CONFIDENTIALITY COALITION

GENERAL COMMITTEE MEETING

Thursday, May 24, 2018
3:00 PM to 4:00 PM

Healthcare Leadership Council

750 9th Street, NW, Suite 500 Washington, D.C. 20001

Conference line: (857) 232-0157, 30-40-73#

1. Welcome and introductions

2. Guest Speaker: Jane Thorpe, J.D., Associate Professor and Vice Chair for Academic Affairs, George Washington University **Attachments 1,2**

a. ONC Document: Overview of Legal and Ethical Architecture for PCOR Data
b. Speaker Biographies
c. Overview of Health Information Law

3. OCR RFI Feedback on NPP and on Consumer Harm

4. Debrief on HSCC Cybersecurity Work Group

5. Articles on Data and Privacy **Attachments 3,4,5,6**

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Milken Institute School of Public Health
Department of Health Policy

950 New Hampshire Ave, NW
6th Floor
Washington, DC 20052

t 202-994-4100
f 202-994-4040
publichealth.gwu.edu

Jane Hyatt Thorpe, JD

Jane Hyatt Thorpe, J.D. is an Associate Professor and Vice Chair for Academic Affairs in the Department of Health Policy and Management in the Milken Institute School of Public Health and Director of the Healthcare Corporate Compliance Program at the George Washington University. She specializes in healthcare law and policy in the areas of Medicare, Medicaid, health care delivery systems and financing, health information exchange and technology, and corporate compliance. In addition to teaching courses in policy analysis, health care quality, and corporate compliance, Professor Thorpe is currently focusing her research and writing on legal and policy issues related to the impact of health reform implementation on health care quality, delivery, and payment with a particular focus on health information law and policy. Professor Thorpe also served as a Senior Advisor in the Office of the National Coordinator for Health Information Technology (ONC) as well as the Deputy Director of the Office of Policy for the Centers for Medicare & Medicaid Services (CMS) both within the U.S. Department of Health and Human Services (HHS). Prior to her academic career and government service, Professor Thorpe served as the Associate Vice President for Payment and Policy at the Advanced Medical Technology Association (AdvaMed) and practiced healthcare law providing regulatory and transactional counsel.

Professor Thorpe has an AB *magna cum laude* in History and a Certificate in American Studies from Princeton University and a JD from the Vanderbilt University School of Law. She is a member of the American Health Lawyers Association, the Healthcare Corporate Compliance Association, Academy Health, and the D.C. Bar Health Law Section and is admitted to the bar in Tennessee and the District of Columbia.

Lara Cartwright-Smith, JD, MPH

Lara Cartwright-Smith, JD, MPH, is an Associate Professor in the Department of Health Policy and Management in the Milken Institute School of Public Health and Program Director for the MPH Program in Health Policy. In addition to teaching and program administration, Professor Cartwright-Smith maintains a research portfolio focusing on the intersection of law and health policy, with a recent focus on breaking down real and perceived barriers to sharing health information for delivery system reform. She co-directs the Health Information & the Law project, an online resource for all federal and state laws related to the use and exchange of health information. Before her health policy career, Professor Cartwright-Smith practiced public interest civil rights and environmental law in a small law firm and worked as an attorney for both the federal Third Circuit Court of Appeals and the Pennsylvania Supreme Court.

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Milken Institute School of Public Health
Department of Health Policy

950 New Hampshire Ave, NW
6th Floor
Washington, DC 20052

t 202-994-4100
f 202-994-4040
publichealth.gwu.edu

Professor Cartwright-Smith received her BA *cum laude* in Philosophy from Bates College, her JD from Georgetown University Law Center, and her MPH from George Washington University. She is admitted to the bars of Maryland, Pennsylvania, and the District of Columbia.

Elizabeth Gray, JD, MHA

Elizabeth Gray is a Research Scientist and Professorial Lecturer in the Department of Health Policy and Management at the Milken Institute School of Public Health at the George Washington University. Elizabeth teaches in the undergraduate public health program, the residential and online MHA programs, and the health care corporate compliance graduate certificate program. Her research specialization is in health care law and policy, with a focus on health information collection and use, data privacy, and healthcare corporate compliance. Elizabeth has also worked on projects related to Medicaid coverage policy, health insurance benefit regulations, and health care reform.

Elizabeth holds a BS *magna cum laude* in Human and Organizational Development from Vanderbilt University, a JD from the George Washington University Law School, and an MHA *with honors* from the Milken Institute School of Public Health at the George Washington University. She is certified in health care compliance and a member of the bar in Pennsylvania, New Jersey, and Ohio.

Why Health Information Law?

An information revolution is occurring in U.S. health care and we are rapidly approaching a new era in which all medical records and related information will be maintained electronically. Data on a scale only recently imaginable will pass between individuals and institutions and be used in ways we cannot yet predict as the current healthcare delivery and public health system undergo a major transformation towards a more robust, evidence-based endeavor highly reliant on healthcare data for purposes ranging from research to surveillance to improved real-time care coordination. At the same time, access to, use, and release of health information, particularly individually identifiable data, is highly regulated at both the federal and state levels. How do current laws enable or limit this transformation? Are modifications of current laws or new laws necessary? How does the current legal landscape affect the roles and priorities of health system stakeholders ranging from patients and consumers to employers and insurers, health care providers and states? How do emerging technologies create new legal standards? How do legal issues differ depending on the particular data exchange model in question? How can data inform the elimination of racial and ethnic disparities in health care? All of these questions are critical to the future of the American healthcare delivery and public health system.

Although the move to electronic data raises new legal issues, it's important to remember that many of the questions above have existed in some form for a long time. Some of the most pressing legal issues related to health information, such as privacy considerations and liability for healthcare quality stretch back hundreds of years, to the origins of modern medicine. However, several things make today's landscape different. Our legal system is addressing the role of information in these age-old relationships in new ways, from the Health Insurance Portability and Accountability Act (HIPAA, 1996), the American Recovery and Reinvestment Act's Health Information Technology for Economic and Clinical Health Act (ARRA HITECH, 2009), and the Affordable Care Act (ACA, 2010) to state regulations on health insurance exchanges. Now more than ever, the law places real as well as perceived barriers and burdens on the collection and use of healthcare data. Important issues of privacy and consumer protection arise around new payment structures and new expectations for patient safety and high quality care. At the same time, there continues to be little awareness of the legal issues surrounding access to and use of healthcare data both clinical and financial.

Health information law and policy exists at the intersection of many crucial and interrelated fields: law, health care, consumer protection, information technology, public health, and insurance. Each small change can trigger a daunting set of issues and challenges. HealthInfoLaw.org offers keys to understanding the laws that govern health information and the implications they can have across health care and beyond.

Health Information & the Law Database and Resource (www.healthinfolaw.org)

Health Information and the Law (HealthInfoLaw.org), a project of the George Washington University's Hirsh Health Law and Policy Program developed with support from the Robert Wood Johnson Foundation, is designed to serve as a practical online resource to federal and state laws governing access, use, release, and publication of health information. Constantly updated, the site addresses the current legal and regulatory framework of health information law and changes in the legal and policy landscape affecting health information law and its implementation with commentary and key documents.

Contents

The database is a translational legal library including summaries, analyses, and links directly to relevant federal and state law (including Washington, D.C.) organized by a topical taxonomy. The database holds complete data on 45 states with 20 of those publicly available to users and others in the posting queue. Research is ongoing for the remaining 6 states. The website also includes several 50 state plus D.C. legal surveys related to specific areas of law, comparative state maps, decision support tools, interviews with experts from the field, and analytical briefs that allow users to see and understand the application of the law in their own geographic areas and how state law intersects with federal requirements and programs.

Audience

The Healthinfolaw.org site has been visited more than 1.1 million times between May 2012 (launch) and January 2018. The highest monthly total occurred in October 2016 with over 37,000 visits by approximately 29,000 unique visitors. Significantly, the website is accessed continuously (not limited to days in which new content is published) highlighting the value of the depth and breadth of legal and policy resources. Users include health care providers, consumers, administrators, policymakers, researchers, advocates, academics, and members of the press. Several government agencies are currently using the website to support their efforts, including CMS, ONC, FTC, SAMHSA, and NIH.

Topics Addressed by the Database

Antitrust	Medicaid/CHIP Data Requirements	Peer Review
Care Coordination/ Management	Medical Records Collection, Retention, & Access	Private Insurance Data Requirements
Cost/Utilization Measurement & Reporting	Medicare Data Requirements	Public Health Data Collection & Reporting
Equity & Disparities	Patient Engagement	Quality Measurement & Reporting
Federal & State Program Integrity	Patient Safety	Research
Health Information Technology	Privacy & Confidentiality	Security of Health Information

Frequent Users (email subscribers and Twitter followers)

Federal government agencies
- HHS OIG
- Health IT Team at HHS Office of Population Affairs
- Center for Medicare and Medicaid Innovation
- CMS
- Qualified Entity Certification for Medicare Data Program
- AHRQ
- NIH
- CDC
- SAMHSA

State & local government entities
- Illinois Office of Health Information Technology
- Kansas Department of Health & Environment
- Delaware Department of Health and Social Services
- New York Department of Health
- New Jersey Department of Health
- Office of Kentucky Health Benefit Exchange
- Minneapolis Health Department
- Massachusetts Dept of Housing and Community Development
- Massachusetts eHealth Institute
- San Luis Obispo County Public Health Department
- Los Angeles County Department of Mental Health

Health Information Exchanges
- Health Link NY
- Great Lakes Health Connect
- VITL (Vermont's HIE)

Healthcare providers & associations
- American Medical Association
- American Hospital Association Health Forum
- Pennsylvania State Nurses Association
- Mayo Clinic
- Louisiana Hospital Association
- The Cleveland Clinic
- Meriter Home Health
- Greater New York Hospital Association
- Providence Health System
- American College of Legal Medicine

Insurers & health plans
- United Healthcare
- Kaiser Permanente
- Wellcare
- BlueCross BlueShield of Illinois
- Cigna

Consultants & compliance officers
- Deloitte
- Health Law Consultancy
- ResDAC Assistance Desk
- Evident

Advocacy & interest groups
- AARP
- American Health Information Management Association
- CT Health Foundation
- Seattle Privacy Coalition
- Seattle Cancer Care Alliance
- Workgroup for Electronic Data Interchange Colorado Consumer Health Initiative
- Asthma and Allergy Foundation of America
- Privacy & Security Forum

Law firms & legal associations
- American Health Lawyers Association
- Feldesman Tucker
- Sidley Austin
- Squire Patton Boggs
- Morgan Lewis
- Manatt
- ABA Managed Care and Insurance Interest Group
- Crowell & Moring

Policy analysts
- Enroll America
- The Hilltop Institute
- Center for Health Policy and Research at the University of Massachusetts Medical School
- Universities
- University of Michigan School of Public Health
- Emory University
- University of Minnesota
- University of Pennsylvania Medical School

Other key health policy organizations
- National Academy for State Health Policy
- Joint Commission
- Center for Health Care Strategies
- Catalyst for Payment Reform

Press/Publications
- Annals of Internal Medicine
- Kaiser Health News
- Medline

mHealth & data management
- Striiv
- HealthJoy
- OnRamp Data Centers

Europe's Data Protection Law Is a Big, Confusing Mess

By Alison Cool

Ms. Cool is a professor of anthropology and information science at the University of Colorado, Boulder.

May 15, 2018

There is a growing realization that our data is under attack. From breaches at Equifax to Cambridge Analytica's misuse of the profile information of more than 87 million Facebook users, it seems as if none of our personal data is safe. And more and more about us is being captured, stored and processed by smart devices like thermostats, baby monitors, WiFi-connected streetlights and traffic sensors.

In the United States, people who are concerned are looking to Europe. They see Europe's "right to be forgotten," by which citizens can force companies to erase some of their personal data, as a step toward regaining ownership of their online selves. And on May 25, the European Union will bring into force the most sweeping regulation ever of what can be done with people's data.

This law, the General Data Protection Regulation, will give citizens greater control over their data while requiring those who process personal data in the European Union or about its citizens to take responsibility for its protection. The G.D.P.R. will give Europeans the right to data portability (allowing people, for example, to take their data from one social network to another) and the right not to be subject to decisions based on automated data processing (prohibiting, for example, the use of an algorithm to reject applicants for jobs or loans). Advocates seem to believe that the new law could replace a corporate-controlled internet with a digital democracy.

There's just one problem: No one understands the G.D.P.R.

The law is staggeringly complex. After three years of intense lobbying and contentious negotiation, the European Parliament published a draft, which then received some 4,000 amendment proposals, a reflection of the divergent interests at stake. Corporations, governments and academic institutions all process personal data, but they use it for different purposes.

There's another reason for the regulation's complexity and ambiguity: What are often framed as legal and technical questions are also questions of values. The European Union's 28 member states have different historical experiences and contemporary attitudes about data collection. Germans, recalling the Nazis' deadly efficient use of information, are suspicious of government or corporate collection of personal data; people in Nordic countries, on the other hand, link the collection and organization of data to the functioning of strong social welfare systems.

Thus, the regulation is intentionally ambiguous, representing a series of compromises. It promises to ease restrictions on data flows while allowing citizens to control their personal data, and to spur European economic growth while protecting the right to privacy. It skirts over possible differences between current and future technologies by using broad principles.

But those broad principles don't always accord with current data practices. The regulation requires those who process personal data to demonstrate accountability in part by limiting data collection and processing what is necessary for a specific purpose, forbidding other uses. That may sound good, but machine learning, for example — one of the most active areas of research in artificial intelligence, used for targeted advertising, self-driving cars and more — uses data to train computer systems to make decisions that cannot be specified in advance, derived from the original data or explained after the fact.

In 2017, the year after the regulation was approved, I interviewed scientists, data managers, legal scholars, lawyers, ethicists and activists in Sweden. I learned that many scientists and data managers who will be subject to the law find it incomprehensible. They doubted that absolute compliance was even possible.

One expert at Sweden's national bioinformatics platform said: "We often wonder, like, what does the law say about this? Nobody knows." Or as a scientist in charge of computing and storage facilities at a major university put it, the G.D.P.R. says, more or less, "that adequate safety should be in place, and so on. Right — what does *that* mean?"

Many of the law's broad principles, though they avoid references to specific technologies, are nevertheless based on already outdated assumptions about technology. "I think it's very clear that they imagined some company that has your data physically stored somewhere, and you have the right to take it out," a law professor told me of the G.D.P.R.'s approach to data portability. But in the era of big data and cloud services, data rarely exists in only one place.

What the regulation really means is likely to be decided in European courts, which is sure to be a drawn-out and confusing process.

Still, the G.D.P.R. is not a lost cause. We do need rules about data. But legal frameworks, particularly when they are long, complex and ambiguous, can't be the only or even the primary resource guiding the day-to-day work of data protection.

If the ultimate goal is to change what people do with our data, we need more research that looks carefully at how personal data is collected and by whom, and how those people make decisions about data protection. Policymakers should use such studies as a basis for developing empirically grounded, practical rules.

In the end, pragmatic guidelines that make sense to people who work with data might do a lot more to protect our personal data than a law that promises to change the internet but can't explain how.

Alison Cool is a professor of anthropology and information science at the University of Colorado, Boulder.

GAO Report: Patients Think Access Fees for Medical Records are Too High

Some patients encounter provider fees for medical record access so high they decide to cancel their requests, a Government Accountability Office investigation published today finds.

Though HIPAA laws require providers to give patients access to their data — and to charge at most a "reasonable, cost-based fee" — patients sometimes consider the costs a barrier, according to GAO interviews. Patients were often unaware that they could challenge providers who withheld their records, and some canceled their requests for records after learning the cost.

Patient advocates described patients being charged $500 for a single record; one patient paid $148 for a single PDF. Others were required to pay an annual subscription fee for their records, according to the report.

Providers incur their own costs when fulfilling patient and third-party requests, including staff time, the report found. Some also reported that extracting medical records from EHR systems is excessively complicated.

The GAO interviewed four provider associations, seven vendors, six patient advocates, state officials, and HHS officials for the study.

In interviews with providers in Kentucky, Ohio, Rhode Island and Wisconsin, GAO found that fee structures varied by state. Providers in Ohio, Rhode Island and Wisconsin had per-page fees; in Kentucky, patients get one free copy of records and are charged up to $1 per page for additional copies.

The 21st Century Cures Act directs GAO to look into patient access issues.

GAO Highlights

Highlights of GAO-18-386, a report to congressional committees

May 2018

MEDICAL RECORDS

Fees and Challenges Associated with Patients' Access

Why GAO Did This Study

HIPAA and its implementing regulations, as amended by the Health Information Technology for Economic and Clinical Health Act, require health care providers to give patients, upon request, access to their medical records, which contain protected health information (i.e., diagnoses, billing information, medications, and test results). This right of access allows patients to obtain their records or have them forwarded to a person or entity of their choice—such as another provider—in a timely manner while being charged a reasonable, cost-based fee. Third parties, such as a lawyer or someone processing disability claims, may also request copies of a patient's medical records with permission from the patient.

The 21st Century Cures Act included a provision for GAO to study patient access to medical records. Among other things, this report describes (1) what is known about the fees for accessing patients' medical records and (2) challenges identified by patients and providers when patients request access to their medical records. GAO reviewed selected HIPAA requirements and implementing regulations and guidance, and relevant laws in four states selected in part because they established a range of fees associated with obtaining copies of medical records. GAO also interviewed four provider associations, seven vendors that work for providers, six patient advocates, state officials, and Department of Health and Human Services' (HHS) officials. The information GAO obtained and its analysis of laws in the selected states are not generalizable. HHS provided technical comments on this report.

View GAO-18-386. For more information, contact Carolyn L. Yocom at (202) 512-7114 or yocomc@gao.gov.

What GAO Found

Available information suggests that the fees charged for accessing medical records can vary depending on the type of request and the state in which the request is made. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations, providers are authorized to charge a reasonable, cost-based fee when patients request copies of their medical records or request that their records be forwarded to another provider or entity. In the case of third-party requests, when a patient gives permission for another entity—for example, an attorney—to request copies of the patient's medical records, the fees are not subject to the reasonable cost-based standard and are generally governed by state law. According to stakeholders GAO interviewed, the fees for third-party requests are generally higher than the fees charged to patients and can vary significantly across states.

The four states GAO reviewed have state laws that vary in terms of the fees allowed for patient and third-party requests for medical records. For example, three of the states have per-page fee amounts for patient and third-party records requests. The amounts charged are based on the number of pages requested and vary across the three states.

- One of the three states has established a different per-page fee amount for third-party requests. The other two do not authorize a different fee for patient and third-party requests.
- One of the three states also specifies a maximum allowable fee if the provider uses an electronic health records system. The other two do not differentiate costs for electronic or paper records.

In the fourth state, state law entitles individuals to one free copy of their medical record. The statute allows a charge of up to $1 per page for additional copies.

Patient advocates, provider associations, and other stakeholders GAO interviewed identified challenges that patients and providers face when patients request access to their medical records.

- Patients' challenges include incurring what they believe to be high fees when requesting medical records—for example, when facing severe medical issues that have generated a high number of medical records. Additionally, not all patients are aware that they have a right to challenge providers who deny them access to their medical records.
- Providers' challenges include the costs of responding to patient requests for records due to the allocation of staff time and other resources. In addition, according to provider associations and others GAO interviewed, fulfilling requests for medical records has become more complex and challenging for providers, in part because providers may store this information in multiple electronic record systems or in a mix of paper and electronic records.

The Big Read **Genomics**

Biotechnology: the US-China dispute over genetic data

The FBI is beginning to raise national security questions about genetic data going overseas

YESTERDAY by: David J Lynch

There are not many agents in the Federal Bureau of Investigation like Ed You. In a workforce that cultivates anonymity, his clean-shaven head gleams. While most of his colleagues are notoriously tight-lipped, Mr You is the chatty star of technology conferences such as South-by-Southwest and DEFCON.

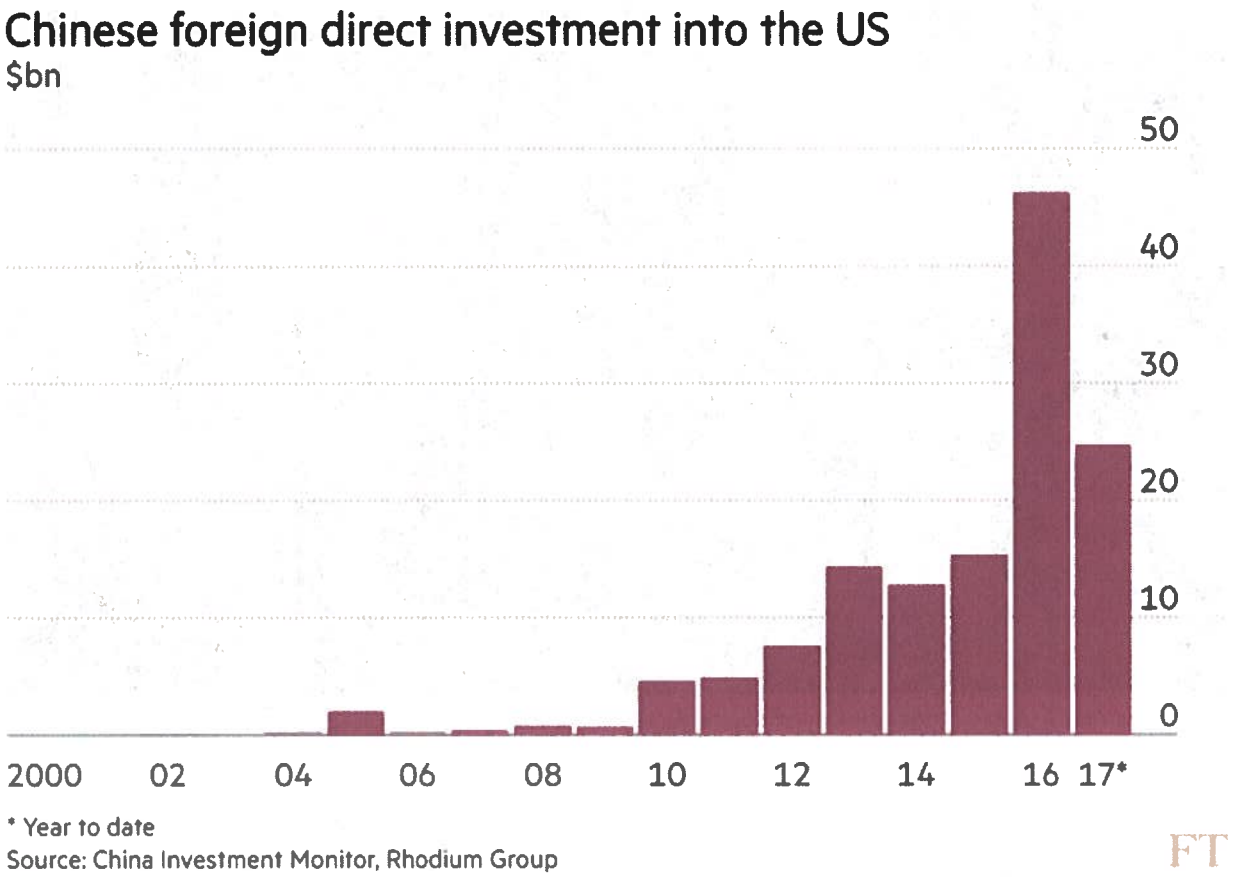
He is also at the forefront of a potential dispute between the US and China, which could have implications for both commercial relations between the world's two biggest economies and for the future of biomedical research.

The high profile that Mr You has adopted is part of an unusual FBI campaign to highlight the risks in America's headlong pursuit to unlock the secrets of the human genome. A supervisory special agent in the bureau's biological countermeasures unit, Mr You warns that the US is not protecting the genomic data used to create lucrative new medicines — but which can also be used to develop fearsome bioweapons.

"We don't know how much bio data has left our shores," he says. "Our concept for biological security needs to be broadened."

Sophie Liu, a research scientist at California's Complete Genomics. In 2013 it was bought by China's BGI-Shenzhen © Bloomberg

That has led him to focus on China, which the veteran lawman says is gaining access to US genomic data — the biological software that governs human organisms. In recent years, Chinese investors have purchased stakes in, or partnered with, US biomedical companies that specialise in genomics. At the same time, state-sponsored hackers believed to be Chinese have penetrated the laboratories, health insurers and hospitals where other valuable patient records reside. Mr You suggests stricter controls might be needed on what sort of health data can be transferred overseas — to China and elsewhere.



Nearly two decades after the first human genome was decoded, the field is one of the most exciting in biomedical research — and one that relies on an open network of international collaboration.

But it is also the latest area where national security questions — about Chinese objectives and the links between its companies and the state — are leading to calls for important sectors of the US economy to be ringfenced.

Since the 2014 decision to bar Huawei from selling into parts of the US telecoms infrastructure market, America has blocked Chinese acquisitions of a wind turbine company in Oregon, a California cloud computing firm, and the US-based division of a German semiconductor maker. The Pentagon has raised concerns about Chinese investment in artificial intelligence.

FBI agent Ed You has called for limits on the kind of biodata that can be sold or transmitted outside US borders © FBI

Traditionally, the FBI's weapons of mass destruction directorate has concentrated on preventing toxins such as Ebola or anthrax from falling into the wrong hands — and contributing to the spread of new germ weapons.

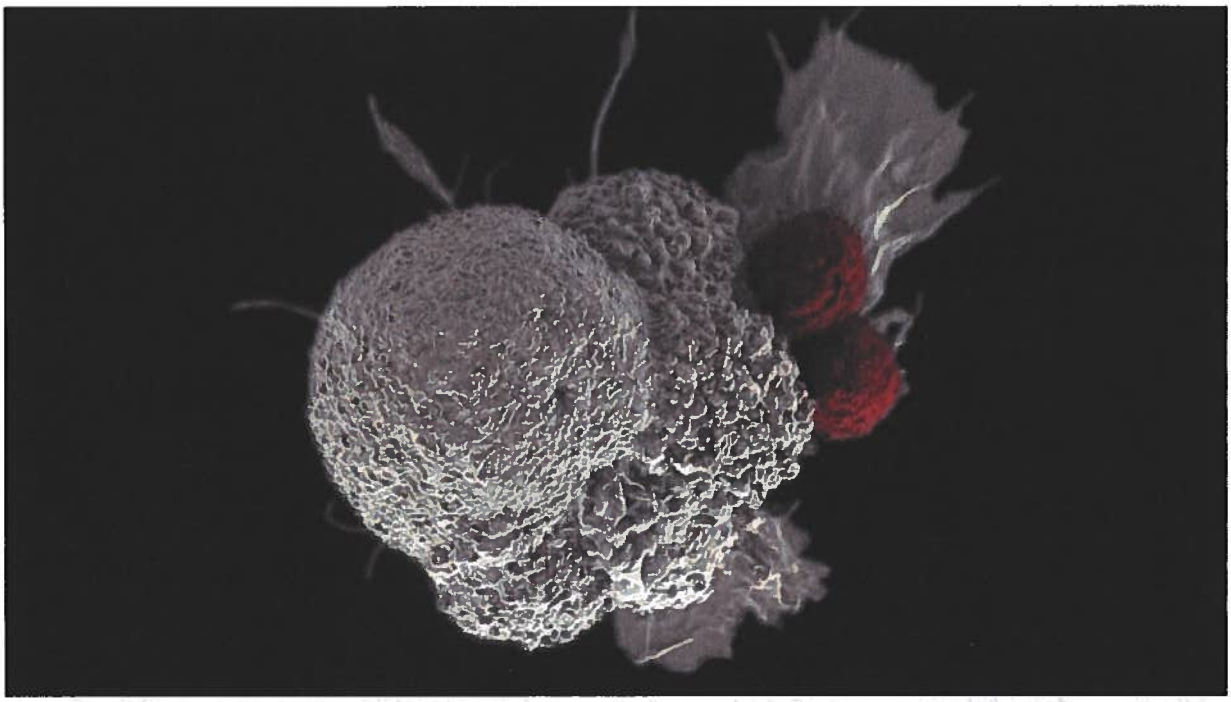
Now, the bureau fears that digital data sets may prove just as lethal. The concerns about large volumes of US genetic data being scooped up help explain why a law enforcement agency is tracking the potential loss of US competitive advantage. "The economic impact is the principal near-term threat — the monetisation of large data sets," says Mr You.

Some observers believe the US government is right to ask questions about the implications of Chinese investment in genomics. "I've never seen an agency, the FBI, come out of the woodwork like this," said Michael Wessel, a member of the US-China Economic and Security Review Commission, a congressionally-chartered advisory body. "This is a critical area that needs a lot more attention . . . It's a real threat."

Others worry that it would be damaging for the US to put up excessive barriers to Chinese biomedical investment. Dan Rosen, founding partner at the Rhodium Group in New York, points out that China has invested more than $3.2bn in the US biotech and pharmaceuticals sector over the past five years — cash that often brings with it talented Chinese scientists. In some disciplines, such as large-scale, low-cost gene sequencing,

China leads the US. If Chinese companies become less welcome in the US, he says, they will go elsewhere.

"I don't think drawing a line around biotech and calling the entire industry a critical sector is going to do the trick," said Mr Rosen. "We're going to have to maintain the ability to look at investments case by case."



A cancer cell being attacked by two cytotoxic T-cells. Genome sequencing could bring a better understanding of who is at risk of developing cancer and personalised treatments © Rita Elena Serda/Duncan Comprehensive Cancer Centre at Baylor College of Medicine; NCI;NIH

The promise of genomics is a new era of precision targeted drugs that make traditional one-size-fits-all medicine look like a second world war dumb bomb. But treatments that are customised for a patient's individual genetic make-up remain in their early stages.

Both the US, the acknowledged global leader, and China are pursuing personalised treatments for diseases such as cancer, cystic fibrosis or Alzheimer's. China last year unveiled a $9bn 15-year research initiative, dwarfing an Obama-era plan that earmarked $215m for the National Institutes of Health.

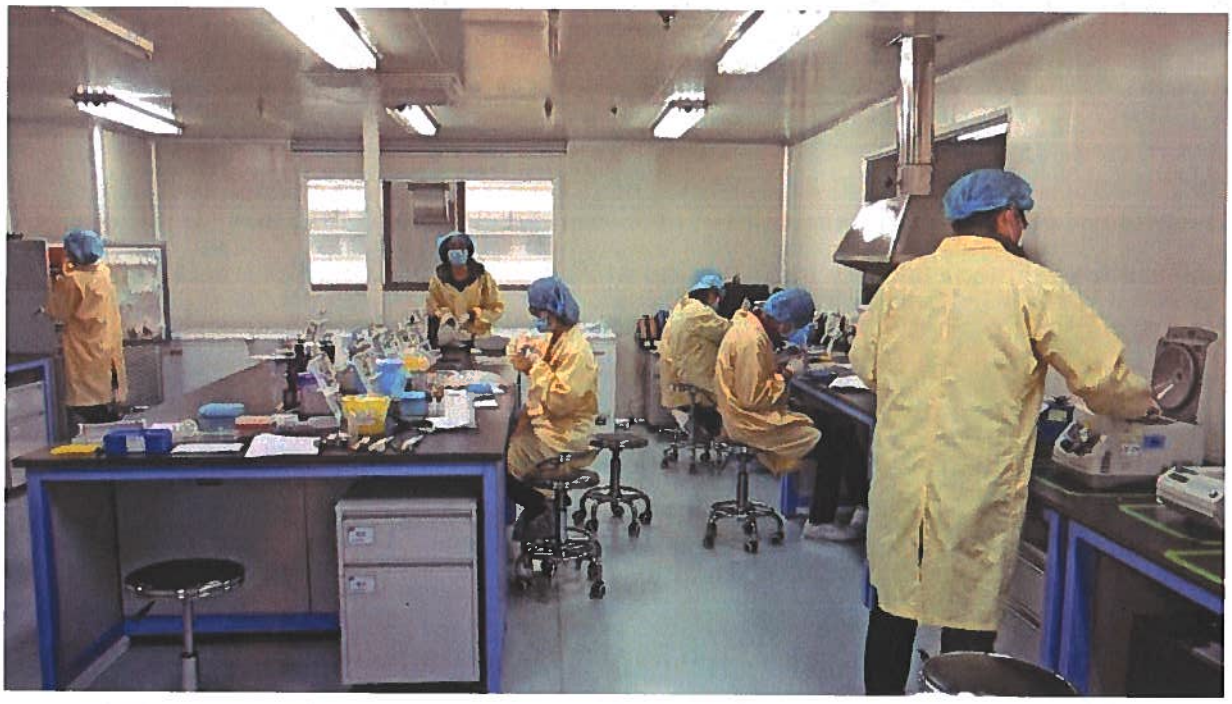
DNA science has leapfrogged since 2000 when the human genome was first sequenced. What once required years of work and cost billions of dollars now takes less than a week

and costs just $1,000. The US is gathering genetic data from more than 1m volunteers, so that automated lab systems can investigate how individual genes interact.

"The first problem is having access to data . . . You need a lot of data," says Eleonore Pauwels at the Wilson Center in Washington.

Beijing's ambitions in this area have led some Chinese companies to go on the acquisition trail — especially in the US. In January, for example, iCarbonX of Shenzhen, which aims to create personalised health treatments by combining AI with large pools of genetic data, invested more than $100m in PatientsLikeMe. The US company says it is the world's largest personalised health network with more than 500,000 individuals sharing their medical details. PatientsLikeMe, based in Cambridge, Massachusetts, says that its data are anonymised and retained on US-based servers.

That kind of data — stored in 100 gigabyte to 1 terabyte digital files — could be used to develop new drugs. Laboratories gather enormous numbers of such files, then combine them with detailed demographic, diet, health and lifestyle records. Supercomputers search for patterns, identifying genetic malfunctions and suggesting new remedies.



Researchers in a laboratory in Tianjin. China has made genome sequencing a research priority © Reuters

The same data sets can, however, be used to develop bioweapons. The FBI, which first raised its biomedicine concerns in late 2014, has not officially offered any policy recommendations. Mr You, who has a masters degree in biochemistry and molecular biology, suggests tightening regulations on health records to make it harder to transfer them overseas.

Although most of the Trump administration's top science jobs are vacant, Mr You insists the FBI's concerns are "starting to get more traction" inside government.

Outside Washington, views are mixed. "I don't think he's an alarmist. He's raising some questions that need to be asked and answered," says Ben Shobert, senior associate at the National Bureau of Asian Research.

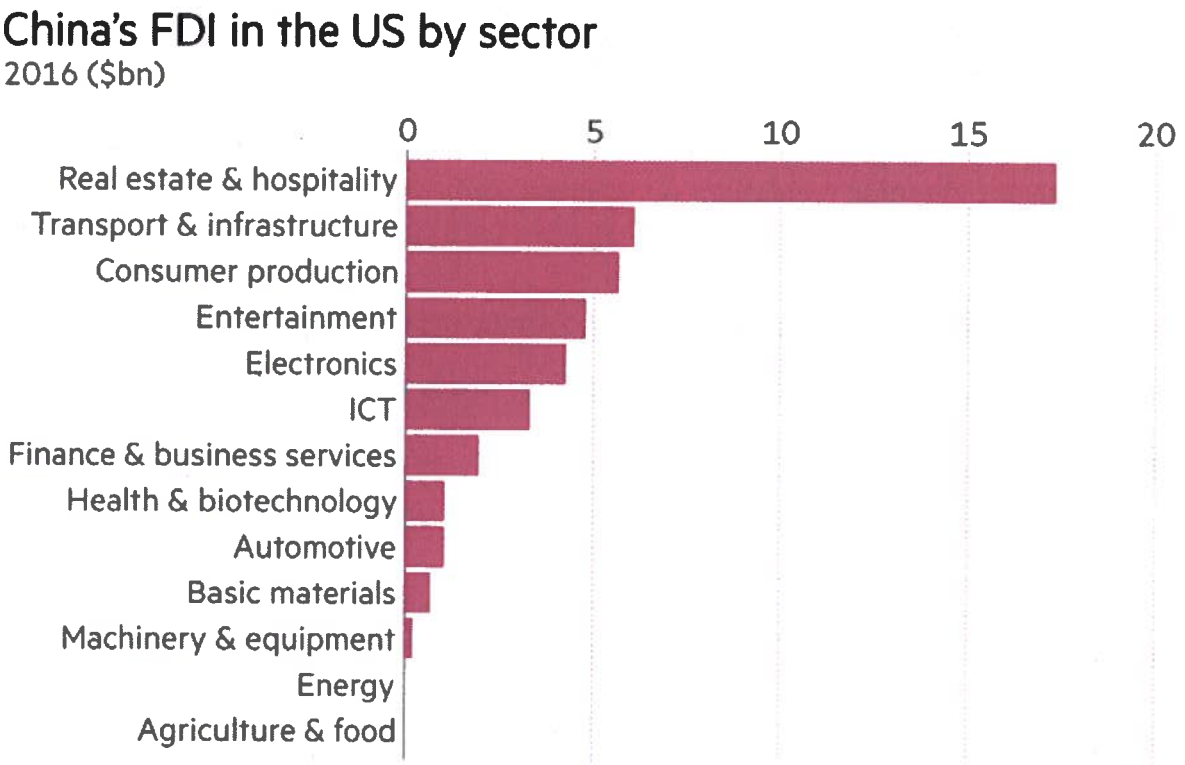
But Bernard Munos, senior fellow at the Milken Institute's FasterCures, says the bureau's concerns are exaggerated. "What they can steal from us is data," he says of competitors. "Data are a necessary ingredient, but not sufficient. You need bright people who are going to extract knowledge from that data and from that knowledge imagine potential new treatments. At the moment, the capabilities of the Chinese to do that are limited."

FBI officials recognise that science is a global endeavour that would wither if confined within national borders.

The US Human Genome Project, for instance, would have taken far longer without help from the UK, Germany, France, Japan and China. And roughly 40 per cent of the biomedical scientists in the US hail from China or India, according to Mr Munos.

"US biomedical research could hardly function today without this contingent of people," he says. "The collaboration is an essential part."

That's why cross-border deals so far have faced few objections. In 2013, the US government's committee on foreign investment (Cfius) approved BGI-Shenzhen's purchase of Complete Genomics in California, which has sequenced more than 20,000 human genomes.

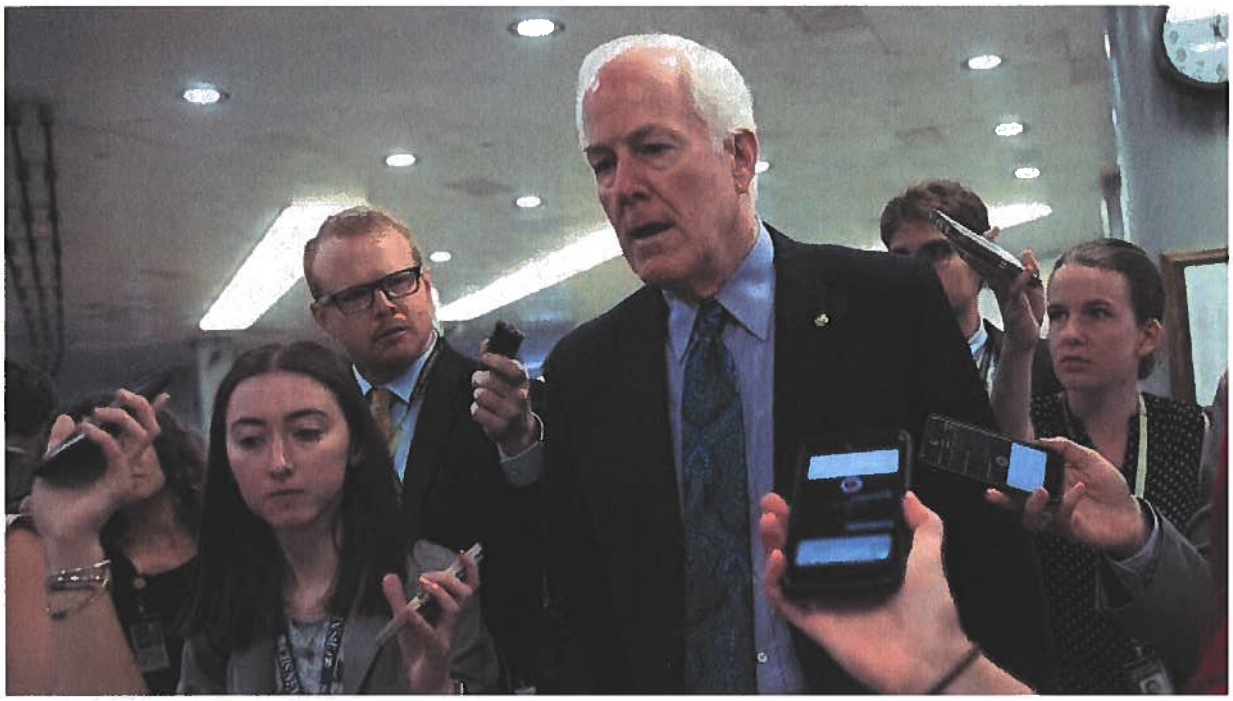


Today such a deal might be rejected, says Mr Wessel, a member of the US-China Commission. One reason is a lack of reciprocity. Even as Chinese groups take stakes in US biomedical companies, Chinese regulations prevent foreign companies from taking genetic data out of China, according to Mr Shobert.

Cfius also does not track most foreign loans, non-controlling investments of less than 10 per cent — such as the iCarbonX deal — or stakes in start-ups.

"That's what's scaring the crap out of the FBI," says Mr Rosen. "That the most early-stage interesting stuff, the stuff happening in garages, could get sort of infiltrated with Chinese money."

In Congress, Senator John Cornyn, a member of the Republican leadership, plans to introduce legislation to expand government reviews of foreign investments to include joint ventures and other technology company acquisitions. "The status quo on investment from China is simply unsustainable," Mr Cornyn said at a June Council on Foreign Relations event.



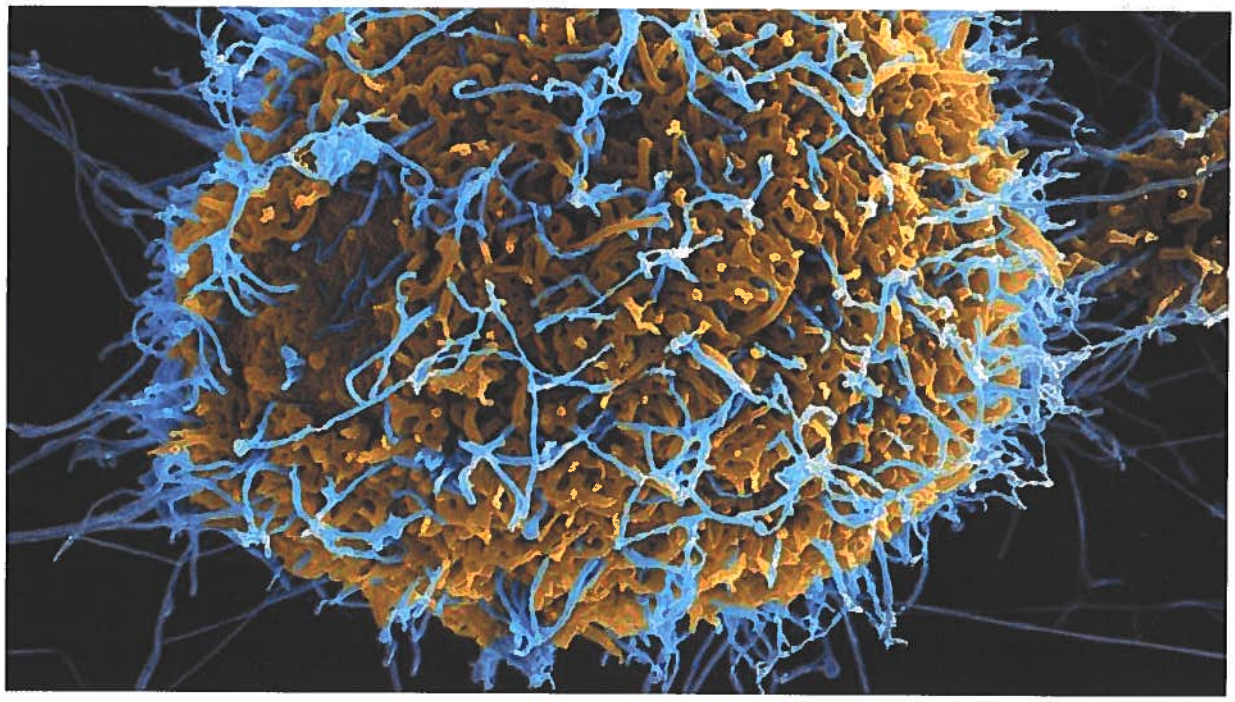
Senator John Cornyn wants to expand legislation on foreign investment to cover joint ventures © Getty

Cross-border deals are not the only risks to US genetic data. The healthcare industry is notoriously vulnerable to cyber attacks. Though most public attention to date has centred on identity theft or pilfered credit card details, patient medical records are even more valuable, says Mr You. Some recent hacks involved "actual penetration and acquisition of clinical data", he told the US-China commission in March.

In December, hackers infiltrated Quest Diagnostics, which boasts the world's largest clinical lab database, and gained access to 34,000 patient records, including laboratory results.

Although there is no evidence of foreign involvement in that episode, hackers who US officials believe were operating on behalf of the Chinese government broke into Anthem's networks in 2014 and spent a year rummaging through records of 78.8m customers, California regulators said in announcing a January settlement with the insurer.

"The healthcare industry in general is far less secure than many other industries and sectors out there. So the ability for a determined actor to get access to that type of information is certainly feasible if they're motivated to do so," says Charles Carmakal, vice-president at Mandiant, a cyber security company. "We just haven't seen it yet."



Genome sequencing could enable researchers to weaponise or adapt deadly diseases such as ebola. Pictured, a scanning electron micrograph of Ebola virus particles budding from an infected cell © National Institute of Allergy and Infectious Diseases; NIH

Meanwhile, national security risks loom. The US government has long invested in defences against about 60 pathogens and 10 toxins that pose a "severe" health risk, including the Ebola virus, the H1N1 flu virus and ricin.

But advances such as gene editing and next-generation DNA sequencing allow scientists to weaponise new viruses, perhaps including custom pathogens engineered to overcome existing immunities or to be impervious to current drugs. Some experts warn of bioweapons engineered to kill specific populations or even individuals.

Last year, James Clapper, director of national intelligence, included gene editing aimed at producing new biological weapons as among the nation's top security threats. "The risks are real," a White House scientific advisory panel said in November, "and will only grow as biotechnology becomes more sophisticated in the years ahead."

Insider threat: Scientist accused of stealing trade secrets

With a PhD in biological chemistry and four patents to her name, Yu Xue was "one of the top protein biochemists in the world", prosecutors

said when they charged her with stealing trade secrets from her employer.

Sitting in her GlaxoSmithKline office, across from a golf course in Upper Merion, Pennsylvania, **Ms Xue** emailed confidential documents to her alleged co-conspirators while downloading others on to a thumb drive.

Ms Xue was helping develop a monoclonal antibody, which acts as a homing device to carry a medical agent directly to cancer cells in order to slow or kill the cancer. It is an early example of the precision medicine that offers so much promise for tackling tough diseases — and keeping western drug companies in the global lead. The case highlights what US officials allege is a comprehensive Chinese campaign to acquire US technological secrets.

The alleged conspirators established a company in Nanjing, China, called Renopharma Inc. to market the stolen secrets, which included "step-by-step instructions" for performing tests, GSK's process for purifying proteins to be injected into patients, as well as experiment results, according to an updated indictment filed on May 24 in the US District Court in Philadelphia.

Renopharma received Chinese government funding, easy loans, a tax holiday and a 4,000-square-foot laboratory rent-free, according to Tao Li, a co-owner who also faces charges.

"Governments in different levels have helped us a lot," he wrote in an email cited by prosecutors. "This confirmed [to] us that the road we chose is right."

The group expected Renopharma to have almost $75m in sales this year, by producing "a new type of drug which possesses Chinese intellectual property rights", said another email.

Mr Li, Ms Xue and her twin sister Tian Xue, who was also charged, pleaded not guilty. Lucy Xi, who also worked at GlaxoSmithKline, the

UK-based company, has not yet entered a plea and no attorney is listed in court filings for Yan Mei, the final defendant.

At one point, Ms Xue emailed an article about an Eli Lilly scientist indicted for theft. "So scary," she said.

Health IT Security: Most Healthcare Workers Admit to Non-Secure Healthcare Data Sharing

Most healthcare workers surveyed admit to non-secure healthcare data sharing using email.

Source: Thinkstock

By Fred Donovan

May 21, 2018 - Most healthcare workers surveyed admit to non-secure healthcare data sharing using email.

A disturbing 87 percent of healthcare workers admit to using non-secure email to send sensitive information, including PHI, according to survey data provided

to *HealthITSecurity.com* by Kickstand Communications, which conducted the survey for secure file sharing services firm Biscom.

Healthcare workers are 36 percent more likely to share regulated data such as patient information and credit card information via non-secure methods such as email than those working in financial services.

Dig Deeper

- Benefits, Challenges of Secure Healthcare Data Sharing
- Maintaining Healthcare Data Security with File Sharing Options
- Considering Healthcare Data Privacy with Health Data Sharing

Yet, healthcare workers are 25 percent more likely to agree that their organization's security and policies are good compared with employees working in financial services, the survey found.

Virtually all healthcare companies have secure document delivery tools, and 92 percent of employees report they have been trained on how to use them. Eighty-eight percent of healthcare employees understand how to use tools and understand company rules around security, but 10 percent admit they do not abide by them.

A majority of healthcare workers said when it comes to transferring data, documents, or information, they do whatever is easiest. Close to three-quarters of respondents who work in healthcare agreed that they consider email to be a secure form of data, document, or information delivery, and 64 percent said when it comes to sharing data, email is the easiest tool.

The methods that healthcare employees are using to share sensitive information and the type of information that is being shared both internally and externally are concerning.

For example, more than one-third of respondents said they share sensitive data, documents, or other sensitive information internally using a cloud storage service, like Google Drive or Microsoft One Drive, or cloud sync and share service, like Dropbox.

Around 60 percent share customer data, such as names, phone numbers, and addresses, internally, and a similar percentage share regulated data, such as PHI and financial information, internally.

More than one-quarter of respondents share sensitive data, documents, and information externally using personal sync and share service like Dropbox. Less than one-quarter share sensitive data, documents, or other sensitive information using secure file transfer and file transfer protocol.

A majority of healthcare workers admit to sharing customer data externally, and a similar percentage admit to sharing regulated data, such as PHI, externally.

"The survey's results uncover some interesting factors that contribute to non-compliance," said Biscom CEO Bill Ho. "It would surprise most companies who have made major investments in security that so many people just fall back to the easiest method, namely sending confidential messages and files through email."

Across industries, 62 percent of the 600 US employees surveyed said they share customer data via non-secure email internally, 46 percent share strategy documents and presentations via non-secure email internally, 45 percent share company business and financial data via non-secure email internally, and 43 percent share regulated data via non-secure email internally.

Half of respondents across industries reported sharing customer data via non-secure email externally, 49 percent share regulated data via non-secure email externally, 35 percent said they share strategy documents or presentations via non-secure email externally, and 29 percent sharing intellectual property via non-secure email externally.

While 78 percent of respondents across industries said they understand and agree with their company's security policies, an overwhelming number of respondents reported non-securely sharing information both internally with their colleagues (74 percent) and with people outside of their organization (60 percent).

When asked why they did not use company tools or comply with company policies, respondents across industries agreed complexity was the biggest challenge. In fact, when deciding how to send sensitive documents, 60 percent said they simply do what is easiest.