomitant need to guarantee certain protections to patients' privacy, Congress included section 264 within Subtitle F, Title II of HIPAA. Section 264(a) instructs HHS to provide Congress with 'recommendations on standards with respect to the privacy of individually identifiable health information' within twelve months of HIPAA's enactment date. Subsection (b) of Section 264 directs HHS to make recommendations concerning at least the following subjects: (1) The rights that an individual who is a subject of individually identifiable health information should have. (2) The procedures that should be established for the exercise of such rights. (3) The uses and disclosures of such information that should be authorized or required. 101 Stat. 2033. Section 264(c) states that if Congress should fail to enact legislation governing 'standards with respect to the privacy of individually identifiable health information' within 36 months of the enactment of HIPAA, HHS shall promulgate 'final regulations' containing such privacy standards not later than 42 months after the enactment of HIPAA. Such HHS regulations shall 'not supercede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation.' 110 Stat. 2033-34. By August 21, 1999, Congress had not enacted privacy standards pursuant to HIPAA. Accordingly, on November 3, 1999, HHS issued a notice of proposed rulemaking. After receiving approximately 52,000 public comments, and following the publication of several proposed rules and amendments, on February 13, 2001, HHS promulgated final regulations (the 'Privacy Rule'). Although the effective date of the Privacy Rule was April 14, 2001, covered entities were given two years, or until April 14, 2003, to come into compliance with the Privacy Rule. Smaller health plans and entities were given three years, or until April 14, 2004, to comply. Following publication of the Privacy Rule, and in response to further public comments, HHS published on its website additional guidance concerning the Rule's practical impact.
threats to privacy, a district court has upheld its validity against those constitutional challenges, and the Fifth Circuit has affirmed without opinion.\textsuperscript{26} Interestingly, Dr. Richard Seelig, a retired Montville surgeon who helped develop the Verichip™ and Vice President of Medical Applications for Verichip Corporation, points out that Verichip™ is “HIPAA-friendly, because it doesn’t convey a name or any information identifier, only a number.”\textsuperscript{27}

Although we have yet to see the UHID enforced nationally, President Bush has followed suit in calling for a national healthcare database and electronic medical records for most American citizens within the next ten years.\textsuperscript{28} According to the President, by changing

\begin{flushright}
\end{flushright}

The court upheld the validity of HIPAA and the Privacy Rule, HHS’s rule regarding the regulation of individually identifiable health information, against constitutional challenges. See Buckman, \textit{supra} note 14, at 133. The plaintiffs in the case, a not-for-profit organization and patients, brought First, Fourth, and Tenth Amendment claims for review. However, the court held that the plaintiffs’ lacked standing to pursue any of their claims, and the Fourth Amendment claim was not ripe for review. The court also concluded that HIPAA was constitutional, as it was within Congress’ commerce powers to enact it. Additionally, the court held that the Privacy Rule was within the scope of HIPAA, and the HHS were justified in promulgating it when Congress failed to enact its own standards. Association of American Physicians & Surgeons, 224 F.Supp.2d at 1127.

\begin{flushright}
Bob Groves, Lifesavers in their Arms, http://www.northjersey.com/print.php?qstr=ZmdiZWw3Zjd2cWVIRUV5eTY2MzMOOTkmeXJpcnk3ZjcxN2Y3dnFlZUVVFeXk1 (last visited Jan. 9, 2006). Seelig decided to begin working on the chip after watching rescue workers write their badge numbers on their arms before going into the rubble of 9/11 to look for survivors. \textit{Id.} Other physicians agree with Seelig’s call for the chip, including Dr. Michael Gerardi of Morristown Memorial Hospital and past state chapter president of the American College of Emergency Physicians. “We’re heavily invested in electronic medical records...We’re all concerned with HIPAA, and we do everything we can to maintain security and protect information.” \textit{Id.}
\end{flushright}

The President believes that better health information technology is essential to his vision of a health care system that puts the needs and the values of the patient first and gives patients information they need to make clinical and economic decisions - in consultation with dedicated health care professionals. The President’s Health Information Technology Plan will address longstanding problems of preventable errors, uneven quality, and rising costs in the Nation’s health care system.” In addition, the effort is also being pushed by Democrats. Sen. Hillary Clinton (D, N.Y.) has introduced a five-point plan to
the way in which medical information is stored, primarily by moving to
electronic storage of health records and the secure exchange of medical
information, health care in America will be completely transformed for
the better.\textsuperscript{29} The Bush Administration has been committed to creating
a "Health Information Technology Infrastructure" – that is, a national
standard for the electronic storage of health information to make it
easier for facilities to communicate to one another.\textsuperscript{30}

To achieve this goal, Bush has called for adoption of
interoperable electronic health records in an Executive Order, as well as
issued statements in his public addresses that support electronic
records.\textsuperscript{31} President Bush believes that electronic records\textsuperscript{32} will greatly
improve the quality of health care, prevent incorrect medical records,
reduce health care costs, improve efficiency, reduce paperwork, and
increase access to more affordable healthcare – "[b]y computerizing
health records, we can avoid dangerous medical mistakes,\textsuperscript{33} reduce
costs,\textsuperscript{34} and improve care."\textsuperscript{35}

dsn.org/amednews/2004/02/09/gysa0209.htm.
\textsuperscript{29} Transforming Health Care, \textit{supra} note 3.
\textsuperscript{30} Gonzalez, McHugh Introduce National Health IT Act: Legislation Encourages
Doctors to Transition from Paper to Electronic Health Records, February 11, 2005,
[hereinafter Gonzalez Health IT Act].
\textsuperscript{31} In his State of the Union Address, President Bush encouraged Congress to "[g]ive
physicians incentives to acquire health information technology." \textit{Id.}
\textsuperscript{32} Electronic medical records are certainly not just a figment of future imagination, as
software designed to manage patient's medial records electronically is already on the
market. One company just launched on Dec. 1, 2004. \textit{See} Physician's Microsystems,
MedicWare, http://www.paperlessmd.com/products/medicware/medicware.html (last
(last visited Jan. 10, 2006); AltaPoint Medical, http://www.altapoint.com (last visited
Jan. 10, 2006); SoapWare, http://www.docs.com (last visited Jan. 10, 2006);
\textsuperscript{33} \textit{See generally} Transforming Healthcare, \textit{supra} note 3. "The Institute of Medicine
estimates that between 44,000 and 98,000 Americans die each year from medical
The President has drawn attention to his plan for electronic medical records in public addresses. On April 24, 2004, the President addressed the Department of Veterans Affairs Medical Center in Baltimore\(^{36}\) and praised the abilities of electronic health records in eliminating current problems.\(^{37}\) Present at the address included

errors. Many more die or have permanent disability because of inappropriate treatments, mistreatments, or missed treatments in ambulatory settings.” \(\text{Id.}\)

\(^{34}\) See generally \textit{id.} “Health care spending and health insurance premiums continue to rise at rates much higher than the rate of inflation. Despite spending over $1.6 trillion on health care as a Nation, there are still serious concerns about preventable errors, uneven health care quality, and poor communication among doctors, hospitals, and many other health care providers involved in the care of any one person.” … “Studies have found that as much as $300 billion is spent each year on health care that does not improve patient outcomes - treatment that is unnecessary, inappropriate, inefficient, or ineffective.” \textit{Id.}


\(^{36}\) \textit{Health Care IT Speech, supra note 35.}

\(^{37}\) \textit{Id.} One of the problems the President discussed was the inefficiency of handwritten prescriptions and records; panelists discussed the difficulties inherent in a handwritten system, including deciphering handwriting of physicians. \textit{Id.}

Pharmacists have to figure out the handwriting of a doctor. Vital medical information is scattered in many places. X-rays get misplaced. Problems with drug interaction are not systematically checked,” Bush said in a speech in Minneapolis. “We need a system where [all patients] have their own personal electronic medical record that they control and can give to a doctor when they need to.” He also said the Department of Health & Human Services and other federal agencies would begin to
Secretary of Health and Human Services Tommy Thompson and other panelists\textsuperscript{38} invited to speak on the topic of electronic medical records. Thompson highlighted benefits of the national system such as opportunities to reduce expenditures, develop a common medical vocabulary, create uniform medical records for each American, and assign barcodes to drugs and patients to prevent mistakes.\textsuperscript{39}

In another public address on electronic medical records on Jan. 27, 2005, the President stated that changing to electronic records will "help change medicine and save money and save lives."\textsuperscript{40} The President pointed out that health analysts had concluded that electronic medical records could reduce current medical errors by twenty percent.\textsuperscript{41} He also pointed out that he would be asking Congress for $125 million for Health IT for the 2006 budget at that meeting.\textsuperscript{42}

In addition to his public appearances, the President has outlined a plan to ensure that most Americans will have electronic health care records within the next ten years.\textsuperscript{43} Participation in the plan, according to the President, will be voluntary.\textsuperscript{44} Currently, some of the groundwork is already being completed. The Department of Health and Human Services has already made possible the ability to transmit x-rays and lab results over the internet to be read by doctors not physically present in the hospital, or to forward to other experts for a second opinion.\textsuperscript{45} On the agenda for this year is Bush's 2005 budget, which includes a hefty $100 M for projects that will "help us determine the effectiveness of health information technology and establish best practices for more widespread adoption in the health care industry."

come up with plans on how to offer private contractors incentives to develop innovative new technologies.

\textsuperscript{38} Bush Health Care IT Speech, supra note 35. In addition to President Bush and Tommy Thompson, Secretary of Veterans Medical Center, Tony Principi, Director of Quality and Safety Initiatives at John Hopkins, Dr. Marlene Miller, and Administrator of Veterans Medical Center Dennis Smith were also invited panelists. Id.

\textsuperscript{39} Tommy Thompson, Secretary of Health and Human Services, Address to Department of Veterans Affairs Medical Center (April 27, 2004).

\textsuperscript{40} Michael Fletcher, President Promotes Switching To Electronic Medical Records, WASH. POST, Jan. 28, 2005, at A07.

\textsuperscript{41} Id.

\textsuperscript{42} That $126 million will be in addition to the $100 million already granted for 2005. Id.

\textsuperscript{43} Transforming Healthcare, supra note 3.

\textsuperscript{44} Id.

\textsuperscript{45} Id.
The amount is up from the 2004 budget of $50 M. The President also created a new sub-cabinet level position called National Health Information Technology Coordinator, who is to report directly to the Health and Human Services Secretary on health information standards and identify "the various steps needed to support and encourage health information technology in the public and private health care systems." Already in the works is a "medical Internet," which will allow for the transfer of medical records across the country confidentially. Despite concerns of some liberty and privacy groups, proponents of the project insist that the records will remain confidential.

To aid in attaining President Bush's goal of having an electronic national network of information technology in place within the next 10 years, Congressman Charlie Gonzalez (D-TX) and John McHugh (R-NY) recently introduced a bill called The National Health Information Incentive Act of 2005 on February 10, 2005. The bill has been described as "a bipartisan effort to encourage the nation's healthcare providers to adopt interoperable health information technologies that both improve quality and efficiency and lower costs for the healthcare consumer." Also known as the "Health IT Act," the bill provides a number of incentives for health care providers to make the necessary changes to implement health information technology in their own practices. The bill authorizes the Department of Health and Human Services to give grants, tax credits, and revolving loans to those participating in the changeover from paper records to electronic records in an effort to aid those practicing physicians that otherwise could not make the changeover. It also approves "add-on bonus payments" to

46 Id.
48 Id.
49 Fletcher, supra note 40, at A07.
50 Groves, supra note 27.
52 Gonzalez National Health IT Act, supra note 30.
53 Id.
54 Id.
55 Transforming Health Care, supra note 3. The average cost for an electronic health records is estimated at $30,000 per physician. American College of Physicians, ACP Supports New Bill to Encourage the Adoption of Health Information Technology,
physicians for using electronic medical records that meet certain standards.\textsuperscript{56} Finally, the Act orders the Office of the National Coordinator for Health Information Technology to create a pilot program to create the national standards.\textsuperscript{57}

To bolster support for the Health IT Act, Gonzalez cites numerous benefits of health information technology, such as improving the quality of care and benefiting medically underserved populations.\textsuperscript{58} Support has already been gained from organizations such as the American College of Physicians, the largest medical specialty organization in the United States.\textsuperscript{59}

Could the FDA’s approval of the Verichip\textsuperscript{TM} and the Health IT Act be the wings President Bush’s plan needs to get off the ground?\textsuperscript{60} Although there has been no official indication, it seems that the Verichip\textsuperscript{TM} may finally be just what the doctor ordered.

\textbf{PART II: THE VERICHIP\textsuperscript{TM}}

\textbf{The Technology for UHID?}

The FDA’s power to approve devices for medical use is codified in scattered sections of 21 U.S.C. under the Act known as the Federal Food Drug and Cosmetic Act, 21 U.S.C. § 301 and in the Medical Device Amendments Act of 1976, PL 94-295.\textsuperscript{61} This is the power

\textsuperscript{56} http://www.acponline.org/college/pressroom/adopt_healthinfo.htm (last visited Feb. 2, 2006) [hereinafter ACP].

\textsuperscript{57} ACP, supra note 55.

\textsuperscript{58} Gonzalez Legislation Encourages Doctors to Transition from Paper to Electronic Health Records, http://gonzalez.house.gov/issues2.cfm?id=10405 (last visited Feb. 2, 2006). Other benefits listed include: more current medical information, reducing errors due to poor handwriting, providing timely and appropriate treatment information, savings of close to $140 billion, providing medical treatment to inner-city and remote rural areas, and improving privacy and accuracy of records in general.

\textsuperscript{59} ACP, supra note 55.

\textsuperscript{60} PAT NECERATO, THE SHOCKING TRUTH ABOUT THE VERICHIP ... AND HOW IT MAY CHANGE LIFE AS YOU KNOW IT 18 (2004), available at http://www.theverichip.com/Verichipebook2.pdf. “William A. Pierce, an HHS spokesman, could not say whether Verichip and its accompanying secure database of medical records fit within that initiative...‘Exactly what those technologies are is still to be sorted out,’ Pierce said. ‘It all has to respect and comport with the privacy rules.’” Id.

\textsuperscript{61} See Pub. L. No. 94-295, 90 Stat. 539 (1976) (codified in scattered sections of 21 U.S.C.). In addition, the definition of the word “device,” which is the definition under
under which the Verichip™, an implantable medical device, was approved by the FDA on October 13, 2004.62

The Verichip™, which is produced by Applied Digital, Inc.63 is the world's first implantable "radio frequency identification device" (RFID)64 for humans and can store up to about six lines of text.65 A

which Verichip™ was accepted, can be found at 21 U.S.C.A. §321(h) (2004). “The term ‘device’ ... means an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is -- ... (2) intended for the use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevent of disease, in man or other animals ....” 21 U.S.C.A. §321 (h) (2004). See Jay M. Zitter, What is “Device” Within the Meaning of §201(h) of Federal Food, Drug, and Cosmetic Act, 129 A.L.R. Fed. 343 (2004).

64 NECERATO, supra note 60, at 13. RFIDs are the same technology that allows drivers to pass through the drive-thru lane on freeways without stopping to pay the tolls or so-called “EZ-PASS” lanes. Although not as well known currently, major companies have announced plans to begin to equip their products with RFID tags. On such company is Gillette, who plans to put the RFID tags in their razors and blades, so that the products can be tracked from the factory until the consumer checks out with them in the store. Tracking the products is believed to avoid the high cost of stolen product every year. Another company, Benetton also had plans to sew the tags into their clothing, but their plans were halted when a group launched a boycott of their products. Today, both Wal-Mart and the US Military have set guidelines to have all of their cartons and pallets marked with RFID tags by January of 2005. Privacy advocates are concerned that the RFID technology will be used not only to track from factory to store but also after the consumer has purchased the product. As a result, those advocates propose that the RFID tag have a “switch” that turns off at checkout, preventing further tracking. Simson L. Garfinkel, The Trouble with RFID, The Nation, Feb. 3, 2004, available at http://www.thenation.com/doc.mhtml?i=20040216&s=garfinkel. In addition, RFID tags have been used in Buffalo, New York in an elementary school. There, director Gary Stillman uses the technology to track the time that students arrive in the morning; he plans to expand the use of the technology to track library loans, disciplinary records, cafeteria purchase, and visits to the nurse’s office. According to Stillman, “...[W]e could confirm that Johnny Jones got off at Oak and Hurtle at 3:22...All this relates to safety and keeping track of kids...Eventually it will become a monitoring tool for us.” These Last Days Ministries, The Three R’s: Reading, Writing, RFID chips, http://www.tldm.org/News4/MarkoftheBeast.htm (last visited Feb. 2, 2005). Finally, RFID chips may already be in euros, the European currency, and tires. Id.
glass casing contains the chip, which is shaped and measured at about the size of a grain of rice. In a relatively simple, quick, and painless outpatient procedure, a hollow needle places the chip beneath the skin. The whole procedure is often compared to getting a shot.

The recommended area for implantation of the Verichip™ is in the tricep, between the elbow and the shoulder of the right arm, and the cost of the procedure is nominal right now. For humans, the implantation procedure currently costs about $150-200 in addition to the $200 fee for the chip itself. To promote use of the chip, Applied Digital has provided about 200 scanners to trauma centers for free. For pets, a similar device has been marketed for years for about $50 per pet.

Supporters and some media reporters have affectionately referred to the implantation procedure as "getting chipped," and praise its capabilities. Once implanted with the chip, each patient is issued a “unique subscriber number” that provides access to a “Global Verichip™ Subscriber” (GVS) registry, which is maintained on the web by a secure server and two GVS Registry Operations Centers located in Riverside, California and Owings, Maryland. Each


Coughlan, supra note 65.

Rob Stein, Use of Imprinted Patient-Data Chips Stirs Debate on Medicine vs. Privacy, WASH. POST, March 15, 2006, at A01, available at http://www.washingtonpost.com/wp-dyn/content/article/2006/03/14/AR2006031402039.html (featuring a picture of the Verichip); Groves, supra note 27 (featuring a picture of a patient being implanted with the Verichip).

It is described as a “quick, painless outpatient procedure (much like getting a shot)” NECERATO, supra note 60, at 13.

NECERATO, supra note 60, at 15.

Id. at 19.

Groves, supra note 27.

NECERATO, supra note 60, at 19.


Id.

NECERATO, supra note 64, at 14.
Verichip™ stores the patient’s code, which is read by a scanner when it passes over it. The closest analogy to the Verichip’s™ capabilities is a UPC code on food and other products. When an UPC code is scanned by a cashier, the price pops up on the cashier’s screen in the same way that a patient’s number would pop up on a scanner when his/her chip is scanned. The chip itself will contain no medical records, but instead, numerical codes that can aid health providers in accessing the patient’s information through a database. Medical personnel will use a handheld scanner to pick up the low-level frequency emitted by the chip to read the patient’s unique code. After obtaining the code, health providers will then use the code in a database to access the patient’s entire profile and determine past treatments and other information. The database, and not the chip itself, would be updated with each of the patient’s visits.

In his interview with Today show host Matt Lauer, President Scott R. Silverman demonstrated the chip’s powers. After a scanner passed over Silverman’s arm, a laptop displayed his picture, name, and a unique number that he identified as a health identification number than can hopefully, one day, access all his medical records from a national medical database.

According to Silverman, about 1,000 people world-wide have already been implanted with the chip, including a half dozen of the company’s own executives. An entire family from Florida, the Jacobs, was one of the first to volunteer for the chip. Jeff and Leslie Groves, supra note 27.

---

1331
Jacobs and their 14-year-old son, Derek, decided to “get chipped,” because they thought that the chip would be an ideal way to store their medical information. Dr. John D. Halmaka, MD, MS, Chief Information Officer of Harvard Medical School, also volunteered to be chipped in December of 2004 so that he could assess the technology before deciding whether to recommend it for his patients.

Silverman also claims that nearly 80 percent of Americans would have the chip implanted if it offered a medical benefit, and Applied Digital’s medical advisor, Dr. Richard Seeley, has stated that the chip offers great advantages to those who see multiple physicians, such as patients with Alzheimer’s disease and diabetes. Before families, a similar chip was implanted in about 10 million pets in Europe and the United States to help prevent them from getting lost.

In the United States, Henry Schein, Inc., which is the largest provider of healthcare products in all of North America and Europe and serves 45-50% of all the U.S. medical practices, has agreed to market the Verichip™, so it seems the Verichip™ is certainly in the early stages of major success. Indeed, the Molly Foundation for Diabetes Research at Hackensack University in New Jersey has approved the Verichip™ and will begin using it for diabetic patients if the hospital agrees to it. The chip is thought to be of utmost importance and incredibly helpful for diabetics, because of the likelihood of them being...
unconscious and unable to relay important information about their medical history when brought to the hospital.

As a precursor to its success, Applied Digital has begun to try to ally any concerns. At the World ID conference in Barcelona, Spain, Silverman outlined a privacy policy and announced the appointment of Michael Krawitz to the position of Chief Privacy Officer of Applied Digital. His primary duty is to address privacy concerns and patients' rights issues. At the same time, Applied Digital has offered scanners, at a cost of $650 each, for free to trauma centers and hospitals nationwide in a promotional campaign.

Outside the United States, the Verichip™ has been marketed and used in a variety of other ways with almost no public notice. For example, in Mexico, a governmental agency has used the Verichip™ for security purposes. There, the few employees who have access to certain high security governmental areas have been implanted with the Verichip™ and now can move through the building effortlessly, as security personnel track and monitor their movement. In addition, approximately 1,000 Mexican citizens have had the chip implanted to link to their medical records.

As in Mexico, SurgeIT Solutions, a British company, has signed an agreement to use the Verichip™ to control access to governmental facilities as well. In Italy, Antonia Giorgio Antonucci, an Italian physician, is leading a study using Verichip™ at the National Institute for Infectious Diseases Lazzaro Spallanzani in Rome to see whether

---

93 See id.
94 Id.
96 Id.
97 Groves, supra note 27.
98 Feder & Zeller, supra note 1, at A1.
99 Id.
100 Rafael Macedo de la Concha, Mexico’s attorney general, claims that use of the Verichip by he and his subordinates have been vital in Mexico’s struggle with drug cartels and controlling access to secure documents and areas. Id. See Will Weissert, Chip Implanted in Mexico Judicial Workers, WASH. POST, July 15, 2004 at A5, available at http://www.washingtonpost.com/wp-dyn/articles/A51444-2004Jul15.html (last visited Apr. 25, 2006).
physicians believe that the device is useful. In Brazil, Applied Digital has signed contracts with distributors in Brazil to help combat the problem of kidnapping. In Japan, some parents are inserting RFID tags into their children’s backpacks and pockets of clothing to prevent kidnapping. And on January 21, 2005, exclusive rights were granted to Verichip Corporation to distribute the chips in Thailand/Indonesia, Malaysia, and South Korea.

The Verichip™ has been marketed socially, as well. In Barcelona, Spain, a nightclub decided to market the chip to its VIP members; VIP members implanted with the chip can order drinks and pass to exclusive areas of the club with a simple wave of the hand. Their chips are linked to their own VIP accounts, allowing for automatic deductions and payments with each drink order without the patron every having to reach for his/her wallet.

Concerned citizens have objected tremendously … and they aren’t just clubbers worried about their bar tabs. Specifically, privacy advocates argue that the Verichip™’s capabilities make it much easier for patient privacy to be sacrificed as well as present unique possibilities for abuse. Democratic Senator Patrick Leahy and


103 NECERATO, supra note 60, at 54.


105 Applied Digital, supra note 95.

106 See Baja Beach Club online, http://www.bajabeach.es; see also Baja Beach Club, Design, Construction, Supervision, & Technology, http://www.baja.nl/corporate.aspx?CorID=5 ("[w]e pride ourselves on being on the cutting edge of technology is all of our clubs and in the corporate office. We are constantly reviewing new computer hardware and software that can help us accomplish our daily tasks more efficiently."); Violet Jones, Baja Beach Club in Barcelona, Spain Launches Microchip Implantation for VIP Members, available at http://www.prisonplanet.com/articles/april2004/040704bajabeachclub.htm [hereinafter Baja Beach Interview]; Feder & Zeller, supra note 1, at A1.

107 See Baja Beach Interview, supra note 106.

108 According to Leahy, administration officials, “have been silent on the extent to which these important security, privacy, and civil-liberties implications and have been considered during the process of approving this new technology.” Editors, I’ve Got You Under My Skin: Tracking Technology Gets Personal, 7 The New Atlantis: A J. of Tech. and Sci. 133, 134 (Fall 2004/Winter 2005), at http://www.thenewatlantis.com/archive/7/soa/underskin.htm (last visited Apr. 25, 2006).
privacy advocate and CEO of Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), Katherine Albrecht, have separately expressed concerns about the FDA’s approval of the Verichip™ device.\textsuperscript{109} Other critics worry that it will deprive individuals of personal privacy,\textsuperscript{110} which has already been lost to inventions such as DNA testing, genetic profiling, fingerprinting, optical scans, credit cards, Social Security numbers, drivers’ licenses, and other information-gathering systems.\textsuperscript{111} Most recently, State Representative Marlin Schneider initiated a bill in his state of Wisconsin which would prohibit anyone from requiring residents to have the chips implanted; any violation would render a fine of $10,000.\textsuperscript{112}

There are other concerns, too. Apparently, in addition to storing text and offering the ability to link to accounts or security systems, this little bug can cause quite a stir; the FDA has been accused of failing to consider and publicize risks such as adverse tissue reaction, migration of the implant, electromagnetic interference, failure of the transponder, electrical hazards, and magnetic resonance imaging (MRI) incompatibility.\textsuperscript{113}

\textsuperscript{109} See Katherine Albrecht, \textit{Supermarket Cards: The Tip of The Retail Surveillance Iceberg}, 79 DEN. U. L. REV. 534, 539 (2002) (noting that profiling using information gained from supermarket cards has already begun; in Arizona, DEA agents obtained records of individuals who had purchased large amounts of plastic bags and, post 9/11, supermarket records were consulted to determine suspected terrorists eating habits). \textit{See generally ACLU.org, RFID Position Statement of Consumer Privacy and Civil Liberties Organizations,} \textit{at} http://www.aclu.org/safefree/resources/17423pub20031130.html (last visited Jan. 25, 2006).


\textsuperscript{111} Groves, \textit{supra} note 27. "Technology has moved at the speed of light, but laws protecting privacy are in the Stone Age," said Deborah Jacobs, executive director of American Civil Liberties Union of New Jersey." \textit{Id.}


\textsuperscript{113} Infowars.net, Digital Angel Exiting Applied Digital? Did Company Fail to Publicize Verichip Risks?, \textit{at} http://www.infowars.net/Pages/Oct_04/211004_digital_angel.html (last visited Jan. 25, 2006). Indeed, on October 14, 2004, the day after the FDA approved the Verichip™, Digital Angel sold its 1,069,650 shares of Applied Digital common stock for the net proceeds of $4 million. \textit{Id. See also NECERATO, supra note 64, at 60.}
In any event, now that the FDA has approved the device for use in this country, the plan is for the chip to contain a unique number that can only be used by health care providers to access a patient’s medical history from a to-be-formed national medical database, although the details of the database are still unknown.\textsuperscript{114}

Part III. MAINSTREAM USE OF THE VERICHIPTM

A Call For Legislation

"Respect for persons will be best served not by insisting on absolute privacy, which is unattainable in modern life anyway, but by seeking informed consent to reasonable use of health information under strictly delimited conditions; by safeguarding personal data carefully; by genuinely affording fair-information-use rights to data-subjects; and by enforcing sanctions against improper use." William H. Lowrance, Ph.D., Privacy and Health Research.\textsuperscript{115}

Aside from initial privacy concerns,\textsuperscript{116} which have been covered rather extensively, the chip also presents issues of consent.\textsuperscript{117} Although the company and its president continually maintain that the chip will be implanted on a \textit{voluntary and consensual} basis only, one has to

\textsuperscript{114} Feder & Zeller, \textit{supra} note 1, at A1. However, David J. Brailer, MD, is the national coordinator for healthcare information technology and recently spoke at the Healthcare Information and Management Systems Society (HIMSS) 2005 Annual Conference and Exhibition in Dallas, Texas. \textit{See} Fred Bazzoli, \textit{Brailer Mobilizes Government to Review NHIN Responses}, Feb. 22, 2005, \textit{available at} http://www.healthcareitnews.com/story.cms?id=2511 (last visited Jan. 25, 2006). There, he discussed a task force that is currently reviewing plans for the national healthcare information network. \textit{Id}. The federal task force includes about 100 individuals from 20 different agencies, divided into three different workgroups. \textit{Id}. One group is identifying legal issues, the second is addressing technical problems, and the third is looking at policy issues. \textit{Id}. Brailer’s office expects to present some prototypes based on their conclusions. \textit{Id}


\textsuperscript{116} According to a Gallup Survey on Medical Privacy, 78% of persons feel that it is very important that their medical records be kept confidential. Institute for Health Freedom, \textit{Public Attitudes Toward Medical Privacy}, http://forhealthfreedom.org/Gallupsurvey/IHF-Gallup.html (last visited Jan. 25, 2006).

\textsuperscript{117} \textit{See generally} Albrecht, \textit{supra} note 109.
question the practical consequences of the chip becoming mainstream.\textsuperscript{118} Indeed, as in Mexico, the Verichip\textsuperscript{TM} does have the ability to be used for tracking purposes, and Applied Digital has expressed interest in moving the Verichip\textsuperscript{TM} into other marketable areas, such as credit-card verification.\textsuperscript{119}

Therefore, this section will discuss and speculate whether “non-chipped” patients will be at a disadvantage in the future for not having consented to be “chipped,” and calls upon legislators to attend to this timely issue preemptively, rather than post-hoc. Primarily this section speculates as to the results of the Verichip\textsuperscript{TM}’s success, specifically the possibility that consent on a voluntary basis will no longer be truly voluntary. That is, if Verichip\textsuperscript{TM} becomes the universal carrier for HIPAA’s UHID and scanners become the norm in hospitals\textsuperscript{120} to recover medical records, what of the unwilling population? Will those persons be at a disadvantage and receive substandard medical treatment as a result of not being chipped?

Illustrations most properly demonstrate the concern. Imagine an emergency room, and the number of patients coming in and out of the hospital every day. An ambulance screeches to a halt outside the emergency room door, and the paramedics wheel out a gurney carrying an unconscious and bloody patient. They tell the physicians that they found the patient slumped over the wheel in a truck that had crashed into a guidepost but there were no witnesses. According to protocol, one of the attending physicians quickly passes a scanner over the body as it is being wheeled into the hospital. The scanner registers a reading in the patient’s arm with a number that the physician quickly rattles off to a nurse at a computer. The nurse types the number into the National Healthcare Database and pulls up the patient’s profile; his name is John Doe, he is allergic to latex and has been diagnosed with diabetes recently. A quick check of his demographics confirms his home address and phone number. The nurse quickly relays the information about his allergy to the doctors, who promptly change into non-latex gloves, and picks up the phone to call his home phone number and contact any family. From the profile and the body before them, the doctors quickly discern that John passed out at the wheel when his

\textsuperscript{118} Id.
\textsuperscript{119} Langberg, supra note 65, at 1E.
\textsuperscript{120} “Company officials say if the chip's use becomes routine, scanning people's arms for hidden chips would become second nature at hospitals.” NECERATO, supra note 64, at 19.
blood sugar became too low. The entire process takes less than five minutes.

Conversely, a few hours later at the same hospital another unconscious patient is wheeled into the emergency room. He has no identification on him of any kind and was found on the sidewalk by a passerby. The doctor with the scanner again passes the scanner over the body but registers no number. The doctors begin checking his vitals and taking actions to stabilize the patient, while the nurse at the computer leaves her computer and contacts a social worker to research who the man is and if he has any family. The doctors proceed with treatment without being aware of any allergies or past medical history.

Or consider a regular medical practice where a mother is taking her terminally ill child to yet another physician for another opinion. Efforts to get her child’s medical records transferred from the last office to this one have failed, due to the sheer volume of his file. Instead, she has resorted to compiling her own records, which she wheels into the new office with her. As usual, the receptionist passes her a clipboard with a New Patient form on it, and she busily begins to fill out the lengthy history.

The second two scenarios are most familiar to us, as they reflect current practices in healthcare, while the first represents “the future” if use of the Verichip™ became universal. That is, if patients more often than not are able to be identified through the use of a national healthcare database and a unique health identifier number on an implanted Verichip™, it is likely that medical professionals will become dependent upon the technology in carrying out their jobs. Therefore, like the unconscious man in the second scenario and the mother in the third, patients will be disadvantaged in their access to medical care. For example, if the man in the first scenario, identified to have an allergy to latex, was treated by physicians wearing latex gloves, causing a near-death reaction, he arguably would have legal recourse against those physicians for negligence, because that information was available to them through his electronic medical records. However, if the same events were to happen to the second man, he would not be able to assert an action, because the doctors would not have been aware of any of his conditions. Because of these far-fetched implications, even if legislation assures that the Verichip™ will only be implanted on a voluntary basis, once occurrences such as those outlined above become more common, people will be persuaded to get the chip.
Moreover, certain populations are at particularly high risks of being victimized by this technology. Prisoners, probationers, and parolees are among those that could potentially be abused by the Verichip's abilities and information storing capabilities. Already, those populations are subject to home monitoring systems, commonly known as "house arrest," that monitor their movements through the wearing of an electronic anklet. Military personnel are also at risk of being issued the Verichip and other similar tracking devices. Other populations, such as nursing home patients and other elderly, also seem to be threatened. Indeed, Dr. Seelig, a retired surgeon who helped develop the Verichip, has already mentioned that "[c]onsent is needed from people who hold power of attorney for patients, such as some nursing home residents who cannot speak for themselves."

Other risks include possible "kickbacks" or incentives to use the Verichip technology. First, employers may begin to advocate use

121 Christopher Newton, US to Weigh Computer Chip Implant, AP Online, Feb. 27, 2002, available at http://www.cephasministry.com/now_chip_news.html (last visited Jan. 25, 2006). "The problem is that you always have to think about what the device with be used for tomorrow," said Lee Tien, a senior attorney for the Electronic Frontier Foundation, a privacy advocacy group. Id. "It's what we call function creep. At first a device is used for applications we all agree are good but then it slowly is used for more than it was intended." Id.

122 See Feder & Zeller, supra note 1, at A1. "Critics warn that such technology could be used to track prisoners and parolees, as well as soldiers, who would not be able to withhold their consent if usage became mainstream." Id.

123 Langberg, supra note 65, at 1E. See also House Arrest Services, Inc., http://www.housearrest.com.


125 Groves, supra note 27.

126 Id.

127 Unatin, supra note 65, at 24.

The proposed initial applications [of the Verichip™] may be worthwhile, but many fear this technology would quickly snowball into a severe threat to individual privacy. Like any technology, the computer chip implant could potentially be abused. Once the chip is implanted, there could be little to prevent the wrong people from accessing it. In addition to the wrong people accessing the information, there is concern that authorized people would use it for the wrong reasons. For instance, a private company that monitors the tracking signals from these chips might be tempted to sell such information to advertisers.
of the technology as Mexico’s Attorney General has done in certain secure facilities.\textsuperscript{128} Legislation must be adopted to address and reaffirm each employee’s own personal right\textsuperscript{129} to refuse the technology. Employees should not be forced to accept the Verichip\textsuperscript{TM} as part of their occupations. Also, insurance companies should be prohibited by law from offering incentives to certain medical facilities or patients who opt-in to the technology. As insurance is expensive enough in America, patients should not be faced with a choice between insurance plans and decide based on a price-cut, if they get the Verichip\textsuperscript{TM}.

In general, legislators must face these challenges. Applied Digital has already issued its own statement regarding what legislation must cover.\textsuperscript{130} The six point statement lists the following:

1. The Verichip\textsuperscript{TM} should be voluntary and voluntary only. No person, no employer, no government should force anyone to get ‘chipped.’
2. Privacy must be a priority at the highest levels of our organization and as such we will have a Chief Privacy Officer who, with privacy experts, will be charged with addressing the day-to-day global evolution of this technology.

\textit{Id.} \textsuperscript{128} See Feder & Zeller, \textit{supra} note 1, at A1.


The factors which should be considered in deciding whether an intrusion into an individual’s privacy is justified are the type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy or other recognizable public interest militating toward access.

\textit{Westinghouse Electric}, 638 F.2d at 578.

3. We will immediately address privacy and patients’ rights in all consumer, distributor and medical documents related to Verichip™.

4. VeriChip™ subscribers are able to have their chip removed and discontinued at any time.

5. Privacy means different things to different people, so only the Verichip™ customer should designate the groups that may have access to his or her database information.

6. We pledge to thoughtfully, openly and considerately engage government, privacy groups, the industry and consumers to assure that the adoption of Verichip™ and RFID technology is through education and unity rather than isolation and division.  

However, this statement addresses only privacy concerns with the Verichip™. Other concerns, especially the consent issue, must be addressed both by the company and legislators. Specifically, individuals should be in control at all times; the chip must be able to be deactivated and removed, and insurance companies and other agencies should not be able to offer the chip as an incentive for any reason, especially for at-risk populations such as the elderly, prisoners, and parolees. As to the concern of the Verichip™ becoming mainstream, hospitals adopting the technology should stay vigilant in keeping personnel updated on protocol and procedures. Although the Verichip™ may have attractive qualities to the healthcare industry, training sessions must emphasize the probability of the widespread use of the device, while stressing the importance of treating patients without the device. Otherwise, physicians and other medical personnel could become dependent on the device and its capabilities and, as a result, render substandard care to the non-chipped patients.

In conclusion, even if the Verichip™ does not achieve the mainstream success, some similar technology will be in place in the healthcare industry in the near future. Therefore, the same issues of consent and privacy are timely, regardless of the Verichip’s™ ultimate destiny. For these reasons, legislators must address these issues and approach such powerful technology with caution. Given our society’s

---

131 Id.
132 Id.
133 See Langberg, supra note 65, at 1E. In addition, scanners should not be hidden; a universal symbol should show where the scanners are. Currently, they “can be built into walls, door frames or even highway signs.” Id.
acceptance of any device aimed at ease and efficiency, it is likely that the Verichip™ could be accepted in mainstream society without much thought to these concerns. Unless legislators are attentive and purposeful with legislation, major issues of privacy and consent will go unnoticed. The healthcare industry has a very promising future in its marriage to health IT technology; that future can be both bright and immensely helpful with preemptive legislation attacking consent and privacy issues.