CALIFORNIA HEALTH LAW NEWS

VOLUME XXXIV, ISSUE 1, WINTER 2016 *A Publication of the California Society for Healthcare Attorneys*

HEALTH CARE'S ADVENTURES IN WONDERLAND:

Provider Agreements for Electronic Health Records

By Craig B. Garner

and Jessica Weizenbluth

"Now, here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!" [1]

I. INTRODUCTION

Y93.J1: Activity, piano playing[2]

Today's health care provides its own spin on the word "complex,"[3] while at the same time forging possible paths to what may be "unwinnable" scenarios.[4] For the modern physician,[5] the universe within which he or she exists requires updated definitions for words such as "complex" and "challenging," especially as that "perfect storm" [6] also known as health care reform continues to rage. Somewhere in between the 2015 Physician Quality Reporting System (PQRS) [7], the Physician Value-Based Payment Modifying Policies (VBP)[8] and tenth revision of the International Statistical Classification of Diseases and Related Health Problems (also known as ICD-10),[9] physicians find themselves still struggling to adopt electronic health records (EHR) in practice.[10]

As technology continues to evolve, there remains a general landscape with which those in the health care field must familiarize themselves. Even from this challenging vantage point, providers still have opportunities to bolster their position and practice their craft as they continue down the digital path and adopt an EHR system for which the federal government established incentive payments.[11]

II. WHAT COULD GO WRONG?

Z73.4: Inadequate social skills, not elsewhere classified

In 2004, President George W. Bush announced his administration's objective for "development and nationwide implementation of an interoperable health information technology infrastructure to improve the quality and efficiency of health care."[12] In fact, President Bush predicted that by 2014 there would be "an interoperable electronic health record for each U.S. resident."[13] Needless to say, President Bush's goal is still a work in progress. Still, a decade later, 2015 has been a busy year for federal regulations on EHR incentive programs and meaningful use for eligible providers (EPs), all of which occurred concurrently with the downward payment adjustments under the Medicare EHR Incentive Program,[14] updates to the certification criteria, as well as the Health IT Certification Program by the Office of the National Coordinator (ONC),[15] and the solidification of the fate of the Merit-Based Incentive Payment System (MIPS) for EPs long into the future.[16]

Today, the federal government has outlined four specific goals in its attempt to apply the "effective use of information and technology to help the nation achieve high-quality care at lower costs, a healthy population, and engaged individuals."[17] These goals include: (1) the advancement of person-centered and self-managed

health; (2) the transformation of health care delivery and community health; (3) the fostering of research, scientific knowledge and innovation; and (4) the enhancement of the nation's health IT infrastructure.[18] A laudable objective notwithstanding, EHR implementation nevertheless has encountered certain challenges along the way.[19]

These so-called challenges present for certain providers as larger obstacles to implementation. On the front line of health care reform, physicians must lead the EHR charge, even as they face the greatest risk individually without many opportunities to align independently. Even though many consider EHR to be cost prohibitive, the federal government addressed implementation, in part, when it encouraged physician and hospital alignment to further EHR.[20] The track on which EHR exists appears to be incapable of derailment, but providers would be remiss to think that the contractual agreements that create a vehicle with which they can join the convoy, contain the entire gamut of necessary rails. Rather, each provider should examine the path ahead, paying careful attention to key terms that may prove the difference between digital success and demise.

III. SOME IMPORTANT TERMS TO CONSIDER

W61.33XA: Pecked by a chicken, initial encounter

When transitioning from paper to digital in any medical practice, providers must familiarize themselves with basic field-related terminology, as well as gain a general understanding of the pending technological acquisition, not to mention what the potential developer/partner provides and what it demands in return. To be sure, such information is far more useful *before* signing an agreement than after execution. Not understanding some of the more salient terms and conditions of an agreement to acquire an EHR system, especially terms unique to this new digital frontier, can compromise a provider's medical practice, and have the potential to create vulnerabilities in the delivery of patient care as set forth below, if unfavorable terms were to evolve into medical risks.[21] This section provides a general overview of key terms, the knowledge of which all providers should be mindful.

A. Indemnification

1. Indemnification as a Moving Target

In many contractual relationships, the notion of indemnification serves as the cornerstone for protection.[22] In an EHR contract, the party charged with technology development must offer the EHR software to the health care provider with certain necessary services, and the provider agrees to pay the cost (alone or with one or more third parties).[23] Bound and isolated by the agreement, success is typically dependent upon the actions and omissions of the developer and provider.[24] Indemnification language in developer contracts is critical, especially when third party claims loom in the distance.[25] The degree to which one party must indemnify the other for transgressions, set forth in contractual indemnity provisions, can be the difference between success and failure.[26] Other times, however, an agreement may be altogether[27] silent on indemnification.

When drafting an indemnity clause, the developer may insist that the provider bear liability for any third party claims that arise from the EHR technology software.[28] Providers should be reluctant to accept such liability, especially for technology outside the scope of the provider's expertise and control.[29] Reasonable parties generally accept responsibility for the risk of reasonable culpability, but not much more. Developers will insist the providers indemnify for all personal injury or death claims, at least to the extent such a claim includes third parties like developers. Unless the harm to patient care resulted from an unlikely issue on the part of the developers, such potential liability is not unreasonable for providers to keep. Other claims, such as privacy violations, may not be as objective for purposes of allocating culpability. While this is a fundamental tenet of the system, there is often a fine line between a technical malfunction and "user error." If possible, it is best to approach indemnification through mutuality, so that each party is responsible for its own acts and omissions.

2. Indemnification (Intellectual Property)

When providers and developers contract, it would be nice to assume that all necessary software licenses and legal rights are in order, to accommodate the transaction.[30] There are instances in which a developer intentionally, unintentionally or recklessly fails to obtain certain legal rights and, as a result, the third party who holds exclusive or superior ownership rights to the intellectual property, takes issue.[31] Under California law, the owner of a patent or copyright for intellectual property has the right to sue

anyone who uses the intellectual property without having first obtained the necessary rights.[32] Indemnity can be as broad as a contract provides or even implied through its absence in an agreement, or in equity.[33] Insurance, too, is prudent in an agreement, and those between provider and developer are no exception.[34]

B. Confidentiality and Non-Disclosure Agreements

Z73.1: Type A behavior pattern

Both provider and developer may insist on certain confidentiality requirements before, during, and possibly even after the existence of a contract between them.[35] Developer contracts may define "confidential information" too broadly, and such scope is almost always prudent to measure. To be sure, the developer may include provisions restricting disclosure of the technology to third parties, not to mention the consequences for failing to comply, such as the right to terminate the agreement upon a confidentiality breach.[36]

Too broad a definition, however, could prevent a provider from entering into meaningful negotiations, especially if a confidentiality agreement creates restrictions on disclosure to trusted advisors. Restrictions that prevent sharing certain information with other providers could compromise certain networks if the sharing of such information proves important yet prohibited.[37] In the field of health care, confidentiality is almost always important, but even privacy has certain limitations. Providers should be mindful not to become unnecessarily bound, especially when it comes to conducting business.[38] At the same time, providers should insist on protecting sensitive practice information, thereby making it critical that the confidentiality agreement is mutual. If this creates a source of contention with the developer, it may signal yet again the importance of finding a different developer.

There are also exceptions to confidentiality obligations, despite the language in an agreement.[39] One such instance includes disclosure mandated by law.[40] Certain situations, however, may not create a legal obligation to disclose, but there may be other reasons why a party desires to volunteer information at the center of a confidentiality agreement, so appropriate language in a confidentiality agreement can still preserve the integrity of a provider's practice, as well as his or her reputation. Only by understanding the terms for a confidentiality agreement, can a provider make certain, sensitive disclosures with confidence.[41]

C. A Storm is Coming

The path toward EHR has not always been without skeptics.[42] While modern medicine may accept the importance of creating a digital record of each and every patient experience, the resulting disruption is not overlooked.[43] "One of the under-told stories from the digitizing of patient records is the burden computerized documentation places on doctors. They are being tasked with greater data entry, and less with analysis and care. This goes beyond anecdotes."[44] To be sure, technology today creates new opportunities for providers that simply did not exist in the past, not to mention the possibility of delivering superior medical care due to the accessibility of the information at hand.[45] Notwithstanding, some architects of the proverbial cloud, including Amazon, Google and Microsoft, fail to embrace this technology in the way that federal and state laws mandate health care's acquiescence.[46] Only time will tell, however, if the cloud is ready for health care and its EHR requirements.[47]

D. Warranties and Disclaimers

Y92241: Hurt at the library

A warranty is an express or implied assurance from one party that what it promises in the contract will in fact be provided to the other party.[48] An implied warranty is one that may be contractually binding, even if unstated,[49] while an express warranty is set forth in the agreement.[50] If parties prefer to avoid any implied warranties, a contract can always expressly disclaim them.[51]

At times, developer contracts may include an express warranty, but only as it relates to the developer's "then current" technology.[52] Understanding a transaction's "then current" status is challenging, yet critical for both sides. Providers should review the documentation to identify which provisions refer to and determine the technology needed at the time the parties enter into an agreement, at least to the extent the provider desires an express warranty.[53] As an extra measure of protection, a provider may want to include language that protects against any adverse impact from future changes and technology, or states that these same changes down the road will not retroactively compromise the express warranty in place. Rather than predicting future technology, however, a sound practice should be the inclusion of all material specifications, initial developer proposals and provider needs, leaving nothing to chance outside the four corners of the final agreement.[54]

1. Meaningful Use Warranty

"Meaningful Use" is part of the foundation for most agreements between developer and provider.[55] Standard terminology in developer contracts designed to identify provider eligibility for participation in Medicare and Medicaid EHR Meaningful Use Incentive Programs should always include an express warranty covering Meaningful Use certification for the present, as well as the necessary and appropriate future modifications required by federal law.[56] If a developer is not willing to expressly warrant for Meaningful Use, providers must determine the developer's status for certifying the same.[57] Providers should be cautious when a developer expressly certifies Meaningful Use at the time the parties enter into an agreement but refuses to make any representations for the future.[58] With no future warranties, a change in the developer's system that results in a loss of certification, or perhaps even the loss of the developer, will create sizable challenges for any provider. Planning for such an event can be even more complicated, especially if the developer cannot provide price information on the cost to comply with that which is unknown.

2. Integration Clauses

"Terms set forth in a writing intended by the parties as a final expression of their agreement with respect to the terms included therein may not be contradicted by evidence of a prior agreement or of a contemporaneous oral agreement."[59] This standard integration clause language, common in most agreements, "vitiates" any and all promises and representations made before the parties agreed to contract. Irrespective of what was discussed in the past, the inclusion of similar language effectively ensures that the agreement is all that really matters from this point forward. While this applies to the "four corners" of the agreement between provider and developer, providers should always make sure the acquisition is comprehensive enough to address all facets of EHR and that it communicates directly with the surrounding digital landscape from where the provider is expected to make meaningful use of its EHR. Anything less than such a demand may defeat the very purpose for the software.

E. Limitation of Liability

Y92.253: Opera house as the occurrence of external cause

A limitation of liability clause is a provision that limits the financial risk a company faces in the event of a lawsuit usually by placing limits on the amount of potential damages a company may be required to pay.[60] In an EHR contract, providers should be reluctant to limit the liability for the developer, either with monetary caps on payout obligations or by excluding consequential and other special damages so that the developer is only liable for direct damages.

Before signing any agreement, providers should determine if the developer has set a maximum dollar amount for liability. If there is a maximum dollar threshold, providers should analyze how this amount could impact business under different scenarios. Rather than limiting liability based on a dollar amount, providers may consider liability limitations in terms of possible categories of damages, although it is difficult to waive liability for direct damages (arising from costs incurred as a result of a party's breach).[61] A developer typically will seek to avoid liability for consequential damages, which are damages that result on account of the breach, such as lost profits or damage to reputation.[62]

F. Termination and Wind Down

R46.1: Bizarre personal appearance

It is never too soon for a provider to think about the end, or at least the end of an agreement with a developer. Continuous access to patient records is critical for almost all practices, and equally important is the language in an agreement addressing a possible transfer of information from one EHR system to another.[63] It is also important that the operative business associate agreement (BAA) include a provision that ensures the return or destruction of all protected health information (PHI).[64] While providers would be prudent to demand the return of their own information, at a minimum they must ensure there is no compromise on the integrity of that information.

One of the Health Insurance Portability and Accountability Act's (HIPAA's) original tenets was portability, at least for the patient's health records. Patient health information quickly evolved into "PHI" and "the meaning ascribed to it in the regulations concerning the confidentiality of individually identifiable health information promulgated by the Secretary of Health and Human Services" pursuant to HIPAA.[65] After enactment of the Health Information Technology for Economic and Clinical Health Act (HITECH), the idea of portability merged with data portability, the purpose of which includes the following:

Data portability. Enable a user to electronically create a set of export summaries for all patients in EHR technology formatted according to the standard adopted at § 170.205(a)(3) that represents the most current clinical information about each patient and includes, at a minimum, the Common MU Data Set and the following data expressed, where applicable, according to the specified standard(s):

- *(i) Encounter diagnoses. The standard specified in § 170.207(i) or, at a minimum, the version of the standard at § 170.207(a)(3);*
- *(ii) Immunizations. The standard specified in § 170.207(e)(2);*
- *(iii) Cognitive status;*
- *(iv) Functional status; and*
- *(v) Ambulatory setting only. The reason for referral; and referring or transitioning provider's name and office contact information.*
- *(vi) Inpatient setting only. Discharge instructions.*[66]

Providers are like shepherds, only guarding medical records instead of sheep. With an appropriate BAA in place between providers and developers, the collection of the medical records at the conclusion of the agreement should resemble the return or destroy language in most BAAs.[67] It is important that providers preserve the default provisions of a BAA in agreements with developers, and even more important that the developers comply.

The standard by which developers must maintain an EHR system for purposes of certification is always evolving, yet the standards remain strong. Until January 13, 2016, the patient summary record must meet the following standards:

(1) Standard. Health Level Seven Clinical Document Architecture (CDA) Release 2, Continuity of Care Document (CCD) (incorporated by reference in § 170.299). Implementation specifications. The Healthcare Information Technology Standards Panel (HITSP) Summary Documents Using HL7 CCD Component HITSP/C32 (incorporated by reference in § 170.299).

(2) Standard. ASTM E2369 Standard Specification for Continuity of Care Record and Adjunct to ASTM E2369 (incorporated by reference in § 170.299).

(3) Standard. HL7 Implementation Guide for CDA ® Release 2: IHE Health Story Consolidation, (incorporated by reference in § 170.299). The use of the "unstructured document" document-level template is prohibited.[68]

After January 13, 2016, the standards include a fourth requirement:

(4) Standard. HL7 Implementation Guide for CDA ® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use, Volume 1—Introductory Material, Release 2.1 and HL7 Implementation Guide for CDA ® Release 2: Consolidated CDA Templates for Clinical Notes (US Realm), Draft Standard for Trial Use, Volume 2—Templates and Supporting Material, Release 2.1 (incorporated by reference in § 170.299).[69]

No matter how the relationship between provider and developer may end, it does not modify the EHR-related obligations on the part of the provider. Even as the standards evolve, provider compliance is not optional. As important as termination and wind down may be for the provider, it is only a transition.[70] The ease with which a provider can move from one developer to another depends on the developer agreement, not to mention the condition of the provider's information upon retrieval from the system, assuming the information the provider can retrieve exists in a usable format.[71] Outright denial by a developer, of course, creates an entirely added level of complexity for the provider,[72] although strict adherence to federal law in drafting BAAs should prevent such an unpleasant result.[73] Ultimately, providers must retrieve patient information in an accessible format upon termination of the agreement. "Portability" (another term from HIPAA) remains critical. The cost and timing for such a transition is also an important item to negotiate before entering into an agreement with a developer. Providers should always be mindful that business stability upon termination is critical.

G. Dispute Resolution

Z63.1: Problems in relationship with in-laws

The dispute resolution provisions within an EHR contract are integral to avoid any disruption in patient care and business operations.[74] To determine the best option for providers, consider what is available, and how implementation would occur. Providers should be mindful that during a dispute the need to maintain an EHR system most likely remains.[75] The costs of replacement or disruption of services, however, may be more challenging and expensive than the dispute itself.[76] While alternative dispute resolution and arbitration in particular may be just as difficult to avoid as the underlying disagreement, the effectiveness of these options in litigation depends upon the speed with

which a resolution may occur.[77] Providers should not ignore the additional benefits to mediation, especially when the dispute involves sensitive business information or even PHI.[78]

H. The Take Away is that EHR is Not Going Away

As a result of California Senate Bill 945 (2010),[79] Medi-Cal can distribute one billion four hundred million dollars ($1,400,000,000) to Medi-Cal providers over the next 10 years for EHR support purposes.[80] The federal and state commitments to wide scale implementation of EHR are unmistakably clear, but ultimate success depends upon the ways in which providers and developers interact to accomplish these objectives. Health care is a business,[81] and for providers to successfully participate in EHR implementation, they must focus on all salient provisions of any developer agreement.

IV. HITECH WITHOUT THE EHR BUBBLE

A. There Is Always Room to Improve

Z62.891: Sibling rivalry

Notwithstanding the importance of provider success when it comes to EHR implementation, each and every provider path intersects with HITECH and the privacy obligations set forth in HIPAA. The success of health care reform depends in large part on innovation, including the replacement of paper medical records with EHRs. Still, the federal government recommends the same degree of vigilance as before.[82] In a January 2014 study, the Office of Inspector General (OIG) for the United States Department of Health and Human Services (DHHS) noted:

> *[C]ertain EHR technology features may be used to make true authorship of the medical record and distort information to inflate health care claims. The transition from paper records to EHRs may present new vulnerabilities and require the Centers for Medicare & Medicaid Services ("CMS") and its contractors to adjust their techniques for identifying improper payments and investigating fraud.*[83]

More recently, the OIG urged the federal Office for Civil Rights (OCR)[84] to *strengthen* its oversight of the ways in which covered entities comply with the privacy standards under HIPAA[85] as well as OCR's follow up on reported breaches of patient health information.[86]

B. When Things Go Wrong

V9542XA: Spacecraft crash injuring occupant

Even the best-made plans for EHR do not always work, the result of which can be a "data breach."[87]

Violation[88]	Minimum Penalty	Maximum Penalty	Annual Maximum Penalty
Entity did not know (even with reasonable diligence[89])	$100 per violation	$50,000 per violation	$1.5 million
Reasonable cause,[90] not willful neglect	$1,000	$50,000	$1.5 million
Willful neglect,[91] but corrected within 30 days	$10,000	$50,000	$1.5 million
Willful neglect, not corrected	$50,000	None	$1.5 million

Monetary penalties notwithstanding, HIPAA and HITECH obligate providers to mitigate the damage caused by privacy transgressions, including the use or disclosure of PHI.[92] Federal law also requires the provider to give notice to each individual whose unsecured PHI has been disclosed due to a breach, or there is a reasonable belief of a disclosure.[93] State law also requires licensed facilities (including hospitals, skilled nursing facilities, etc.), clinics, home health agencies and hospices to notify patients and CDPH of breaches within 15 business days of identification.[94]

V. CONCLUSION

In the past several years, the United States has spent billions of dollars to safeguard the gamut of health information, from broken bones to heart surgery to mental illness, all of which are protected by federal and state law from public disclosure.[95] The OCR handled 109,722 HIPAA-related complaints registered between April 2003 and February 1, 2015.[96] Private practices and acute care hospitals were among the worst offenders.[97] When it comes to PHI and EHR, the law of our nation affords strict confidentiality to each and every patient.[98] The influence of HIPAA and HITECH on health care has changed its very infrastructure, protecting the disclosure of a broken finger equally as a diagnosis of iatrophobia.[99]

Without provider participation and cooperation, however, HIPAA and HITECH mean nothing. Failure by a provider to follow the strict requirements of HIPAA and HITECH may result in loss of license, significant financial penalties, or both.[100] To be sure, providers have financial incentives to comply with HIPAA and HITECH, including Meaningful Use.[101] To avoid penalties and enjoy the financial incentives of statutes and regulations relating to EHR, there will be a developer agreement along the way, into which providers must enter. Providers should be mindful that such agreements, although necessary, can be treacherous, and providers must pay careful attention to all terms included therein, especially since HIPAA and HITECH are rather unforgiving.[102]

ABOUT THE AUTHORS

Craig B. Garner is an attorney and health care consultant, specializing in issues surrounding modern American health care and the ways in which it should be managed in its current climate of reform. His law practice focuses on health care mergers and acquisitions, regulatory compliance and counseling for providers. Craig is a Fellow of the American College of Healthcare Executives and an adjunct professor of law at Pepperdine University School of Law. Between 2002 and 2011, he was the Chief Executive Officer at Coast Plaza Hospital in Norwalk, CA. Craig may be reached at craig@garnerhealth.com.

Jessica Weizenbluth is an attorney specializing in health care law with a particular focus in regulatory compliance, business transactions and providing counsel to providers. She is licensed to practice in both California and Ontario, Canada, a member of the California Society for Healthcare Attorneys, Los Angeles County Bar Association and the American Bar Association. Jessica is also a member of the Beth Tzedek New Leadership Council. She may be reached at Jessica@garnerhealth.com.

ENDNOTES

1 Lewis Carroll, *Through the Looking Glass and What Alice Found There* at 16 (Macmillan 1871).

2 This is one example from the tenth revision of the International Statistical Classification of Diseases and Related Health Problems (also known as ICD-10). *See infra* n.9.

3 *See, e.g.*, Roy Smythe, *Applying Complexity Theory to Health Care Delivery Is Not Complicated*, FORBES MAGAZINE (Jan. 8, 2015), *available at* http://www.forbes.com/sites/roysmythe/2015/01/08/applying-aspects-of-complexity-theory-to-health-care-delivery-its-not-complicated/ ("[There is] no other 'system' that is more complex, or less predictable than health care.").

4 History, science and the arts provide the discerning individual with numerous examples of unwinnable scenarios: In Colonial America, an accused witch faced the "water test" to determine guilt or innocence. *See generally* Matthew Hopkins, The Discovery of Witches (1647). After landing in a body of water, if the individual could float, the town concluded the now-proven witch forwent baptism after contracting with the devil. If she could not float, however, her innocence was celebrated post mortem. *Id.* "Morton's fork" (a term originating with John Morton, Archbishop of Canterbury, in the late 15th century) refers to contradictory arguments leading to the same unpleasant result. *See, e.g., United States v. Winters*, 782 F.3d 289, 299 n.5 (6th Cir. 2015). One such example is the Scylla and Charybdis, both unpleasant results when traveling by water between mainland Italy and Sicily *circa* 800 B.C.E. *See, e.g.*, Homer, The Odyssey at Book 12 (Robert Fagles trans., Penguin Books 1996) ("Deadly Charybdis – can't I possibly cut and run from her and still fight Scylla off when Scylla strikes my men?"). Even Star Trek's "Kobayashi Maru" provides a modern twist to this time-tested dilemma. *See*, Janet D. Stemwedel, *The Philosophy of Star Trek: The Kobayashi Maru, No-Win Scenarios, And Ethical Leadership*, Forbes Magazine (Aug. 23, 2015), available at http://www.forbes.com/sites/janetstemwedel/2015/08/23/the-philosophy-of-star-trek-the-kobayashi-maru-no-win-scenarios-and-ethical-leadership/. And of course there is Zugzwang, that moment in chess when the next move will unavoidably make things worse. *Lasker's* Chess Magazine, at 105 (Feb. 1905).

5 In addition to physicians, "[t]he term 'health care provider' includes a hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, health care clinic, community mental health center ... renal dialysis facility, blood center, ambulatory surgical center ... emergency medical services provider, federally qualified health center, group practice, a pharmacist, a pharmacy, a laboratory ... a provider operated by, or under contract with, the Indian Health Service or by an Indian tribe ... a rural health clinic ... a therapist ... and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the [HHS Secretary]." 42 U.S.C. § 300jj(3).

6 *See, e.g.*, William M. Thackeray, *Vanity Fair: A Novel Without a Hero*, Ch. 8 (Punch Magazine 1847-48).

7 *See* 79 Fed. Reg. 67548, 67763 (Nov. 13, 2014).

8 79 Fed. Reg. 40318, 40325 (July 11, 2014).

9 *See generally* 74 Fed. Reg. 3328 (Jan. 16, 2009) (to be codified at 45 C.F.R. pt. 162). ICD-10 applies for reimbursement claims with a date of service on or after October 1, 2015. *See id.*

10 *See* M.F. Furukawa, J. King, J., V. Patel, C.J. Hsiao, J. Adler-Milstein and A.K. Jha, *Despite Substantial Progress in EHR Adoption, Health Information Exchange and Patient Engagement Remain Low in Office Settings*, Health Affairs, 33 (9), 1672-79 (2014).

11 Congress passed and President Clinton signed into a law the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in August 1996. Pub. L. 104-191, 110 Stat. 1936. Part of a broader effort under the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act (enacted under Title XIII of the 2009 American Recovery and Reinvestment Act, *see* Pub. L. 111-5), Congress established incentive payments to eligible professionals (EPs) and eligible hospitals, among other entities, to promote the meaningful use of interoperable health information technology and qualified electronic health records (EHRs). *See, e.g.*, 80 Fed. Reg. 16732, 16767 (Mar. 30, 2015) (to be codified at 42 C.F.R. pt. 495); Cal. Welf. & Inst. Code § 14046 ("[The Medi-Cal Program] shall establish and administer the Medi-Cal Electronic Health Records Incentive Program for the purposes of providing federal incentive payments to Medi-Cal providers for the implementation and use of electronic health records systems."). The term "qualified electronic health record means an electronic record of health-related information on an individual that—[¶] (A) includes patient demographic and clinical health information, such as medical history and problem lists; and [¶] (B) has the capacity—
(i) to provide clinical decision support;
(ii) to support physician order entry;
(iii) to capture and query information relevant to health care quality; and
(iv) to exchange electronic health information with, and integrate such information from other sources." 42 U.S.C. § 300jj (13).

12 Exec. Order No. 13335, 69 Fed. Reg. 24059 (Apr. 27, 2004).

13 *See* Michael J. Daray, Esq., *Negotiating Electronic Health Record Technology Agreements*, 22 No. 2 Health Lawyer 53 (Dec. 2009). By 2009, an estimated 30 to 70% of EHR deployments failed. *Id.*

14 *See* 80 Fed. Reg. 62762, 62765 (Oct. 16, 2015) (final rule) ("The Stage 1 final rule established the foundation for the Medicare and Medicaid EHR Incentive Programs by establishing requirements for the electronic capture of clinical data, including providing patients with electronic copies of their health information. [¶] [Stage 2] focused on the . . . exchange of essential health data among health care providers and patients to improve care coordination [and] finalized a set of clinical quality measures (CQMs) that all providers participating in any stage of the program" must report to CMS. Stage 3 built on the groundwork of both earlier stages, and "focuses on the advanced use of EHR technology to promote improved patient outcomes and health information exchange." *See also* 80 Fed. Reg. 20346 (Apr. 15, 2015) (proposed rule).

15 *See* 80 Fed. Reg. 62602, 62603-62604 (Oct. 16, 2016) (final rule) (making the ONC Health IT Certification Program more accessible to other types of health IT and not just EHR, including the technology of health information service providers and health information exchanges so that they can "receive appropriate attribution and not be referenced by a certificate with 'EHR' included in it").

16 *Medicare Access and CHIP Reauthorization Act of 2015*, Pub. L. 114-10, amending 42 U.S.C. § 1395w-4(o)(2).

17 Office of the National Coordinator for Health Information Technology Federal Health IT Strategic Plan (2015-2020) at p. 5 (2015).

18 *Id.* at p. 9.

19 *See, e.g.*, Jeffrey A. Singer, ObamaCare's Electronic-Records Debacle, Wall Street Journal (Feb. 17, 2015), available at http://www.wsj.com/articles/jeffrey-a-singer-obamacares-electronic-records-debacle-1424133213; Catherine M. DesRoches, Dr.P.H., Eric G. Campbell, Ph.D, et al., *Electronic Health Records in Ambulatory Care – a National Survey of Physicians*, 359 N. Engl. J. Med. 50 (July 3, 2008).

20 *See* 42 C.F.R. § 1001 (promulgating regulations to create an "Electronic Health Records Safe Harbor" under the Anti-Kickback Statute).

21 *See, e.g.*, Sharona Hoffman and Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 Berkeley Tech. L. J. 1523 (Fall 2009).

22 *See, e.g., E.L. White, Inc. v. City of Huntington Beach*, 21 Cal. 3d 497, 510 (1978) (noting that indemnity has been defined as "the obligation resting on one party to make good a loss or damage another has incurred.").

23 *See, e.g.*, Cal. Civ. Code § 1605 (good consideration defined).

24 *See, e.g.*, Cal. Civ. Code § 3529 ("That which ought to have been done is to be regarded as done, in favor of him to whom, and against him from whom, performance is due.").

25 *See* Cal. Civ. Code § 2860.

26 *See, e.g., Myers Bldg. Indus., Ltd. v. Interface Tech., Inc.*, 13 Cal. App. 4th 949, 968 (1993) ("An indemnity agreement is to be interpreted according to the language and contents of the contract as well as the intention of the parties as indicated by the contract.").

27 *But see Miller v. Ellis*, 103 Cal. App. 4th 373, 380 (2002) (holding equitable indemnification is not automatically available, but rather at times is a decision for the court to make).

28 For the rules of interpretation of a contract of indemnity, *see* Cal. Civ. Code § 2778.

29 *See, e.g., Rooz v. Kimmel*, 55 Cal. App. 4th 573, 583 (1997). "When the parties knowingly bargain for the protection at issue, the protection should be afforded." Id. at 583 (quoting *Rossmoor Sanitation, Inc. v. Pylon, Inc.*, 13 Cal. 3d 622, 633 (1975)).

30 *See, e.g.*, Cal. Com. Code § 2312. The taxing authorities, at least, understand this tenet. *See* Cal. Rev. & Tax Code § 6011(c)(10)(D).

31 *See e.g., Lim v. The TV Corp. Int'l*, 99 Cal. App. 4th 684 691 (2002).

32 *See generally Lugosi v. Universal Pictures*, 25 Cal. 3d 813 (2007) (lawsuit by the widow of Bela Lugosi claiming violation of her intellectual property right to the Dracula character).

33 *See e.g., Rossmoor Sanitation, Inc. v. Pylon, Inc.*, 13 Cal. 3d 622, 628 (1975). Insurance, too, is also useful should licensing issues arise, although contractual indemnity claims prevail over "theoretical noncontractual rights of indemnification between insureds." *Id.* at 634.

34 *See e.g., Buss v. Superior Ct.*, 16 Cal. 4th 35, 45-46 (1997) (The insurer's duty to indemnify runs to claims that are actually covered, in light of the facts proved ... By definition, it entails the payment of money in order to resolve liability.").

35 *See, e.g., Altavion, Inc. v. Konica Minolta Sys. Lab. Inc.*, 226 Cal. App. 4th 26, 37 (2014).

36 *Grail Semiconductor, Inc. v. Mitsubishi Electric & Electronics USA, Inc.*, 225 Cal. App. 4th 786, 800 n.12 (2014).

37 *See, e.g., Pettus v. Cole*, 49 Cal. App. 4th 402, 426 (1996).

38 *See generally Sheppard v. Lightpost Museum Fund*, 146 Cal. App. 4th 315 (2006).

39 *See, e.g., Cassel v. Superior Ct.*, 51 Cal. 4th 113, 126-27 (2011).

40 *See, e.g., Sanchez v. County of San Bernardino*, 176 Cal. App. 4th 516. 525 (2009).

41 The importance of a business associate agreement should not be forgotten for "any health care provider who transmits any health information in electronic form in connection with a transaction." 45 C.F.R. § 164.104. The logistical requirements, however, are not always simple and can involve a multitude of variables, all of which create challenges on their own. *See* 45 C.F.R. § 164.530.

42 "It is a widely accepted myth that medicine requires complex, highly specialized information technology (IT) systems. This myth continues to justify soaring IT costs, burdensome physician workloads, and stagnation in innovation – while doctors become increasingly bound to documentation and communication products that are functionally decades behind those they use in their 'civilian' life." Kenneth D. Mandl, M.D., M.P.H., and Isaac S. Kohane, M.D., Ph.D., *Escaping the EHR Trap – The Future of Health IT*, 366:24 N. ENG. J. MED. 2240 (June 14, 2012).

43 *See, e.g.*, Nicole Fisher, *Electronic Health Records – Expensive, Disruptive and Here to Stay*, Forbes (Mar. 18, 2014), available at http://www.forbes.com/sites/nicolefisher/2014/03/18/electronic-health-records-expensive-disruptive-and-here-to-stay/.

44 *Id.; see also* Mark W. Friedberg, Peggy G. Chan, et al., *Factors Affecting Physician Professional Satisfaction and Their Implications for Patient Care, Health Systems, and Health Policy* at p. xvi (2013 Rand Corporation, sponsored by the American Medical Association), *available at* http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR439/RAND_RR439.pdf:

> "EHRs had important effects on physician professional satisfaction, both positive and negative. In the practices we studied, physicians approved of EHRs in concept, describing better ability to remotely access patient information and improvements in quality of care. Physicians, practice leaders, and other staff also noted the potential of EHRs to further improve both patient care and professional satisfaction in the future, as EHR technology—especially user interfaces and health information exchange—improves. However, for many physicians, the current state of EHR technology significantly worsened professional satisfaction in multiple ways. Poor EHR usability, time-consuming data entry, interference with face-to-face patient care, inefficient and less fulfilling work content, inability to exchange health information between EHR products, and degradation of clinical documentation were prominent sources of professional dissatisfaction. Some of these problems were more prominent among senior physicians and those lacking scribes, transcriptionists, and other staff to support data entry or manage information flow. Physicians across the full range of specialties and practice models described other problems, including but not limited to frustrations with receiving template-generated notes (i.e., degradation of clinical documentation). In addition, EHRs have been more expensive than anticipated for some practices, threatening practice financial sustainability."

45 *See, e.g., "Cloud Computing: An Overview"* Standard Medicine Information Resources & Technology, *available at* https://med.stanford.edu/irt/security/cloud.html ("Before cloud storage existed, in order to provide storage to users an organization would need to: purchase the storage; create a data center where the storage would reside; run servers that would utilize the storage; and employ server administrators, storage experts and data center operators. Today, an organization or even an individual can have the equivalent of a data center's infrastructure, just by using a cloud-based service. It can potentially save thousands of dollars and man-hours, and might even be completely free while being available 24/7. But there are security issues that must be addressed before these services can be verified as truly secure, including data ownership, data separation, data protection, and backup.").

46 *See, e.g.*, Robert McMillan, *Cloud-Computing Kingpins Slow to Adapt to Own Movement*, Wall St. J. (Aug. 4, 2015), available at http://www.wsj.com/articles/cloud-computing-kingpins-slow-to-adapt-to-own-movement-1438731775 ("This market, combined with some other cloud services, has grown from $10.5 billion in 2013 to $19.9 billion this year. . . . It is projected to be worth $26.5 billion in 2016.").

47 *See, e.g.*, Dan Munro, *Healthcare Moves To The Cloud But Is The Cloud Ready For Healthcare?*, Forbes (July 6, 2015), available at http://www.forbes.com/sites/danmunro/2015/07/06/healthcare-moves-to-the-cloud-but-is-the-cloud-ready-for-healthcare/.

48 *See, e.g., Mega RV Corp.* v. HWH Corp., 225 Cal. App. 4th 1318, 1334-35 (2014).

49 *See, e.g.*, Cal. Com. Code § 2314 (implied warranty; merchantability; usage of trade); Cal. Com. Code § 2315 (implied warranty; fitness for a particular purpose).

50 *See, e.g.*, Cal. Com. Code § 2313 (express warranties by affirmation, promise, description, sample).

51 *See, e.g.*, Cal. Com. Code § 2316 (exclusion or modification of warranties); *Delta Air Lines, Inc. v. Douglas Aircraft Co.*, 238 Cal. App. 2d 95, 101 (1965) ("The statutory implied warranties of quality can, of course, be disclaimed by the seller, provided the buyer has knowledge or is chargeable with notice
of the disclaimer before the bargain is complete."). *But see generally International Knights of Wine, Inc. v. Ball Corp.*, 110 Cal. App. 3d 1001 (1980) (claims for fraud, negligent misrepresentation or strict liability may still exist after a disclaimed warranty).

52 *See, e.g., In re Sony Grand Wega KDF-E A10/A20 Series Real Projection HDTV Television Litigation*, 758 F. Supp. 2d 1077, 1090 (U.S.D.C. S.D. Cal. 2010).

53 *See supra* n. 50.

54 *See, e.g., Amtower v. Photon Dynamics, Inc*., 158 Cal. App. 4th 1582, 1609 (2008) ("The purpose of an integration clause is to preclude the introduction of evidence which varies or contradicts the terms of the written instruments. [citations omitted] It does not function to meld the documents it mentions."); *cf. infra* n. 59.

55 *See* 45 C.F.R. § 170.314 (certification criteria for Complete EHRs or EHR Modules effective January 14, 2016).

56 *See id*.

57 This can be done by accessing the following website maintained by the Office of the National Coordinator for Health Information Technology: http://oncchpl.force.com/ehrcert. For more information about the Office of the National Coordinator for Health Information Technology, see 42 U.S.C.A. § 300jj-11.

58 *See, e.g., In re Manville Forest Products Corp*., 209 F.3d 125, 129 (2nd Cir. 2000).

59 Cal. Civ. Proc. Code § 1856(a).

60 *See, e.g*., Cal. Civ. Code § 2176.

61 *See, e.g., McCarn v. Pacific Bell Directory*, 3 Cal. App. 4th 173, 181-82 (1992).

62 *See* Cal. Com. Code § 2715. Developers may also try to exclude "lost data" from damages, *see, e.g., Ward General Ins. Services, Inc. v. Employers Fire Ins. Co*., 114 Cal. App. 4th 548, 559 (2003), although such a provision could subject a provider to different kinds of liability. *See, e.g., Robert F. Kennedy Med. Ctr. v. Belshe*, 13 Cal. 4th 748, 751-52 (1996).

63 *See, e.g*., 22 C.C.R. § 72534.

64 45 C.F.R. § 164.504(e)(2)(ii)(J); *see also* 42 C.F.R. 164.502(a)(3): ("Business associates: Permitted uses and disclosures. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.").

65 Exec. Order No. 13181, 65 Fed. Reg. 81321 (Dec. 20, 2000), § 2, Pt. (b).

66 45 C.F.R. § 170.314(b)(7).

67 *See supra* n. 64.

68 *See* 45 C.F.R. § 170.205 (effective through and including Jan. 13, 2016 as well as on and after Jan. 14, 2016).

69 *See* 45 C.F.R. § 170.205 (effective Jan. 14, 2016).

70 As part of CMS' conditions of participation for hospitals, the medical records for each inpatient and outpatient must be "accurately written, promptly completely, properly filed *and retained, and accessible*." 42 C.F.R. § 482.24(b) (emphasis added); *see also* Cal. Health & Safety Code § 1250.05(d)("All general acute care hospitals ... shall develop and implement policies and procedures to ensure that relevant portions of patient's medical records can be made available within a reasonable period of time ...").

71 Historically the focus of courts in part was determination of constructive possession or actual control. *See, e.g., Ashton v. Burke*, 83 B.R. 716, 724 (D.N.D. 1988).

72 In 2006 certain physicians using Dr. Notes' electronic medical records software claimed outright denial of access to the program and their patient records unless they paid increased technical support fees. *See* Brian Bendell, *Multiple doctors cut off from records by Dr. Notes*, S. Fla. Bus. J. (July 3, 2006), *available at* http://www.bizjournals.com/southflorida/stories/2006/07/03/story8.html; *see also* Christopher Rowland, *Billing dispute leads to blocked patient data in Maine*, Boston Globe (Sept. 24, 2014), *available at* https://www.bostonglobe.com/news/nation/2014/09/21/electronic-health-records-vendor-compugroup-blocks-maine-practice-from-accessing-patient-data/6ILpMv78NARDsrdU5O0T9N/story.html.

73 *See* 42 C.F.R. § 164.504(e)(2)(ii)(J) ("At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form…."); *but see Medassets Net Revenue Systems, LLC v. Downey Regional Medical Center*, 2014 WL 1607633, *13 (C.D. Cal. 2014) ("But HIPPA [sic] does not create an independent duty. Rather, § 164.504(e) sets forth assurances that covered entities must include in a written contract.").

74 *See, e.g*., Thomas J. Stipanowich, *Arbitration and Choice: Taking Charge of the "New Litigation"*, 7 Depaul Bus. & Com. L.J. 383 (Spring 2009).

75 *See, e.g*., Steven L. Schooner, *Fear of Oversight: The Fundamental Failure of Businesslike Government*, 50 Am. U. L. Rev. 627 (Feb. 2001).

76 *Id*.

77 *See* Cal. Civ. Proc. Code § 1281 (validity of enforcement of arbitration provisions); Cal. Civ. Proc. Code § 1141.11(a) ("[A]ll nonexempt unlimited civil cases shall be submitted to arbitration under this chapter if the amount in controversy, in the opinion of the court, will not exceed fifty thousand dollars ($50,000) for each plaintiff"); *but see* Cal. Civ. Proc. Code § 1775.4 (the court cannot force parties into mediation where the action was ordered into arbitration pursuant to Section 1141.11(a), nor can a mediation pursuant to Section 1775.3 be forced into arbitration).

78 *See, e.g., Lappe v. Superior Ct*., 232 Cal. App. 4th 774, 783 (2014) (discussing the broad mediation privilege in California). Such an expansive mechanism for confidentiality exists in stark contrast to the challenges of keeping records confidential in court. *See, e.g., Huffy Corp. v. Superior Ct*., 112 Cal. App. 4th 97, 106 (2003) (court disregarded an agreement not to disclose for failure to show prejudice). This also applies to divorce proceedings. *Burkle v. Burkle*, 135 Cal. App. 4th 1045, 1070 (2006).

79 S.B. 945, 2011 Cal. Legis. Serv. Ch. 433 (Oct. 2, 2011) (repealing parts of the Cal. Welfare and Institutions Code, including Section 14046).

80 *Id*. These funds are made available through the *American Recovery and Reinvestment Act of 2009*, § 4201 (Pub. L. 111-5).

81 *Cf*. Beverly Cohen, *The Controversy Over Hospital Charges to the Uninsured – No Villains, No Heroes*, 51 Vill. L. Rev. 95, 146 n. 316 (2006).

82 *See generally* U.S. Office of Inspector Gen., OEI-01-11-00571, *CMS and Its Contractors Have Adopted Few Program Integrity Practices to Address Vulnerabilities in EHRs* (Jan. 2014), *available at* http://oig.hhs.gov/oei/reports/oei-01-11-00571.pdf.

83 *Id*. at 1. Two examples noted by the OIG include federal guidance on electronic signatures in EHRs and audit logs to authenticate the medical records supporting a claim. *Id*. at p 13.

84 HHS has designated the OCR as the primary agency to enforce the HIPAA Privacy Rule. *See, e.g., Protection & Advocacy System, Inc. v. Freudenthal*, 412 F. Supp. 2d 1211, 1217 (D. Wyo. 2006). OCR oversees complaints relating to HIPAA, and more specifically those 109,722 HIPAA-related complaints registered between April 2003 and February 1, 2015. Of these potential HIPAA infractions, approximately 70% did not fall within OCR jurisdiction or the OCR determined no violation had occurred. But in some 40,000 cases investigated by the OCR, 30% found no violation, while 70% required some corrective action, usually in reference to impermissible uses and disclosures of PHI, failure to keep PHI safe, lack of patient access to PHI, or disclosure of more information than was reasonably necessary. Private practices and acute care hospitals were among the worst offenders. *See generally* Craig B. Garner, *HIPAA — Society's Modern Day Prohibition* (Ca. Healthcare News, May 2015), *available at* http://www.cahcnews.com/newsletters/ca-cgarner-0615.pdf.

85 *See generally* Office of Inspector Gen., OEI-09-10-00510, *OCR Should Strengthen Its Oversight of Covered Entities' Compliance with the HIPAA Privacy Standards* at 11-12 (Sept. 2015) (recommending that OCR (1) strengthen its oversight of covered entities compliance with the Privacy Rule; (2) improve its investigation process; (3) fully implement a permanent audit program; (4) carefully track corrective action; (5) identify previous investigations against providers; and (6) continue to educate covered entities about OCR and the privacy standards.

86 Office of Inspector Gen., OEI-09-10-00511, *OCR Should Strengthen its Followup of Breaches of Patient Health Information Reported by Covered Entities* at 13-14 (Sept. 2015) (recommending that OCR (1) maintain information regarding small breaches in a searchable format; (2) maintain complete documentation of corrective actions; (3) expand outreach and education efforts; and (4) check for prior breaches by covered entity).

87 For purposes of HIPAA, of concern are data breaches where information is not just lost but also used or abused. *See, e.g., In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*, 45 F. Supp. 3d 14, 20 (D.D.C. 2014). The idea of a data breach, however, is not always objective. For example, identify theft is "the unauthorized use of another person's personal identifying information to obtain credit, goods, services, money, or property." See Cal. Civ. Code § 1798.92(b). PHI is individually identifiable health information maintained by a covered entity, such as a hospital. *See* 45 C.F.R. § 160.103. The perpetrator of identity theft can also be the "owner" of PHI, even if admitted to a hospital under the name of the victim. The perpetrator should not be confused, however, with the victim of identity theft, or "a person who had his or her personal identifying information used without authorization by another to obtain credit, goods, services, money, or property, and did not use or possess the credit, goods, services, money, or property obtained by the identity theft, and filed a police report in this regard pursuant to Section 530.5 of the Penal Code." Cal. Civ. Code § 1798.92(d).

88 For a list of all federal civil money penalties, *see* 45 C.F.R. § 160.404. For additional information about California penalties, *see generally* Cal. Civ. Code § 56.101; *but see Sutter Health v. Superior Court*, 227 Cal. App. 4th 1546, 1564 (holding that the loss of an unencrypted computer alone was "not a breach of confidentiality" when a thief stole an unencrypted desktop computer from Sutter Health containing the personal information of over 4 million patients).

89 "Reasonable diligence refers to the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances." 45 C.F.R. § 160.401.

90 "Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect." *Id*.

91 "Willful neglect refers to conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated" *Id*.

92 45 C.F.R. § 164.308(a)(6); 45 C.F.R. § 164.530(f).

93 42 U.S.C. § 17932(a). If only a handful of individuals are affected, notice should be mailed or another type of comparable communication made. 45 C.F.R. § 164.404. If a breach involves more than 500 individuals, notification must be made through the media outlets in the area, *see* 45 C.F.R. 164.406(a), as well as to the Secretary for HHS. 45 C.F.R. § 164.408.

94 Cal. Health & Safety Code § 1280.15(b).

95 *See, e.g.*, Roger Hsieh, *Improving HIPAA Enforcement and Protecting Patient Privacy in a Digital Healthcare Environment*, 46 Loy. U. Chi. L.J. 175 (Fall 2014).

96 *See supra* n. 86; *see also* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html.

97 *See* Erin McCann, *HIPAA data breaches climb 138 percent*, Healthcare IT News (Feb. 6, 2014), *available at* http://www.healthcareitnews.com/news/hipaa-data-breaches-climb-138-percent.

98 *See, e.g.*, 15 C.C.R. § 3361(c) ("Recognizing that mental health care often involves revealing deeply personal and private matters, all mental health care shall be provided in such a manner as to maintain the dignity of the inmate. Professional relationships shall be conducted with proper privacy, with due regard to the professional to take necessary and appropriate action to prevent harm to the patient or to others.").

99 *See* 45 C.F.R. § 160.103 ("Protected health information means individually identifiable health information: (1) Exempt as provided in paragraph (2) of this definition [educational records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232.g], that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium."). In matters of health care records, however, not all records, nor data breaches, are created equal. *But see* 15 C.C.R. § 3361(c)("Recognizing that mental health care often involves revealing deeply personal and private matters, all mental health care shall be provided in such a manner as to maintain the dignity of the inmate. Professional relationships shall be conducted with proper privacy, with due regard to the professional to take necessary and appropriate action to prevent harm to the patient or to others.").

100 *See* 42 U.S.C. §§ 1320-d(5)(a)(1) through 1320-d(6)(a)(2); *Diment v. Cushing*, 2007 WL 2344981, *2 (D.C.W.D. Va. 2007) ("HIPAA imposes civil and criminal penalties on a person who knowingly and illegally obtains or discloses 'individually identifiable health information' from or to another person.").

101 *See, e.g.*, 42 C.F.R. § 495.104 (incentive payments to eligible hospitals); 42 C.F.R. § 496.102 (incentive payments to eligible professionals).

102 *See, e.g.*, 45 C.F.R. § 164.502; *Through the Looking Glass, supra*, n. 3 at 223 ("'It's too late to correct it,' said the Red Queen: 'when you've once said a thing, that fixes it, and you must take the consequences.'").