Life Sciences Essentials

Moving to the Cloud: Privacy and Other Key Considerations for Healthcare Entities

May 13, 2015

Daniel Cooper
Georgia Kazakis
Anna Kraus
Scott Levitt
Lee Tiedrich

COVINGTON

BEIJING BRUSSELS LONDON LOS ANGELES NEW YORK SAN FRANCISCO
SEOUL SHANGHAI SILICON VALLEY WASHINGTON

www.cov.com

Welcome

- Welcome to the latest webinar in Covington & Burling's *Life Sciences Essentials* series. This series looks at critical issues facing pharmaceutical, biotech and medical device companies across a variety of practice areas.
- Our next program in the series will take place on June 3rd and will cover Congressional investigations.
- For information about upcoming programs or recordings of past programs, please visit us on the web: http://www.insideeulifesciences.com/presentations-and-webinars/.

Disclaimer

- The presentations and statements in this program are solely those of the individual attorneys, and are not intended to be construed as presentations or statements of Covington & Burling LLP or of any of Covington's clients. In addition, the presentations and statements in this program are not intended to be legal advice.

Continuing Legal Education

- CLE credit for this webinar is available for California and New York.
- To receive CLE credit, please complete the affirmation form and program evaluation that were attached to the confirmation email you received for this program.
- During the course of this program, we will read aloud and display on slides two codes, which you will need to record on the affirmation form in order to receive credit for attendance. Please note that the codes are case-sensitive.
- If you would like to apply on your own for CLE in another state, please fill out the forms and you will receive a general certificate of attendance. We will send the forms again, along with the presentation slides, to all attendees at the conclusion of the program.
- Please return all completed forms and direct all questions to Caroline Britt at cbritt@cov.com.

Introduction – Q&A

- At the end of the program, we will address the questions that are submitted via the online “chat” feature and we will also take questions by phone at that time.

Agenda

- HIPAA and HITECH Considerations in Negotiating a Cloud Services Agreement
- EU Health Data in the Cloud
- Commercial Considerations in Negotiating a Cloud Services Agreement
- Insurance Coverage for Cloud-Related Liabilities

HIPAA and HITECH Considerations in Negotiating a Cloud Services Agreement

Anna Kraus

HIPAA and HITECH Considerations

- Is your enterprise subject to HIPAA and HITECH?
- Does any of the information to be housed in the cloud constitute protected health information?
- Does the arrangement require a business associate agreement?
- What is a business associate agreement?
- What is not required to be addressed in a business associate agreement?

Is Your Enterprise Subject to HIPAA and HITECH?

Covered entities are subject to HIPAA and HITECH

- Health plans
  - Health insurers (including government programs like Medicare and Medicaid)
  - Employer health plans
- Health care providers
  - Provided that they make claims against third-party health insurance
- Health care clearinghouses
  - Entities that translate electronic health information from nonstandard to standard format
  - Example: billing service

Is Your Enterprise Subject to HIPAA and HITECH?

- **Business associates are subject to HIPAA and HITECH**
  - Entity that, on behalf of a covered entity, creates, receives, maintains, or transmits protected health information
  - Entity that provides to a covered entity certain specified services where the provision of the service requires disclosure of protected health information by the covered entity to the business associate
    - Examples of specified services: accounting, legal, consulting, management, administrative
  - Subcontractor of a business associate

Does Any of the Information to be Housed in the Cloud Constitute Protected Health Information?

Protected Health Information (PHI) is information:

- Created or received by a covered entity or an employer
- Relates to an individual's past, present, or future physical or mental health; payment for the provision of health care to an individual; and
- Identifies the individual or could be used, in conjunction with other readily available information, to identify the individual.

Examples of PHI

- Name
- Address
- Identification numbers
- Dates specific to an individual (birth date; date of treatment)

Does the Arrangement Require a Business Associate Agreement?

- The cloud services arrangement requires a business associate agreement if the answer to **both** of the following questions is "**Yes**"
  - Is your enterprise subject to HIPAA and HITECH?
  - Does any of the information to be housed in the cloud constitute PHI?

- What if the cloud services provider argues that it is not a business associate?
  - Pre-HITECH: Entity that, on behalf of a covered entity, creates, receives, or transmits PHI
  - Post-HITECH: Entity that, on behalf of a covered entity, creates, receives, **maintains**, or transmits PHI

What is a Business Associate Agreement?

- Agreement between the covered entity (or the business associate of a covered entity) to whom service is being provided and the cloud services provider
- Restricts the cloud services provider's ability to use and disclose PHI
  - Only those uses and disclosures necessary to provide the service (e.g., a cloud services provider may need to access data occasionally in connection with security requirements)
  - For the proper management and administration of the cloud service provider's business (e.g., as required by law)
  - No other use or disclosure permitted

What is a Business Associate Agreement?

- Cloud services provider must agree to comply with the HIPAA Security Rule
  - Conduct a security risk assessment
  - Administrative safeguards
    - Security management process
    - Security officer
    - Procedures to define levels of access to PHI
    - Security awareness training for employees
    - Security incident procedures
    - Contingency plans for data back-up and recovery and emergency operation

What is a Business Associate Agreement?

- **Physical safeguards**
  - Limitations on physical access to electronic information systems
  - Limitations on access to work stations
  - Proper removal and receipt of hardware and software containing PHI
- **Technical Safeguards**
  - Access control technology (e.g., passwords)
  - Audit controls to record and monitor system activity
  - Integrity safeguards to prevent improper alteration or destruction
  - Person or entity authentication
  - Transmission security (e.g., encryption)

What is a Business Associate Agreement?

- **Cloud services provider required to report to the covered entity any use or disclosure of PHI not provided for by the agreement or any security incident of which it becomes aware**
  - Timeframe?
- **Cloud service provider required to report to the covered entity any incident that might constitute a breach of unsecured PHI**
  - Require encryption of data at rest to eliminate breach notification requirement?
  - Covered entity has the obligation to conduct a risk assessment to determine whether incident constitutes a breach that requires notice to individuals, HHS, media
  - Timeframe?
  - Delegate risk assessment or notice to cloud services provider?
  - Require that cloud services provider indemnify covered entity for costs of risk assessment and notice?

What is a Business Associate Agreement?

- Cloud services provider must ensure that any subcontractors with access to PHI agree to the same restrictions and conditions
- Cloud services provider must make its internal practices, books and records relating to the use and disclosure of PHI available to HHS for the purposes of determining HIPAA compliance
- Covered entity must have the ability to terminate the arrangement if it becomes aware of a pattern or practice by the cloud services provider that violates HIPAA
- At termination of arrangement, cloud services provider must return or destroy all PHI, if feasible
  - What circumstances would make return or destruction infeasible?
  - If return or destruction infeasible, protections of agreement must continue indefinitely

What is Not Required to Be Addressed in a Business Associate Agreement?

- Ownership of PHI
  - HIPAA and HITECH focus on use, disclosure, security
- Location of PHI
- Liability/indemnification between the parties
- Extent of covered entity oversight

EU Health Data in the Cloud

Daniel Cooper

A Key Period in EU Cloud Regulation

New measures rolling out

- New standards for cloud data protection (e.g. ISO/IEC 27018)
- E-Identification and Trust Services (eIDAS) Regulation
- Cybersecurity Directive (2013)

New laws being debated

- General Data Protection Regulation (GDPR)
- Network and Information Security (NIS) Directive

eHealth and cloud computing as EU strategic priorities

- Creation of the eHealth Network by the Cross-Border Healthcare Directive (2011/24/EU)
- Allocation of significant EU funding for eHealth projects

EU Cloud Privacy Rules Today

"Health Data"

- **Undefined term in the DPD**
- **Article 29 Working Party says that it comprises:**
  1. Data that is clearly medical in nature (*e.g.,* diagnostic notes), and any conclusions or opinions about a person's health status
  2. Raw test/sensor data that can be used in itself or in combination with more data to draw conclusions about current or future health status
  3. Other data which can reasonably be used to infer a person's health status (e.g., membership of Alcoholics Anonymous)

Regulation of Health Data Under the DPD

- **Unlike "normal" personal data, any collection or use is prohibited, unless an exception applies**
- **Main exceptions:**
  - Confidential medical use
  - Explicit consent
  - Vital interests
  - Employment purposes
  - Domestic use only, or made public by data subject
  - Legal claims
  - Public interest national laws
- **Otherwise, regulated the same way as "ordinary" personal data**

National Distinctions: England

- **Strict NHS policies and contracts go beyond DPD requirements, *e.g.*:**
  - Data from dead patients is also protected
  - Vendors must comply with "Information Governance Toolkit", imposing high data protection standards
  - NHS England pushing for all NHS bodies to use secure email solutions that meet NHS standard (ISB 1596) by 2016.
- **Some inconsistency between policies regarding storage of data within England**
  - Most recent: "*there is no Department for Health policy stating that patient information must be held in England*"
  - Earlier NHS England policy not amended or revoked, but scope is limited.
- **NHS is setting up "Accredited Safe Havens" (ASHs)**
  - ASHs are intermediaries handling patient data for secondary uses (linking datasets, anonymising data, *etc.*); main example is HSCIC, which produces NHS statistics.
- **Previously overemphasised "duty to keep private"; now promoting "duty to share"**

National Distinctions: Belgium

- **Pre-2014, hospital laws prevented off-site patient record storage – but not any more**
  - Articles 20 and 25 of the *Loi coordonnée sur les hôpitaux et autres établissements de soins* of July 10th, 2008
  - Amended in April 2014 to remove the restriction:

*« il faut, entre autres, tenir à jour pour chaque patient un dossier médical . . . conservé **à** l'hôpital»*

*« il faut, entre autres, tenir à jour pour chaque patient un dossier médical . . . conservé **par** l'hôpital»*

    - Subject to ensuring compliance with general data protection and medical secrecy laws, hospitals can now use cloud providers, even for patient records.

National Distinctions: France

- **2006 Decree requires services offering patient data storage to be certified by the *Agence des Systèmes d'Information Partagés de Santé* (ASIP Santé)**
  - Certification process reviews the storage provider's model contracts, financial health, technology, ethical governance, and security measures
  - The provider's sub-contractors must also be declared if they have access to the stored data
  - The provider must designate a doctor "in charge" of hosting the data
  - Certification renewal (after 3 years) requires external audit
- **French law also prohibits:**
  - Use of the patient data for purposes other than those for which the data was provided to the storage provider
  - Retention of copies once the contract has ended

Summary: Important Features for Compliance

- **Ease of retrieval, amendment and deletion**
- **Access controls and logging**
- **Encryption**
- **Geo-location (knowledge of which country the data is in)**
- **Model Clauses (or other mechanism for lawful data export)**
  - Emerging rules for processor BCRs
- **Detailed contract (with strong processor guarantees)**
- **Purpose limitation (*e.g.* no scanning of files for advertising)**
- **Transparency**
- **Reliability**
- **Ability to customize content or preserve metadata to meet national requirements**

Privacy Reform

- **The DPD is due to be replaced by a General Data Protection Regulation (GDPR)**
  - However, the legislative process has been slow
  - Even though aim is to achieve greater harmonisation of data protection rules in the EEA, countries have been pushing for freedom to introduce national health-specific rules
  - Many rules (and sanctions) could become more onerous
    - Use of a compliant cloud provider important aspect of compliance strategy

Security

Main legal obligation comes from the DPD (Article 17(2))

Sector-specific laws at the national level

Unauthorized access to computers/electronic data is a criminal act

Electronic signing and authentication are governed under the EU's E-Signature Directive (being replaced by the new eIDAS Regulation (910/2014))

+ Network and Information Security (NIS) Directive

(legislative proposal still being debated)

Security

- **Not just law, but also essential for risk management**
- Industry standards and best practices, *e.g.*:
  - ISO/IEC 27001
  - Industry standard data disposal procedures and wiping solutions
- Example best practices:

Physical	Logical
• Strict access controls • Biometric scanning • Video surveillance • Redundant power supplies from separate providers • Battery & diesel backup generators • Climate control • Fire prevention and suppression	• Strong encryption • Security monitoring • Threat and vulnerability management, • Access control, file/data integrity checks and records • Two-factor authorization • Intrusion detection software • Incident response teams/procedures • Anti-malware • Secure edge routers, firewalls

Further Changes on the Horizon?

The European Commission has a longstanding interest in eHealth and mHealth

- "Action plans" on eHealth adopted in 2004 and 2012;
- Currently taking (non-legislative) policy actions, e.g.:
  - Funding under the Horizon 2020 program and the 3rd Health Programme;
  - Conducting multiple studies
    - A key interest is interoperability (allowing cross-border healthcare and common regulatory framework allowing IT to be used throughout EU)
  - mHealth Green Paper (2014) re. mHealth's potential

So far, no specific legislative proposals; presumably waiting for implementation of NIS Directive, GDPR and eID Regulation

Conclusion

- **We are seeing a gradual, but perceptible, shift to reliance upon cloud arrangements for handling health information, as "cloud" becomes a more familiar.**
  - Where actual legal blocks are in place, they are being removed (*e.g.* Belgium last year)
- **Legislative and policy developments continue to influence how cloud services are offered, with further changes on the horizon. Both EU and national level developments continue to be highly relevant.**
- **General Data Protection Regulation and NIS Directive are hoped to bring even greater trust in cloud providers – *e.g.* mandatory data breach reporting.**

Commercial Considerations

Lee Tiedrich

Data Can be a Valuable Asset

"The insights from big data have the potential to touch multiple aspects of health care: evidence of safety and effectiveness of different treatments, comparative outcomes achieved with different delivery models, and predictive models for diagnosing, treating, and delivering care. In addition, these data may enhance our understanding of the effects of consumer behavior, which in return may affect the way companies design their benefits packages."

Source: "*Why Health Care May Finally Be Ready for Big Data*,"
by Nilay D. Shah and Jyotishman Pathak
Harvard Business Review, December 3, 2014

Contractual Protection of Data

- **Confidentiality provisions can provide protection and help maintain trade secret status of customer data**
- **Contractual provisions can protect ownership of customer data**
- **Contractual provisions can limit the service provider's right to use customer data**
  - Service provider may be limited to using the customer data to provide the services to the customer during the term of the agreement
  - Service provider may be prohibited from using the data to generate other data for its own use about the use of the services, including in a de-identified form

Defining Customer Data

- **"Customer Data" does not need to be limited to PHI or PII**
- **Some Possible Sources of Customer Data**
  - Data provider by the customer to the service provider
  - Data the service provider collects, processes, analyzes or generates as a result of providing services to customer
  - Metadata (e.g., data about data) from the use of the services
  - Derivatives, reports, compilations, aggregations, summaries and analysis

Quality and Availability of Service

- **Privacy and Data Security Provisions**
- **Service Level Terms or Agreements (e.g., “SLAs”)**
  - Service level commitments and standards
  - Service level credits and/or other remedies for failure to meet SLA terms
- **Customer Data Back-up Requirements**
- **Disaster Recovery Plan and Services**
- **Reducing Risk of Viruses and Other Malicious Code**

Provision of Services

- **Location of Services**
  - Data privacy and security laws vary among jurisdictions
  - Specifying jurisdiction in which servers are located can reduce risk of incurring regulatory obligations without notice
- **Subcontracting**
  - Under what circumstances is it permitted?
  - Responsibility for subcontractor's acts and omissions
  - Require that certain terms be included in the subcontract
- **Security Audits**

Transition to a New Provider

- **Transitioning Possession of Customer Data**
  - Customer will need customer data
  - Service provider should delete customer data to the extent permitted by law after it is provided to customer
- **Transition Services**
  - Duration of services
  - Nature of services
- **Software/Technology Escrow Services**
  - Will services be difficult to replace even with transition period?
  - Release conditions

Legal Protections

- **Representations and Warranties**
- **Remedies**
  - Liability Limitations and Exceptions
    - Failure to meet SLA requirements
    - Other breaches and liabilities, including data security breaches
  - Indemnification
  - Injunctive Relief

Insurance Coverage for Cloud-Related Liabilities

Georgia Kazakis and Scott Levitt

Overview

- Loss or liability
  - Who pays?
  - Contractual risk spreading or shifting (indemnity agreements, insurance policies)
- Structure for thinking about risk & insurance
  - How a hypothetical risk might unfold
  - Role and applicability of insurance
    - Categories or type of loss
    - Identification of triggering event
    - Barriers to coverage

How a Hypothetical Risk Might Unfold

- Breach of your system that compromises your cloud computing
  - employee laptop is stolen and hacker gains access to cloud computing services
- Breach of your cloud provider's network
- Cyber risks tend to unfold in layers and often involve deeper penetration and proliferation
  - Weeks later employee innocently opens email purportedly from IT department which launches malware

Role and Applicability of Insurance Coverage

- Does insurance apply? What insurance applies? How does it apply? Can I rely on “traditional covers”? Do I need cyber insurance?
- Surprising sources of coverage under traditional policies (CGL, commercial property, D&O, E&O, crime, etc.)
- Cyber risk insurance not a panacea but necessary
- Potential roadblocks may exist

The Coverage Analysis: Categorize the Risk to Figure Out What Policies Apply

- 2 general categories of risk or loss:
  - risk that causes loss to the enterprise itself (e.g., destruction of data) (“first party insurance”)
  - risk that causes loss to a third party to whom the enterprise may be liable (e.g., negligence) (“third party liability insurance”)
- Cyber events (unlike non-cyber world events) often implicate both types of loss

First-party Losses Potentially Implicated

- costs associate with loss of e-health data
- costs to change account numbers
- costs to manage bad publicity
- loss to business income
- data and systems restoration expenses
- costs associated with extortion demands including ransom payments

Third-Party Losses Implicated

- Lawsuits from customers alleging violation of privacy, damages arising from identify theft like lost time at work or mental anguish

- Lawsuits and other claims by regulatory agencies

Coverage Analysis: Identifying the Triggering Event

- the nature of the triggering event will direct you to the applicable policies/coverages
- some triggering events and corresponding coverages:
  - has a third party to whom you may be liable sustained property damage or bodily injury (CGL)
  - has a third party's privacy been invaded (CGL)
  - have you suffered loss to your own property (property policy)
  - has your business been interrupted (BI or CBI under property policy)
  - have you suffered a loss of money or other property due to the dishonest act of an employee (crime policy)
  - has another party suffered loss due to the wrongful act of the company or its
  - directors or officers (e.g., failure to maintain adequate security measures) (D&O)
  - has a loss resulted from an error in the delivery of your professional services (E&O)
  - has a claim or lawsuit been filed (claims made vs occurrence-based policies)
  - has a government investigation been launched (D&O)

Coverage Analysis: Identify Potential Coverage & Challenges to Coverage

- Commercial General Liability (CGL) Policies
  - Pre-5/1/14 policies – maybe (an intellectual feast for coverage litigators)
  - Post-5/1/14 policies – maybe not:
    - New ISO exclusion (approved in 40+ states) for loss arising out of "any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information"
- Crime Policies
  - Traditional focus on tangible property, money & securities; may exclude computer fraud
- Property Policies
  - "Physical injury to tangible property"; "loss of use of tangible property that is not physically injured"
- Commercial Property Policies
  - "direct physical loss of or damage to Covered Property"
- D&O
  - most exclude claims alleging violations of privacy
- E&O
  - data breach loss from professional services that are technical in nature

Sources for Potential Coverage of Cloud-Related Risks

- **Evaluate Cyber Coverage**
  - Typical Cyber Coverage Grants
    - Network liability
    - Electronic media liability
    - Technology errors & omissions
    - Business income loss/dependent business income loss
    - Data/Network Restoration costs (“digital asset” coverage)
    - Public relations/crisis management expenses
    - Costs of mandatory (and sometimes voluntary) notifications
    - Credit monitoring costs
    - Forensic investigation expenses (often sub-limited)
    - Extortion threat (denial of service attack)
    - “PCI/DSS” Loss – fines, contractual assessments under payment card processing agreements due to failure to protect payment card information
    - Regulatory proceeding legal expenses
    - Sometimes – regulatory fines and “consumer redress funds”

Practical Tips on Preparing For An Incident

- **Evaluate "Other People's Insurance"**
  - Ecosystem of risk-related contractual agreements other than insurance
    - Contracts with vendors and suppliers
    - Contracts with customers, other service recipients
  - Conduct systematic review of:
    - Indemnity provisions
    - Insurance procurement provisions
      - Adequate specification of cyber insurance risks
      - Limits issues
      - Additional/named insured endorsements vs. loss payee endorsements vs. certificates of insurance

Cyber Coverage – Lessons from the Big-Claim Trenches (1)

- Ain't no limits high enough
  - "Cyber attack risk requires $1bn of insurance cover, companies warned" – Gina Chon, Financial Times (2/18/15)
  - BUT "maximum amount of cyber insurance that is currently available is $500m, although most companies have difficulty obtaining more than about $300m in coverage"– id.
  - PCI sublimit issues

- **UNDERWRITING LESSONS:**
  - Highest deductible you can afford,
    - highest limits you can buy
      - then shop for more.
  - Understand "other people's insurance"

Cyber Coverage – Lessons from the Big-Claim Trenches (2)

- Mind the gap, please
  - "Named perils" vs. "all-risks" structure
  - Coverage "modules"/restaurant menu marketing
  - Overlooked cyber risks
    - E.g., "internet of things" exposures
  - Underlooked/underinsured cyber risks
  - Overinsured cyber risks?

- **UNDERWRITING LESSONS:**
  - Study dovetailing language
    - plug the cracks between the modules
  - Think creatively about the insured's cyber exposures
    - match the modules to the exposures
    - match the limits to the exposures

Cyber Coverage – Lessons from the Big-Claim Trenches (3)

- Timing is everything
  - Network intrusions are latent injuries – may predate their discovery by months, years.
    - But retro date provisions keyed to "interrelated wrongful acts," not discovery
  - Prior knowledge exclusions & 20/20 hindsight
  - Unreported "circumstances"
    - Incident seemingly too trivial to notify –> major breach after expiration of "discovery period"

- **UNDERWRITING LESSONS:**
  - Retro date at least one year before inception date
  - Study "interrelated wrongful acts" definition (may link new major breach to prior minor one)
  - Study all "prior [knowledge/loss/claim]" exclusions
  - Study representation and knowledge imputation clauses
  - Study application form's "boilerplate" (may not square with policy's representation/imputation language)

Questions?

COVINGTON

BEIJING BRUSSELS LONDON LOS ANGELES NEW YORK SAN FRANCISCO
SEOUL SHANGHAI SILICON VALLEY WASHINGTON

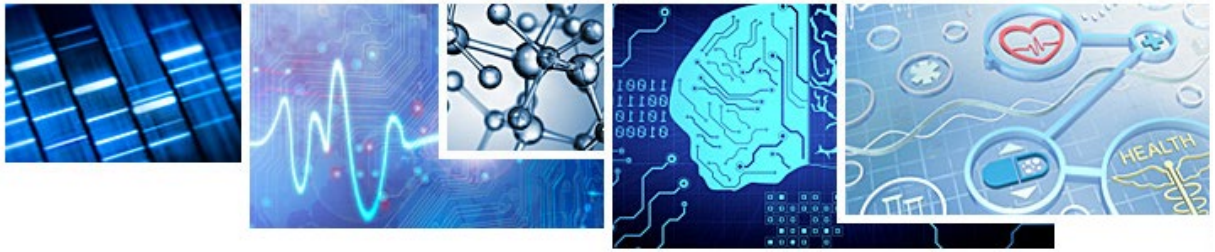
www.cov.com

Visit our Blog at www.CovingtonEHealth.com

COVINGTON eHEALTH

DEVELOPMENTS AND TRENDS IN DIGITAL HEALTH, eHEALTH AND HEALTH IT FROM COVINGTON & BURLING LLP

HOME ABOUT US AUTHORS CONTACT



Moving to the Cloud: Some Key Considerations for Healthcare Entities

By Paige Jennings, Anna Kraus, Ramy Ramadan and Lee Tiedrich on April 2nd, 2015

Healthcare providers, health plans, and other entities are increasingly utilizing cloud services to collect, aggregate, store and process data. A recent report by IDC Health Insights suggests that 80 percent of healthcare data is expected to pass through the cloud by 2020. As a substantial amount of healthcare data comprises "personal information" or "protected health information" (PHI), federal and state privacy and security laws, including the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, raise significant questions for healthcare providers and health plans utilizing the cloud in connection with such data. Such questions include whether HIPAA requirements extend to cloud providers, how and if entities storing health data on the cloud will be notified in case of a breach, and whether storage of data overseas by cloud providers triggers any additional obligations or concerns.

Continue Reading

Presenter Profile: Daniel Cooper

Daniel P. Cooper
Partner
London
dcooper@cov.com

Daniel Cooper advises clients on information technology regulatory issues, particularly data protection, e-commerce and data security matters.

Mr. Cooper regularly assists leading technology companies, including social networking sites, online content and entertainment providers, and e-shopping sites, on their European and global compliance strategies. He also has deep experience with the regulation of mobile and e-health technologies. In addition, Mr. Cooper is known for his ability to guide clients through the issues arising from data breach incidents, and has advised a number of high-profile clients in this area. Mr. Cooper co-authored the data protection standard that governs organized sport.

Mr. Cooper is dual-qualified in the United States and United Kingdom, and has been appointed to the advisory and expert boards of privacy NGOs and agencies, such as Privacy International and the European security agency, ENISA.

For more details please visit http://www.cov.com/dcooper/.

Presenter Profile: Georgia Kazakis

Georgia Kazakis
Partner
Washington
gkazakis@cov.com

Georgia Kazakis uses innovative and creative non-litigation solutions, combined with litigation advocacy, to obtain successful outcomes for her policyholder clients in insurance coverage disputes. She has represented policyholders in coverage disputes before federal and state courts, including disputes over coverage for underlying environmental, asbestos, intellectual property, construction defect, employment practices, errors and omissions, defamation, securities claims and cyber risks. She has developed a particular expertise in construction defect litigation, and has handled multi-party construction defect coverage disputes for a variety of clients, ranging from hospitality chains to pharmaceutical companies. She also has extensive experience representing policyholders in disputes arising under first-party property policies, including coverage for physical damage, extra expense, business interruption and contingent business interruption losses resulting from natural disasters and other perils; disputes arising under crime/fraud, fidelity bond, and professional liability policies; and disputes involving the reconstruction of missing policies. By combining creative strategic vision, trial experience and skilled case management, zealous advocacy for her clients' positions, and an understanding of the practical considerations affecting insurance dispute resolutions, Ms. Kazakis has successfully resolved high-profile coverage disputes, recovering over $150 million arising from a variety of claims and for various clients.

Ms. Kazakis also has an active non-litigation practice. She has assisted clients with policy placements, renewals, and wording modifications, advised clients on the formation of bond facilities for appeals, and has negotiated and mediated favorable settlements on behalf of clients concerning a variety of claims, including "long tail" claims.

For more details please visit http://www.cov.com/gkazakis/.

Presenter Profile: Anna Kraus

Anna D. Kraus
Of Counsel
Washington
akraus@cov.com

Anna Durand Kraus is co-chair of the firm's Health Care Industry group and has a multi-disciplinary practice advising clients on issues relating to the complex array of laws governing the health care industry. Her background as Deputy General Counsel to the U.S. Department of Health and Human Services ("HHS") gives her broad experience with, and valuable insight into, the programs and issues within the purview of HHS, including Medicare, Medicaid, fraud and abuse, and health information privacy.

Ms. Kraus regularly advises clients on Medicare reimbursement matters, particularly those arising under Medicare Part B and the Medicare Part D outpatient prescription drug benefit. She also has extensive experience with the Medicaid Drug Rebate program. She has assisted numerous pharmaceutical and device manufacturers, health care providers, pharmacy benefit managers, and other health care industry stakeholders to navigate the challenges and opportunities presented by the Affordable Care Act.

Ms. Kraus is also a trusted adviser on health information privacy issues, including those arising under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Clinical and Economic Health ("HITECH") Act. Her background in this area dates back to the promulgation of the original HIPAA privacy regulations.

For more details please visit http://www.cov.com/akraus/.

Presenter Profile: Scott Levitt

Scott J. Levitt
Special Counsel
Washington
slevitt@cov.com

Scott Levitt has over fifteen years of experience in recovering insurance proceeds for policyholders. He has represented numerous corporate insureds in virtually every type of insurance coverage claim, including cyber-risk, mass tort, asbestos, silica, mixed dust, environmental, product liability, employment discrimination, errors and omissions, first-party losses, and employee dishonesty. Mr. Levitt has successfully represented policyholders in insurance recovery matters in federal and state trial and appellate courts around the US, as well as in mediation and international and domestic arbitrations. Mr. Levitt's practice often involves negotiating settlements outside of litigation on behalf of his policyholder clients.

For more details please visit http://www.cov.com/slevitt/.

Presenter Profile: Lee Tiedrich

Lee J. Tiedrich
Partner
Washington
ltiedrich@cov.com

Lee Tiedrich brings together an undergraduate education in electrical engineering and over twenty years of legal experience to assist clients on a broad range of intellectual property and technology transaction matters. She has been recognized in *Legal 500* as a Leading Lawyer for patent licensing and transactions for several years and is recommended in *Legal 500* for her "ability to identify critical issues" and her "extremely strong work ethic." Ms. Tiedrich is registered to practice before the United States Patent and Trademark Office.

Ms. Tiedrich has extensive experience negotiating complex intellectual property acquisition, licensing, and development agreements, including software and online services agreements, mobile app agreements, patent licenses, content and media agreements, cloud services and data agreements, branding and trademark license agreements, intellectual property settlement agreements, and hardware development agreements. She also regularly counsels clients on strategic issues, such as developing and maintaining intellectual property portfolios and evaluating and addressing intellectual property-related assets and risks in connection with mergers, acquisitions, investments, capital markets transactions and other transactions. Her work spans several industries, including ehealth, communications and media, life sciences, consumer products, and clean energy. She has experience counseling both private and public companies, as well as venture capital firms and corporate venture groups in their investments.

Ms. Tiedrich co-chairs the firm's Diversity Committee.

For more details please visit http://www.cov.com/ltiedrich/.