Medicaid block grants and/or per capita caps will likely be strongly opposed by Democrats and many current Medicaid stakeholders. Details regarding any proposal may expose new fault lines that may or may not track party lines.

Medicaid Waivers
With or without an expansion repeal, the new administration may take a more liberal view than CMS has to date in approving “premium support” or “private option” expansion coverage through Section 1115 Medicaid waivers, including the approval of beneficiary work requirements and premiums. Republican Governors in Michigan and Arizona have been highly supportive of continuing waiver-based expansion programs. Thus far, CMS has declined to approve mandatory job or work training program components of such waivers, rejecting such proposals from Pennsylvania, Arizona, and Michigan. CMS also has rejected waiver requests to require partial premiums for enrollees with incomes falling at or below 100% of the federal poverty level. The next Secretary would have broad discretion to allow for such requirements under new or renewed expansion waivers, an area in which the CMS Administrator designate is well versed.

Medicaid Supplemental Payment Issues and Managed Care
Medicaid supplemental payments—i.e. payments above Medicaid base rates—comprise a significant portion of Medicaid expenditures. They include Medicaid disproportionate share hospital (DSH) payments, Upper Payment Limit (UPL) payments, and payments made through Section 1115 waivers through a Safety Net Care Pool (SNCP), Low Income Pool (LIP), Uncompensated Care (UC) pool, or Delivery Systems Reform Incentive Payment (DSRIP) pool. Per the Medicaid and CHIP Payment and Access Commission 2015 Chart Book, supplemental payments were over $47 billion in federal fiscal year (FFY) 2014. There are many open questions regarding Medicaid supplemental payments for 2017:

DSH
Medicaid DSH payments, that reimburse hospitals for Medicaid shortfalls and uninsured costs, were scheduled for substantial cuts in the ACA. These DSH cuts, which Congress justified based on projected reductions of uninsured patients, presently are now scheduled for FFY 2018, and would be a significant issue for 2017 if implemented. If the ACA is repealed and/or amended, the impact on DSH cuts is a significant question.

Waiver Pools
Although CMS has permitted supplemental payment pools under waivers, CMS wrote to all states with uncompensated care pools in November 2015, emphasizing that coverage is the best way to secure access to health care and that UC pools are not an alternative to Medicaid expansion. Many states—including Florida and Texas—have waivers that include payment pools and are up for renewal in 2017. How the new CMS will treat these payment pools is an open question.

Medicaid Managed Care Pass-Throughs and Payment Reform
Medicaid managed care—under which benefits are administered by private Medicaid Managed Care Organizations (MCOs) that receive per member per month capitation fees and deliver services through a contracted provider network—already has eclipsed Medicaid FFS programs. Over 60% of all beneficiaries were enrolled in comprehensive Medicaid managed care programs as of 2013, and this trend is increasing. Many states have taken steps to adjust supplemental payments—previously the province of Medicaid FFS—to this new environment by channeling these funds to providers through MCOs. The comprehensive Medicaid Managed Care Final Rule published on May 6, 2016, provided explicit authority to states to require MCOs to make payments to certain providers to encourage value-based purchasing, delivery system reform, or to establish provider payment initiatives within the compass of “actuarially sound” rates. CMS also included a new transitional authority, temporarily permitting “pass-through payments” to hospitals, physicians, and nursing facilities. Under an Informational Bulletin issued on July 29, 2016, and a proposed regulation published on November 22, 2016, transitional MCO pass-throughs—which CMS permitted to avoid service disruptions and economic harm to safety-net providers, despite generally prohibiting such payments—would be limited by the aggregate amount of annual pass-throughs already in place as of July 5, 2016. CMS’ action on managed care supplemental payment issues could be a significant issue in 2017.

4. The Rise of Ransomware
—Jon Neiditz, Kilpatrick Townsend & Stockton LLP

Ransomware is the business model that has risen to dominance of the cybercriminal market. Among the reasons for its success are quick introduction and deployment without the development costs and need for sustained stealth of data exfiltration, and quick and direct payments not requiring complex internet networks for the purchase and sale of personal information. Ransomware attacks have quadrupled this year, averaging 4,000 per day, according to the Justice Department.19 The Federal Bureau of Investigation (FBI) noted ransomware costs organizations have been willing to disclose totaled $209 million in the first three months of 2016, compared to a total $24 million for all of 2015.20 A report released in August found that about 80 new ransomware “families”—an increase of 172%—were discovered in the first half of 2016.21

Beneath the numbers lies a sea change in the way the law will come to see information security incidents, because ransomware is a visible portent of other major threats to cybersecurity that involve controlling, damaging, and interrupting systems, denying access to data and destroying or otherwise harming the integrity of data without acquiring the data, rather than what we have come to know as “breach.”

The popular notion of a data breach today was forged by the California legislature in 2002, when the state became the only jurisdiction in the world to require notification to individuals about breaches of some types of their personal information.22 This innovative law attracted little national attention until
February 2005, when ChoicePoint announced that it suffered a breach affecting 30,000 Californians, and the world soon learned that the only reason Californians were so unlucky was that no other state required notification. Statutes modifying but fundamentally following the California model spread like wildfire across the country. Through their similarity and the similarity of the breaches they forced companies to disclose, those statutes reified—constructed and then petrified—what we think of today as a data breach. Generally, we think of a breach as unauthorized access to or acquisition of unencrypted personal information that compromises the security or privacy of that information. The Health Information Technology for Economic and Clinical Health (HITECH) Act incorporated that concept into the Health Insurance Portability and Accountability Act (HIPAA), and construing “compromise” led HHS over a long and winding road to its simple and elegant four-factor risk assessment.

The information security world, on the other hand, has always been more focused on a wider variety of incidents. Moreover, both security frameworks and standards such as National Institute of Standards and Technology and corporate security processes have evolved more rapidly than law; they have become adaptive programs responding to ever-changing risks and focused on detection and response as well as prevention.

Even though ransomware is the dominant current information security threat to health care providers, notification laws still focus on breach. In other words, until recently, state and federal breach notice requirements did not appear to apply to ransomware because the protected data is encrypted rather than accessed or taken, even though choosing a facility under a ransomware attack may entail much greater risks than the identity harms associated with a facility suffering data breach. For the unprepared health care provider not able to prevent ransomware or quickly contain it to prevent more harm, ransomware may interrupt cancer treatment, render the patient record unavailable, or result in other greater and immediate threats than identity theft.

Recognizing the threat, HHS put out an innovative and comprehensive “Fact Sheet” on “Ransomware and HIPAA,” which treats ransomware as a notice-triggering data breach by default, unless it is determined via the familiar four-part HIPAA breach risk assessment not to constitute or involve the familiar four-part which treats ransomware as a notice-triggering data breach. Like other guidance on ransomware available from the United States Computer Emergency Readiness Team (U.S.-CERT), the FBI, and the Federal Trade Commission (FTC), the Fact Sheet emphasizes key protections such as safe, segregated, and reliable backups and patching, monitoring, and training to avoid phishing, putting them in the context of HIPAA risk analysis. The Fact Sheet then shoehorns ransomware into HIPAA’s Breach Rule “because ePHI encrypted by the ransomware was acquired” in the absence of a determination through the usual four factors of a “low probability that the PHI has been compromised.”

Where the Fact Sheet most reveals that the old legal framework of breach notification is a Procrustean bed for emerging cybersecurity threats is in its response to how a ransomware attack on encrypted PHI triggers breach notification. Since the regulatory paradigm is breach, the Fact Sheet must make such an event notice-triggering only when the underlying data loses its encryption. From the standpoint of harm, of course, that is beside the point; the ransomware harms primarily by interfering with the availability of the information, not with its confidentiality, and the continued encryption of the information to HIPAA standards does not protect its availability.

The biggest emerging cybersecurity threats, like ransomware, are principally about the control of systems rather than breaches of personal information. The threats posed to cyber-physical systems in the Internet of Things—connected cars caused to crash, connected medical devices caused to malfunction, attacks by connected buildings—are a major area of risk of harm, and we now have an IoT botnet threatening the Internet through the Mirai DDoS attack. And beyond the IoT, of course, looms the specter of cyberwar. A robust regulatory regime focused on the diversity of harms that may be caused by security incidents would escape the paradigm of breach and view security harms more broadly. As talk of a uniform federal security breach response law bubbles up again with a new administration and Republican-controlled Congress, the question becomes whether an incident response law can be crafted based on the emerging risks of 2017 rather than those known in 2002.

5. Fraud and Abuse: Defying Gravity —Tony Maida, McDermott Will & Emery LLP

From the industry perspective, the fraud and abuse environment can seem controlled by a mysterious wizard ensconced in the Emerald City, far removed from the challenges of operating a health care business. This year was no exception. Let’s peek behind the curtain for 2017.

Post-Escobar Implied Certification. Much of the Supreme Court’s analysis in Universal Health Services, Inc. v. United States ex rel. Escobar emphasized the “demanding” nature of the implied certification’s materiality standard, which will be the subject of considerable litigation in the coming years. Scienter is another important implied certification issue, including whether the defendant knew compliance with the standard at issue was material to the government. Also, several courts have held that ambiguous regulations cannot state an implied certification claim if the defendant’s interpretation of the regulation was reasonable. Given the abundance of ambiguous regulations in the health care arena, this is a topic to watch.

60-Day Rule. It’s been almost a year since the birth of the Medicare Parts A and B overpayment rule (and over two years for Parts C and D) interpreting the ACA’s requirement to report and return overpayments within 60 days of identification. What triggers the rule’s requirement to conduct reasonable diligence and when the clock starts ticking are just two of a host of questions lawyers and their clients will continue to contend with in 2017. Perhaps the most important question—is there an overpayment—moves beyond a 60-Day Rule analysis to determining whether the Medicare requirement at issue is a condition of payment, participation, or something else. Despite the absence of clear answers, the government has been investigating allegations of 60-Day Rule violations under the reverse false claims principle.