EHRS

Former Dept. of Veterans Affairs Nurse Falsified Records

A former registered nurse at Veterans Affairs (VA) Medical Center in Miami will spend 60 months in prison after pleading guilty to altering and falsifying VA computer records.

The court record states that Enrique Martinez Mathews interfered with an internal investigation at the medical center related to the death of a veteran in Martinez's care. The investigation revealed that Martinez had altered the patient's records while the patient recovered in the surgical intensive care unit. Because of Martinez's actions, appropriate medical treatment was withheld from the patient, who later passed away. Martinez then altered more records to try to hide his prior actions.

Special Agent in Charge Monty Stokes said, "This investigation represents the VA OIG's commitment to investigate obstruction as well as alterations of medical records that needlessly compromise veterans' care and subject them to harm. We will continue to vigorously investigate employees whose actions corrupt the integrity of VA's healthcare records relied upon by VA clinicians who treat our nation's heroes."

E-DISCOVERY

Scheindlin to Step Down From U.S. District Bench

The author of the landmark *Zubulake* decision is retiring her gavel. U.S. District Court Judge Shira Scheindlin, for the Southern District of New York, who has presided over many high-profile cases and made groundbreaking e-discovery decisions, plans to leave the bench for private practice in New York City, *The New York Law Journal* has reported.

Scheindlin told her colleagues in a written letter that she also plans to spend time mentoring, lecturing, and working on alternative dispute resolution, including work as "an arbitrator and mediator and in other neutral capacities with the hope of doing a fair amount of public interest work, as well as working on commercial matters."

Scheindlin, 69, was appointed to the Southern District of New York by President Bill Clinton in 1994. Over the years, she made a name for herself as an expert on e-discovery in a series of opinions in *Zubulake v. UBS Warburg* starting in 2003.

Of course, that decision changed the way companies and lawyers approach electronically stored information. *Zubulake* put companies on notice that they have a duty to preserve data once they reasonably anticipate they might be sued, according to the *ABA Journal*. Similarly, lawyers can no longer simply initiate a hold; they now have an obligation – thanks to *Zubulake* – to oversee the compliance process. The sanctions for not doing so can be harsh and crippling.

According to the *ABA Journal, Zubulake* imposed a far-reaching duty to preserve on every business in the United States, as well as any company in the world that does business with the United States.

"Up until that opinion, the rules of the game for preserving docs were simple and clear. When the other side was interested in getting a document, they'd send over a request for it and, putting aside objections, that's when the duty attached. Scheindlin came along and said 'no more.' She changed the rule – and in doing so, she created an industry, as well as a drastic mess for corporate America," Catalyst CEO and former lawyer John Tredennick told the *ABA Journal*.

E-RECORDS

Report: E-Gov Exacerbates Records Challenges in Developing Nations

In its 2016 World Development Report, "Digital Dividends," the World Bank assesses the impact of digital technologies on countries' development and concludes that these technologies have been disappointing and unevenly distributed despite boosting growth, expanding opportunities, and improving service delivery. For digital technologies to benefit everyone everywhere, the report says countries need to strengthen regulations to ensure competition, adapt workers' skills to the demands of the new economy, and ensure that institutions are accountable.

The World Bank report draws on a number of background papers that are also provided to the public. In "One Step Forward, Two Steps Backward? Does EGovernment Make Governments in Developing Countries More Transparent and Accountable?," Victoria Lemieux, Ph.D., CISSP, discusses the unintended consequences and risks for transparency and accountability associated with the way digitally recorded information is produced and managed by the public sector in developing countries.

According to the paper, many countries are in the process of transitioning from primarily paper-based administrative systems to digital systems by implementing information and communication technology (ICTs) as part of their e-government initiatives. The presumption is that this transition should improve accountability and transparency by making information more readily accessible. Lemieux points out that the transition has not necessarily been a positive one.

"In many countries, the introduction of ICTs has brought about a deterioration in the quality, management, and accessibility of recorded information with concomitant negative impacts upon transparency and public accountability mechanisms, such as the operation of right to information (RTI) laws," the report states. The report presents a compelling argument that "e-government or the rising use of digital technologies for the creation, communication, and storage of information within public administrations has created new challenges that exacerbate previous weaknesses in recordkeeping systems constraining the availability and integrity of information for transparency and accountability."

In most developing countries, the report notes, legislative frameworks haven't been updated and are typically inadequate for addressing e-records and information management concerns. Given all the digital forms of information used today to conduct government business, and especially with the rise of e-government, the report says there is a clear and present need for public officials and information commissioners to have better guidance on how electronic data should be collected and managed under public records and RTI laws.

PRIVACY

B.C. Information and Privacy Commissioner to Step Down

British Columbia Information and Privacy Commissioner Elizabeth Denham has announced that she will step down when her term ends in July to become the United Kingdom's new information commissioner this summer. She has served for the past six years.

"I leave believing that the independence and impartiality of this Office has served the public well," she wrote in her resignation letter. "I also leave knowing that government's awareness of the importance of privacy and security of personal information, the need for good record keeping of government decisions and the public's right to know have been enhanced during my tenure."

Denham

Denham has been outspoken on privacy and access to information in the province. Most recently, according to *CBC News*, she wrote a scathing report about the provincial government's "triple-deleting" of e-mails in various ministries after whistleblower Tim Duncan alleged he was ordered to delete e-mails related to a freedom of information request.

She also has criticized what she called "oral government" within the provincial government, "where business is undertaken verbally and in a records-free way." She said this undermines the freedom of information system by leaving little or no record of government decision-making, *CBC News* reported.

PRIVACY

FCC Seeks Stricter Privacy Rules for ISPs

In March, the Federal Communications Commission (FCC) negotiated a deal with Verizon in which the company agreed to pay $1.35 million for using technology that enabled marketers to track its customers' online activity, *CNET* reported.

The FCC, according to *CNET*, wants to make sure that doesn't happen again, so it has proposed regulations meant to protect private consumer information by:

- Requiring Internet service providers (ISPs) to obtain customers' permission before sharing their data with third parties
- Preventing phone companies and cable operators from repurposing and reselling what they learn about consumers' phone or TV viewing activity to marketers

At its March 31 meeting, the FCC voted to open the proposal for public comment. Chairman Tom Wheeler said actual rules likely will be voted on later this year after the comment period ends.

If approved, the proposal would put in place the strongest set of privacy regulations ever established for ISPs, according to *CNET*. The proposed broadband and wireless rules to give consumers more control over their data are similar to those for cable TV and telephone services, which the FCC already regulates. The rules would:

- Require ISPs to clearly disclose how personal consumer data is collected, how it's shared with third parties, and how it's used by these outside firms
- Mandate that customers actively choose to participate in the program rather than be automatically enrolled
- Direct ISPs to strengthen security practices for customer data

According to *CNET*, the regulations would also set broadband and wireless providers apart from Internet and social media sites, including Google or Facebook, which also collect large amounts of consumer data that is used for marketing. But these companies follow different rules because they are monitored by the Federal Trade Commission (FTC), which has limited authority to create specific regulations. The FTC monitors only data collection practices in an attempt to prevent misuse or fraud.

Wheeler may be in for a fight from broadband and wireless industry leaders, who have noted the discrepancy. The lobby group National Cable & Telecommunications Association issued a statement saying it was "disappointed by Chairman Wheeler's apparent decision to propose prescriptive rules on ISPs that are at odds with the requirements imposed on other large online entities."

E-MAIL

IRS Begins Digitizing Records

After years of high-profile missteps and congressional scrutiny, top IRS officials recently told the House Oversight and Government Reform Committee that they are working toward improving their processes for retaining and accessing data.

"We're making significant progress," Ed Killen, director of privacy, governmental liaison, and disclosure at the IRS, told the committee.

FCW.com reported that the e-mail messages of senior IRS executives are being archived in electronically accessible formats in perpetuity, and the messages

of second-tier managers are being stored for 15 years. According to Killen, the IRS is aiming to archive all employees' e-mail electronically by the end of the year as part of a plan to move away from an antiquated approach consisting of printing and filing and using backup tapes.

Moving to an electronic archive will require moving e-mail servers into two main data centers, said IRS Chief Technology Officer Terry Milholland.

PRIVACY

California Judge Orders Release of 10 Million Student Records

A federal judge for the Eastern District of California has ordered the release of about 10 million California public school students' records – including each child's name, Social Security number, address, mental health assessment, medical history, and test scores.

In her ruling, Judge Kimberly Mueller granted a small, parent-run, non-profit group working for the rights of disabled children access to the sensitive information of each student in kindergarten through 12th grade who has attended public school in California since Jan. 1, 2008. The records must be made available to a court-appointed data analyst so they can be analyzed on behalf of the Morgan Hill Unified School District parent group, according to *USA Today*.

The parent group is suing the California State Department of Education because it does not believe the state requires school districts to provide appropriate special education services for children needing them, as mandated under federal law. The California Concerned Parents Association, which advocates for students with disabilities statewide, joined Morgan Hill's lawsuit. The state vehemently denies the allegations and is defending itself against the lawsuit, a spokesman told *USA Today*.

The Concerned Parents group requested statewide data to prove its case that students with special needs are not being given adequate attention. But the parent groups said they never asked for, nor do they want, students' personally identifiable information.

"We asked repeatedly, many times, for the data without identifiable information," the group's president, Linda McNulty, told the *San Jose Mercury Sun*. She said the state education department refused.

The state said it's just following the judge's orders.

"The California Department of Education has been fighting vigorously to defend the privacy rights of students throughout California, but we are required to comply with the court order in this case," department spokesman Peter Tira responded.

The *Mercury Sun* said it was not clear why Social Security numbers and other sensitive information couldn't be redacted.

The court order allowed parents who wish to opt-out of the release of their child's information to do so by filling out an exemption form.

After any exemptions are received, the state will turn over the entire database of student data to the plaintiff's attorneys. According to the *Mercury Sun*, the court order allows fewer than 10 people to access the student data, and their review will be closely overseen by a court-ordered special master in electronic discovery.

According to *USA Today*, the attorneys reviewing the records are required by a protective order to keep the data private and confidential. Once the group completes its statistical analysis, it is required to "either return or destroy the confidential data at the conclusion of the lawsuit. No student's identifying records will be disclosed to the public," the parent group said.

CLOUD

Use of Cloud Apps Rose 50% in 2015

The average number of cloud apps a global business uses rose almost 50% to 917 applications, increasing 21% alone between October 2015 and the end of the year, according to Netskope's "Cloud Report."

The majority of those apps are well known, and the top 20 include Outlook, Lync, OneDrive for Business, LinkedIn, Facebook, Twitter, and YouTube.

FOIA

Obama Administration Sets FOIA Records

U.S. federal government searchers said they could not find a single page of information in response to nearly 130,000 Freedom of Information Act requests for information (about 17%) in the 2015 fiscal year – a record number, according to a new Associated Press (AP) analysis of government data.

The AP's annual review covered all requests to 100 federal agencies during fiscal 2015. In 39% of cases – or 5,168 times – the Federal Bureau of Investigation couldn't find any records. The Environmental Protection Agency regional office that oversees New York and New Jersey came up empty handed 58% of the time, and U.S. Customs and Border Protection couldn't find anything in 34% of cases.

The review had no way to determine whether more requests last year involved non-existent files or whether searches for records were not thorough enough. The Obama administration told the AP that it completed a record 769,903 requests, a 19% increase over the previous year, despite hiring only 283 new full-time workers for the issue, an increase of about 7%. The number of times the government said it couldn't find records increased 35% over the same period.

The AP noted that in some high-profile cases involving federal lawsuits, the Obama administration found tens of thousands of pages after it previously said it couldn't find any. The website Gawker sued the State Department last year after it said it couldn't find any e-mails that Philippe Reines, an aide to Hillary Clinton and former deputy assistant secretary of state, had sent to journalists. After the lawsuit, the agency said it found 90,000 documents about correspondence between Reines and reporters.

When the government says it can't find records, it rarely provides detailed descriptions about how it searched for them, the AP said. Under the law, federal employees are required to make a reasonable search, and a 1991 U.S. circuit court ruling found that a worker's explanation about how he conducted a search is "accorded a presumption of good faith, which cannot be rebutted by purely speculative claims" that a better search might have turned up files.

Overall, the AP found that the government censored materials it turned over or fully denied access to them in a record 596,095 cases, or 77% of all requests. That includes 250,024 times when it said it couldn't find records, a person refused to pay for copies, or the government determined the request to be unreasonable or improper. The White House routinely excludes those cases from its own assessment. Under that calculation, the administration said it released all or parts of records in 93% of requests.

E-DISCOVERY

UK Court Approves Technology-Assisted Review

In 2012, the *Da Silva Moore v. Publicis Group* ruling allowed for technology-assisted review (TAR) and changed the face of discovery in the United States by not requiring litigants to look at every single document. Three years later, a judge in Ireland ruled in favor of predictive coding in *Irish Bank Resolution Corporation Limited & Ors v. Sean Quinn & Ors.*

Now, the world's second-largest discovery market – the UK – has taken a seat at the TAR table. In the case *Pyrrho Investments and MWB Business Exchange v. MWB Property and others,* Master Matthews of English High Court allowed the parties to use predictive coding, marking TAR's first use in UK courts.

In his precedent-setting decision, Matthews cited 10 factors that led him to favor approving predictive coding in the case, including:

- "[t]here is no evidence to show that the use of predictive coding software leads to less accurate evidence than, say, manual review alone"
- "there will be greater consistency in using the computer to apply the approach of a senior lawyer towards the initial sample (as refined) to the whole document set, than in using dozens, perhaps hundreds, of lower-grade fee earners..."

According to *Legaltech News*, proportionality also influenced Matthews' decision. He wrote, "The cost of manually searching these documents would be enormous, amounting to several million pounds at least. In my judgment, therefore, a full manual review of each document would be 'unreasonable'..."

Counsel in the case estimated that the cost of TAR would be much lower, between £181,000 and £469,000 pounds, plus hosting fees.

E-RECORDS STORAGE

Sony Says System Supports 100-Year Data Storage

Sony has unveiled technology it says will keep data safe and sound for up to a century. The scalable, jukebox-like optical library system from Sony Optical Archive Inc., is called Everspan.

It is designed to store, retrieve, and read discs that will hold 300GB, with 150GB on each side. Capacity is expected to grow to 1TB over the next five years, IDG News Service reported.

Everspan will start shipping to customers in July.

Long-term storage promises are not new, though, and they fail to address key factors in long-term data preservation. For starters:

- **Ability to *read* the data:** The hardware and software needed to retrieve the data from any media are more critical than the longevity of the media it's stored on.
- **Technology advances/value of information remains:** With each technology improvement, legacy data gets harder to retrieve and read. Sometimes data can't even be migrated to a new application or system, and vendors drop support for older software and hardware.
- **Need for long-term planning:** To ensure that the information can be retrieved from any media requires long-term planning. The records and information management department must collaborate with the IT department to ensure that conversion and migrations plans coincide with hardware upgrade plans, and management must allocate sufficient resources for data conversion and migration.

Still, the digital storage devices market looks to be a lucrative global business – worth $5.4 billion [£3.75 billion] by 2020, according to a recent Kroll Ontrack article.

E-DISCOVERY

Whistleblower Says VW Deleted Data

According to a lawsuit filed by a former employee, Volkswagen workers illegally deleted electronic data soon after the U.S. government accused the carmaker in September 2015 of cheating on emissions tests.

The lawsuit filed in Michigan accuses Volkswagen of violating the state's whistle-blower protection act in the wrongful dismissal of information manager Daniel Donovan in December. Donovan says he was fired because his superiors believed he planned to report the company to U.S. authorities for obstruction of justice, according to *The New York Times*.

Volkswagen of America said in a statement that the claim of wrongful dismissal was "without merit" and that the dismissal was unrelated to the emissions issue.

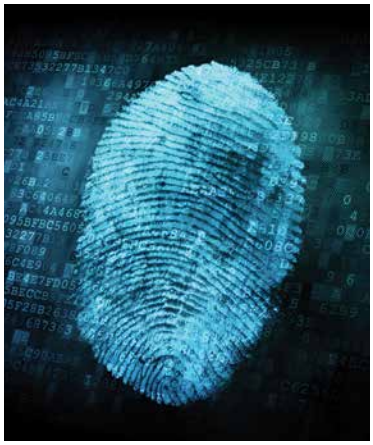
According to Donovan's lawsuit, his superiors told him on September 18 to instruct the chief information officer (CIO) at the company offices in Auburn Hills not to delete any electronic records and that the CIO replied to Donovan's telephone call demanding to know why a lower-ranking employee was giving him instruction.

The lawsuit claims that IT workers continued to delete electronic data until September 21 and that even after that date, employees destroyed backup data because they felt there was not enough storage space. Donovan said he told IT managers they could be accused of obstructing justice and told them he did not want to participate.

INFO SECURITY

Digital Forensics to Grow to $4.8 Billion by 2020

The business of obtaining, interpreting, and uncovering digital data from electronic devices is gaining momentum and won't slow anytime soon, according to a recent report from IndustryARC.



"Digital Forensics Market Analysis" says the digital forensics market is expected to grow at an annual compound rate of just over 14%, hitting $4.8 billion in revenue by 2020. The biggest reason for the growth is a heightened focus by companies and government on cybersecurity and data theft prevention, according to the report.

The exponential growth in the volume of data with the proliferation of a wide variety of mobile devices and formats has led to a rise in the use of digital forensics.

IndustryARC said most of the market growth will occur in the Americas and also found that:

- The digital forensics market in the Americas will hold around 60% share by 2020.
- In Europe, the use of digital forensics in the corporate sector will grow at a maximum rate of 19.2% between 2015 and 2020.
- The Asia-Pacific market will grow at a rate of 25.2% between 2015 and 2020.
- The global market is estimated to grow at about 14.2% during the same period.

"[The] Digital forensics market is majorly driven by the rate of digital crimes in a particular region," Sowmya Kulkarni, associate business consultant at IndustryARC, told *Legaltech News*. "Globally, the rate of digital crimes such as data espionage, cyber-based terrorism, computer intrusions, hacking, malware, and so on is relatively higher in the Americas region. According to the FBI, in the U.S. alone there has been report of over 269,422 complaints of cybercrimes received in 2014 with estimated loss of $800 million."

The use of digital forensics by the federal government "contributes to 45% of the overall market while the legal sector contributes to 55% of the overall market," Kulkarni added. Digital forensic revenue from the federal sector is estimated to increase from $1.1 billion in 2015 to $2.1 billion by 2020, *Legaltech News* reported.

CYBERSECURITY

Survey: CEOs Feel Left Out of Cybersecurity Plans

Only 51% of chief executive officers (CEOs) believe their organization's cybersecurity strategy is "well established," according to a recent IBM survey. The "Securing the C-Suite" survey also found that 77% of chief risk officers (CROs) and 76% of chief information officers or chief technology officers feel the same.

They may feel this way because 55% of CEOs consider themselves to have "little to no engagement" in cybersecurity threat management activities, and more than half of CROs, chief legal officers, chief marketing officers, and chief financial officers agreed with that assessment, IBM's survey revealed.

IBM separated the respondents into three groups:

1. Cyber-secured – 17%
2. Growing capability – 56%
3. Unprepared – 27%

The survey found that 79% of cyber-secured organizations had established an office of information security and appointed a chief information security officer. Just 32% of growing capability organizations and 29% of unprepared organizations had done the same.

"The world of cybercrime is evolving rapidly, but many c-suite executives have not updated their understanding of the threats," said Caleb Barlow, vice president at IBM Security, in a statement accompanying the report. "While chief information security officers (CISO) and the board can help provide the appropriate guidance and tools, CxOs [chief executive officers] in marketing, human resources, and finance, some of the most sensitive and data-heavy departments, should be more proactively involved in security decisions with the CISO."

PROFESSIONAL DEVELOPMENT

Study Reveals Skills RIM Pros Will Need

The records and information management (RIM) profession is becoming more technical and more closely aligned with data analysts and IT staff, according to the research report "What will it take to be a NextGen InfoPro?" from Iron Mountain and AIIM.

By 2020, the study revealed, employers expect their RIM professionals to be competent in risk management – with 50% of employers desiring them to have security and data privacy skills; 47% demanding content and information management skills across a wide range of formats and platforms; and 44% seeking data analytic skills.

Beyond that, the report suggests, employers want RIM professionals who can identify new opportunities for their organization's data and support colleagues during disruptive changes, such as mergers, acquisitions, or divestitures.

"It's no longer enough to be a competent records manager. It's time for them to evolve into next-generation information professionals with stronger technical, analytical, and management skills and the confidence to think, mediate, and guide," said Sue Trombley, managing director of thought leadership at Iron Mountain.

The study also revealed that over the next three to five years:

- The most sought-after professional RIM capabilities will be related to information accessibility, including the use of mobile devices (53% of organizations); data-quality management, data cleansing, and migration (49%); and information security and access control (42%).
- The demand for technical knowledge will center on information security systems and procedures (68% of organizations); enterprise content management, document management, and records management systems (60%); and mobile devices (53%).
- Organizational expectations for RIM professionals will be broad and include soft skills like innovative thinking (70% of organizations) and change management (70%).

According to Iron Mountain, the study may reveal a mismatch between what employers expect and what information professionals currently deliver. The greatest gap is found in the ability to manage change, which is highly regarded by 70% of employers, but only half of RIM professionals are confident about having.

Iron Mountain suggests that RIM professionals must educate themselves continuously on the latest technology, security, and management developments and how each affects their organizations. The survey found that 79% of RIM professionals are proactively enhancing their skills, while only 8% are content with their current abilities.

CYBERSECURITY

Global Survey: Only 1 in 5 Organizations Securely Manages User Identities

Organizations are rapidly developing and hosting new online services but frequently under-invest in adequate cybersecurity measures, according to a recent global survey by Capgemini and RSA.

The survey, "Identity Crisis: How to Balance Digital Transformation and User Security?," polled more than 800 C-level executives in Benelux and the Nordics, France, Germany, the UK, and the United States and found that 62% consider it critical or very important for their organizations to securely enable or extend access for users to digital services, but only 26% have the technology in place to do so.

"As organizations extend to the cloud they must ensure they have solutions in place that address the risk and threats associated with assuring user identities," Jim Ducharme, vice president of identity products at RSA, said in a news release. "These solutions must understand who is accessing what; manage that access effectively; and control access across the various cloud services. These elements are absolutely essential to giving the organization the assurance that users are who they say they are in a cloud environment."

Eighty-four percent acknowledged they need to offer more flexible, adaptive authentication methods and IDs, according to the survey. And, the survey showed, companies are trying to do just that: 68% have increased their identity and access management (IAM) budgets, with 28% reporting a "strong" increase.

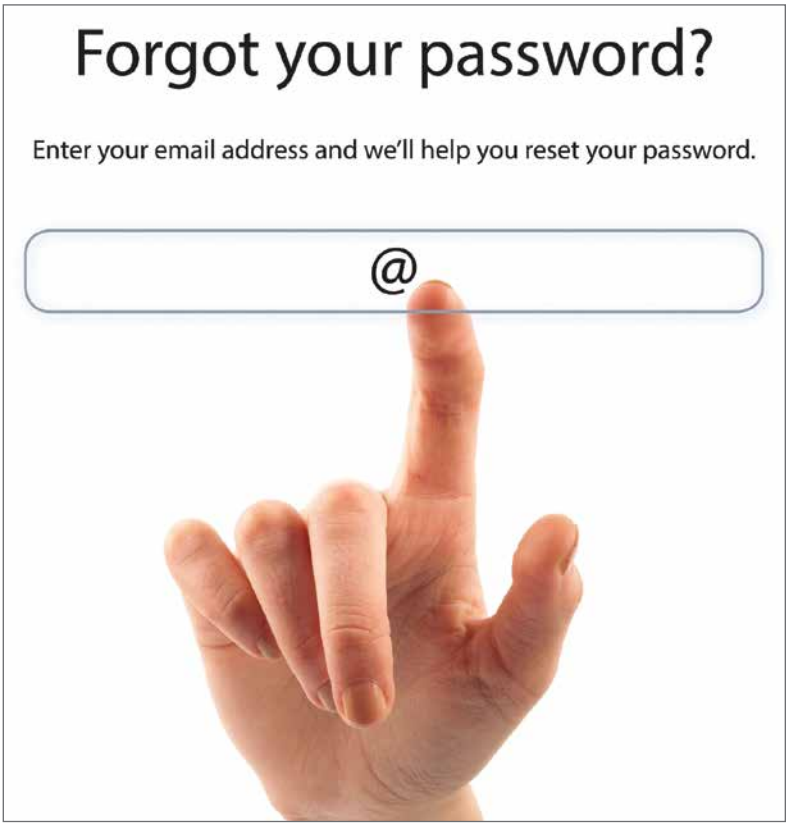
The survey also revealed that the way IAM is being viewed and implemented is changing, as a result of maturing and emerging technologies and user preferences. According to the results, allowing users to log in securely with their existing social identities is the goal of many companies.

The report also revealed that:

- Adaptive authentication is expected to define the future of device and service access for users. Most organizations – 84% – consider the ability to deploy such authentication and offer users more access options a high or very high priority.
- For most companies (85%), it is critical or very critical to add new services underpinned by cloud technology quickly and efficiently and to ensure these are supported by IAM.
- U.S. and European organizations are very sensitive to where security services are hosted, with close to 90% of respondents preferring or requiring data centers that deliver IAM services to be located within their country or region.

"The days of logging into a company's system with a username and password specific to that organization are numbered. Users aspire to log in from anywhere in a variety of ways, including with social media profiles and existing email account," said Mike Turner, COO of Global Cybersecurity at Capgemini Group. "The ownership of online identities is moving away from the organization to more flexible and secure services maintained by the user, addressing access management needs."

Turner added that while it is good to see increasing recognition and investment from senior leadership, most organizations have a long way to go before reaching that goal.



EHRS

Survey: Patients Lack Online Access to Health Records

According to a recent survey of 502 consumers planning to enroll in a health plan in 2016, 53% of patients say they have no online access to their healthcare data. The survey, conducted by healthcare technology company HealthMine, also found:

- 32% have had difficulty accessing their medical records at all.
- 29% have had difficulty accessing their lab records.
- 29% have had difficulty accessing their insurance information.
- 25% have had difficulty accessing their prescription history.

However, according to FierceHealthIT, the Office of the National Coordinator (ONC) for Health IT recently reported that online access to medical records is growing for consumers – from 28% in 2013 to 38% in 2014, the ONC reported.

A $10 million infusion of new funding to expand the OpenNotes program to 50 million patients nationwide may help boost those numbers. The program, which gives patients real-time access to their doctors' clinical notes, has grown to cover 5 million patients, FierceHealthIT reported.

"Based on recent studies and our own enforcement experience, far too often individuals face obstacles to accessing their health information, even from entities required to comply with the HIPAA Privacy Rule. This must change," wrote Jocelyn Samuels, director of the HHS Office for Civil Rights (OCR).

The OCR has released the first of what will be a series of Frequently Asked Questions documents, as well as a fact sheet, covering patients' general rights to their protected health information, what data is excluded from that right to access, how an individual may request access, and how an entity must provide the information.

GOVERNMENT RECORDS

U.S. Agencies Less Cyber-Secure in 2016

Many large U.S. federal agencies are less secure now than they were in 2015, according to an Office of Management and Budget (OMB) report. Overall, the average "cybersecurity assessment score" for the reporting agencies was 68% for the fiscal year, down 8% from the previous fiscal year, *Legaltech News* reported.

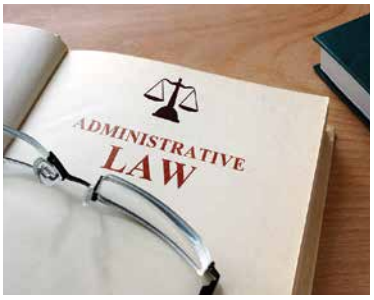
According to the OMB's fiscal year 2015 "Federal Information Security Modernization Act" report to Congress, of the 24 federal departments and agencies named within the CFO Act of 1990, only the General Services Administration – at 91% – scored above 90%, in contrast to the eight agencies that scored above 90% in the 2014 fiscal year.

Thirteen agencies achieved a "moderate" grade between 65% and 90%, including the remaining top-five finishers: Department of Justice (89%), Department of Homeland Security (DHS) (86%), Nuclear Regulatory Commission (86%), and National Aeronautics and Space Administration (85%).

Scoring less than 50% were the State Department (34%), Department of Housing and Urban Development (39%), Department of Agriculture (43%), and Department of Transportation (48%). The Department of Defense was deemed too large to receive an accurate grade, according to *Legaltech News*.

The report found federal agencies reported 77,183 cybersecurity incidents, a 10% increase over the 69,851 incidents reported in FY2014.

According to the OMB, the president's FY2017 budget, which includes $19 billion in cybersecurity resources, may help. It would lead to the creation of the Information Technology Monetization Fund, which aims to facilitate "the retirement of the Government's antiquated information technology (IT) systems and transition to more secure and efficient modern IT systems, funding to streamline governance and secure Federal networks, and investments to strengthen the cybersecurity workforce and cybersecurity education across the nation."



E-DISCOVERY

Courts Applying New FRCP Amendments in Discovery Cases

Courts have not hesitated to employ the December 2015 amendments to the U.S. Federal Rules for Civil Procedure (FRCP) in rulings on preservation, proportionality, and specificity.

In one recent example, *NuVasive v. Madsen Med.* (S.D. Cal. Jan. 26, 2016), a court in the Southern District of California cited amended Rule 37(e) in allowing the plaintiff to vacate a prior order that imposed an adverse inference for failing to preserve text messages. Under the previous Rule 37(e), the court said that NuVasive had spoliated evidence by not saving messages of four employees who were key to the case, and it denied NuVasive when it tried to make a similar claim against Madsen.

But, the court did not say that NuVasive had *intentionally* failed to preserve the text messages, and as the court noted in its January ruling, intention matters. The new rules allow an adverse inference for failure to preserve ESI "only upon the finding that the [spoliating] party acted with the intent to deprive another party of the information's use in the litigation."

The FRCP amendments got the U.S. Supreme Court's attention as well. In the court's 2015 "Report on the Federal Judiciary," Chief Justice John Roberts addressed the changes. Discussing proportionality, he wrote that [Rule 26(b)(1)] "states, as a fundamental principle, that lawyers must size and shape their discovery requests to the requisites of a case. Specifically, the pretrial process must provide parties with efficient access to what is needed to prove a claim or defense, but eliminate unnecessary or wasteful discovery."

The federal court of the District of Colorado must have taken note of Roberts' writings; it referenced them in *Kissing Camels Surgery Center v. Centura Health Corporation* (D. Colo., Jan. 22, 2016).

The case, which concerned an antitrust dispute for ambulatory surgery centers, examined both sides' production requests after the defendant asked the plaintiff to go through the terabyte of data it had produced to identify which documents were relevant to its requests. However, the court did not appreciate the request.

First, the court said that being "mired in continuous disputes over the appropriateness of discovery served and the adequacy of responses" for "six months ... is not what the Federal Rules intended." Thus, the court's ruling called the defendant's requests "omnibus requests" and said that they were "improper on their face." It also criticized the defendant for not trying to tailor definitions of requests to the specific case as well, often including boilerplate terms such as "including, without limitation, any [long list], or any other person(s) acting or purporting to act with or on behalf of the foregoing." **END**

RETENTION

Most UK Businesses Keeping Too Much Data

Seventy-five percent of businesses in the United Kingdom (UK) can't differentiate between a record that must be retained and data clutter, according to a recent survey conducted by Crown Records Management.

The survey, which polled IT decision makers in UK organizations with more than 200 employees, also found that:

- 55% do not have an e-mail retention policy in place.
- 58% do not audit their paper-based data regularly or destroy data that is no longer required.
- 60% do not regularly review what data is stored in the cloud or onsite.
- 64% do not filter what goes into the cloud.
- 76% do not have systems in place to help them distinguish between records that must be retained and other information.

"These results suggest businesses still aren't wising up to the importance of basic common-or-garden records management principle despite the high level of publicity for breaches," said Mike Dunleavy, head of customer development and experience at Crown Records Management, in a news release.