proofpoint.

GUIDE

Guide to Global Digital Compliance for Regulated and Highly Litigious Industries

Overview

Regulated and highly litigious industries face a raft of complex rules that cover how they approach digital communications. As a stakeholder in your businesses risk, you need to keep track of:

- What rules apply to your organization
- How those rules are changing amid an evolving regulatory and litigation landscape
- Whether those rules affect how you manage data privacy, industry-specific requirements, digital communications and long-term data storage

At the same time, your compliance risks keep growing. Compliance was never easy, even when businesses relied mostly on email to connect. Since then, the rise of new communications channels has made it even more complex. Video, collaboration apps and social media networks are all staples of business communications today. Trying to apply the old compliance playbook to this new realm leaves teams uncertain and exposed.

It's all adding up to more noise for compliance officers. According to the 2022 Cost of Compliance report, organizations across the globe face an average of 246 regulatory alerts per day. At 64,152 total alerts, 2021 was the second-noisiest year since 2008.[1]

At the same time, how you capture, store and supervise business communications is more critical than ever. The United States Securities and Exchange Commission (SEC) has set its sights on social media fraud within financial services. The agency has also scrutinized organizations for the way they collect and retain their employees' electronic communications.

Today's workers use everything from collaboration tools such as Slack and Microsoft Teams to social channels such as Twitter or LinkedIn. In the case of social channels, they may access them directly or through third-party apps. Some of your teams may also use business apps with built-in email or chat features. In the face of strict enforcement, compliance teams like yours must carefully manage all of this content. This means being having visibility into what your users are communicating, retaining that content and in some cases, controlling it.

And the risks and rules extend further. Even if you are not in a highly regulated industry, if your business faces frequent litigation, you are also subject to specific rules. An end-to-end audit trail is key for responding to e-discovery evidence requests and complying with relevant rules. ESG recently estimated that the average e-discovery costs for a business total $1.5 million.[2] And more than a third of businesses "believe [it] is getting harder" to satisfy e-discovery requests.

If that weren't challenging enough, consumer data protection has come to the fore. Lawmakers around the world have enacted a wave of data protection laws, and they continue to look more closely at data privacy issues. As a result, you must minimize risk when it comes to handling and storing consumers' personal data.

These challenges and costs can increase your risk. This guide lays out global regulations for digital communications. It lists the rules by industry and by country for easy lookup. We also cover data privacy regulations that apply across all industries.

[1] Thomson Reuters. "Cost of Compliance 2022: Competing Priorities." July 2022.

[2] Proofpoint and ESG. "E-Discovery Market Trends and Challenges." August 2021.

Table of Contents

Privacy Regulations

In recent years, the number of regulations protecting personal data has grown sharply. These regulations are relevant across verticals and sectors. Plus, they apply regardless of where your business is located. If you sell goods or provide services to consumers within the jurisdictions covered, they apply.

Privacy

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	SB-1121 California Consumer Privacy Act of 2018	Requires that businesses disclose to California residents, upon request, what categories of information they have collected about them and for what purpose. Businesses must be able to provide this information for the 12-month period preceding the request. Businesses must notify consumers at collection what categories of information they collect and the purposes for which they use this information. If a business sells consumer information, the notice must include a “do not sell” link. Consumers may request that businesses and their service providers delete the personal information they collected from you, and the business must comply unless there exists a qualified exception.
	Colorado Privacy Act	Consumers may opt out of the processing of their personal data for targeted advertising, sale or other profiling decisions. Controllers must provide a “clear and conspicuous” method to exercise the right to opt out of the sale of data. Consumers have the right to confirm whether a controller is processing their data and to access that data. Consumers have the right to correct inaccuracies in their personal data and to delete their personal data. Up to two (2) times per calendar year, consumers have the right to obtain their personal data in a portable and readily usable format that allows the consumer to transmit the data to another entity “without hindrance.”
	Virginia Consumer Data Protection Act (VCDPA)	Virginia residents are afforded the right to confirm whether or not a controller is processing their personal data and to access such personal data; to correct inaccuracies in their personal data; to delete personal data provided or obtained by them; and to obtain a copy of personal data that they previously provided to the controller in a portable and, to the extent technically feasible, readily usable format. They are also afforded the right to opt out of the processing of their personal data for purposes of targeted advertising, sale, or profiling in support of legal or other decisions.

COUNTRY/REGION	REGULATION	DESCRIPTION
Canada 	Personal Information Protection and Electronic Documents Act (PIPEDA)	The Act gives an individual the right to know why an organization collects, uses or discloses their personal information, and the right to expect that the organization will do so reasonably and appropriately, and not for any purpose other than that to which they had consented. It also requires organizations to obtain consent when they collect, use or disclose the information of individuals, to collect information by fair and lawful means and to have personal information policies that are clear, understandable and readily available.
European Union 	General Data Protection Regulation (GDPR)	All data processing must take place in accordance with seven protection and accountability principles: 1. Lawfulness, fairness and transparency—Processing must be lawful, fair and transparent to the data subject. 2. Purpose limitation—You must process data for the legitimate purposes specified explicitly to the data subject when you collected it. 3. Data minimization—You should collect and process only as much data as absolutely necessary for the purposes specified. 4. Accuracy—You must keep personal data accurate and up to date. 5. Storage limitation—You may only store personally identifying data for as long as necessary for the specified purpose. 6. Integrity and confidentiality—Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (for example, by using encryption). 7. Accountability—The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.
Hong Kong 	Personal Data (Privacy) Ordinance (PDPO)	Ensures that personal data is collected on a fully informed basis and in a fair manner, with due consideration towards minimizing the amount of personal data collected. Once collected, the personal data should be processed in a secure manner and should only be kept for as long as necessary for the fulfillment of the purposes of using the data. Use of the data should be limited to or related to the original collection purpose. Data subjects are given the right to access and make corrections to their data.

Digital Communications Regulations

Financial Services

Policy and Procedures

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	FFEIC Social Media Guidance	Draft social media policy tailored to the organization's use case for social media and incorporating goals and objectives.
	SEC Investment Advisers 206(4)-7	It is unlawful for an investment advisor to provide investment advice unless RIA firms have adopted and implemented written compliance policies and procedures reasonably designed to prevent violations of the Investment Advisers Act.
	SEC Investment Advisers Marketing Final Rule	When providing a testimonial or endorsement on a social media platform, an adviser must clearly and prominently label the testimonial or endorsement as being a paid testimonial or endorsement.
	FINRA Notice 10-06 & 11-09	Adopt policies and procedures to ensure those who participate in electronic communication, including social channels, for business purposes are appropriately supervised, have the necessary training and background to engage in such activities, and do not present undue risks to investors.
	FINRA Notice 07-59	Suggests that members consider taking steps "to reduce, manage or eliminate potential conflicts of interest, to prevent electronic communications between certain individuals/groups or monitoring communications as required by FINRA rules," including communications across social channels.
	FINRA Notice 17-18	Reminds financial institutions that they must train and educate their associated persons regarding the difference between business and non-business communications.
	FINRA Notice 20-16	Advises firms transitioning to a remote work environment to implement supervisory practices and procedures that are reasonably and appropriately designed for this business model. Suggests providing employees additional guidance on maintaining confidentiality of firm and customer information in remote work environments and using new communication tools to replicate traditional "line of sight" supervision in a remote work environment as well as implementing additional central monitoring and reviews of supervisory activities.
	Bank Secrecy Act	Financial institutions must have compliance programs, training and internal controls to ensure effective risk management and adherence to recordkeeping and reporting requirements, including for social media and electronic communications.

COUNTRY/REGION	REGULATION	DESCRIPTION
	Graham-Leach-Bliley Act (GLBA)	Requires financial institutions to develop a written information security plan that describes how the company is prepared for and plans to continue to protect clients' private personal information, including securing and monitoring communications and social channels to ensure data leakage does not occur.
	Federal Trade Commission (FTC) Standards for Safeguarding Customer Information Final Rule	Requires financial institutions to develop, implement and maintain an information security program, identifying reasonably foreseeable risks to the security, confidentiality and integrity of customer information that could result in the unauthorized disclosure or other compromise of the information. The financial institution must then implement safeguards to control the risks identified and regularly test or monitor the effectiveness of key controls.
Canada 	IIROC Notice 11-0349; IIROC Dealer Member Rules 29.7	Requires policies and procedures to avoid misleading or false statements to clients.
United Kingdom 	FCA SYSC 10.2	Firms must take reasonable steps to ensure that ethical walls remain effective and are adequately monitored, across all communications and social media channels.
Hong Kong 	Securities and Futures Commission (SFC), Advertising Guidelines Applicable to Collective Investment Schemes Authorized Under the Product Codes, Applications of the Advertising Guidelines	Guidelines intended to apply to all forms of product advertisements, including the internet, interactive voice message systems, communications and social channels, to which advertising guidelines should be applied.
	Securities and Futures Commission (SFC), Corporate Regulation Newsletter, March 2016	Cautions against using social channels such as Weibo, Facebook or Twitter to disclose time- or business-sensitive information, and cautions firms that messages sent need to be accurate, clear, and balanced.
	Securities and Futures Commission (SFC), Regulatory Technology Watch, COVID-19 Advisory	As work-from-home arrangements were activated, employees turned to personal messaging applications (for example, WhatsApp and WeChat) in order to discuss business issues with their regular bank contacts. All business can be recorded for audit and compliance purposes to ensure banks' compliance with regulatory reporting and other regulatory requirements.
Australia 	Australian Securities & Investments Commission (ASIC), Information Sheet 269, Discussing Financial Products and Services Online	Persons who discuss financial products and services online are legally obligated to publish content that is accurate and balanced. If you carry on a business of providing financial services online, you must hold an AFS license unless exempt.

Content

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	FFEIC Social Media Guidance	Create a content plan and defined review and approval process.
	FINRA 2210 and 2220	Communications with the public must be fair, balanced, and not misleading.
	FINRA Regulatory Notice 15-50	Amends FINRA Rule 2210 to require member firms' websites to include a readily apparent reference and hyperlink to BrokerCheck on affiliated web pages.
	Fair Debt Collection Practices Act (FDCPA)	Debt collectors may not communicate on social media with a person in connection with the collection of a debt if the communication is viewable by the general public or the person's social media contacts. If a debt collector sends text messaging, email or other electronic communications, recipients must be able to easily opt out of receiving those communications.
	FDIC Social Media Consumer Compliance Risk Management Guidance	FDIC or NCUA members who advertise deposit or share insurance on social media must include "Member FDIC," "Federally insured by NCUA," and font must be legible.
	Electronic Fund Transfer Act, Regulation E	Customers must receive all required disclosures, and disclosures must be "clear and conspicuous" and "readily understandable." Disclosures may be made electronically, but electronic disclosures must be in a retainable form.
	Fair Credit Reporting Act	Sets standards for communication, including on social media, using eligibility information, responding to disputes, and collecting medical information in connection with loan eligibility. Collectors of screening data from social media must take steps to ensure the accuracy and relevance of the information and must certify that the information won't be used in a way that violates EEO laws.
Canada 	IIROC Dealer Member Rule 29.7	Requires pre-approval of social media content.

Supervision

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	FFEIC Social Media Guidance	Implement technology to monitor activity and ensure compliance with the established company policy.
	FINRA Notice 10-06 and 11-39; 2210	Supervise static content and interactive communications.
	FINRA Regulatory Notice 11-39	Supervise business communications through personal devices.
Canada 	IIROC Rule 29.7; IIROC Dealer Member Rule 1300.1	Requires monitoring of content delivered to social networks, as well as having a tool in place to monitor social media activity for non-compliant trigger words or phrases; communications that constitute recommendations must be subject to due diligence.

COUNTRY/REGION	REGULATION	DESCRIPTION
United Kingdom 	FCA, FG15/4: Social Media and Customer Communications	Clarifies that if a communication includes an invitation or an inducement to engage in financial activity, it is considered a "financial promotion" and is subject to financial promotions guidelines. The FCA's social media guidelines require firms to demonstrate that they have the processes and systems in place to pre-approve all communications sent via social media channels.
Switzerland 	Swiss Financial Market Supervisory Authority (FINMA) Operational Risks at Banks Circular 2008 (FINMA-Circ. 08/21)	Banks must diligently select, supervise (including monitoring content of staff communications send on instant messaging, unified communications, social networks, and so on), and train staff and third parties who have access to client-identifying data.
Singapore 	MAS Technology Risk Management Guidelines, Article 11.1.5	Measures should be implemented to prevent and detect the use of unauthorized internet services that allow users to communicate or store confidential data. Examples of such services include social media, cloud storage and file sharing, emails, and messaging applications.
	MAS Guidelines on Risk Management Practices—Internal Controls, Article 3.5.1	An institution should have adequate management information systems (MIS) for effective management and control of all aspects of its operations, including identifying technology that can monitor, supervise, capture, archive, and reproduce content sent across multiple communications and social channels.
Australia 	Australian Securities and Investments Commission (ASIC), Corporations Act, Section 912	Have procedures and systems to monitor employees with potential conflicts of interest so they cannot communication with each other across all communication and social channels.

Archive

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	FFEIC Social Media Guidance	Establish a recordkeeping system to archive activities.
	SEC 17a-3 and a-4	Preserve relevant communications for a period of not less than three years, such that legible, true, complete and current copies of those records can promptly be produced.
	SEC DFA Section 764 and CFTC SEA Section 15F(g) (1)	Daily trading communications, including email, instant messages, phone calls and social media, of security-based swaps and all regulated records to be recorded for the period required by the Commission by rule or regulation.
	FINRA Regulatory Notice 10-06 and 11-09	Every firm that intends to communicate, or permit its associated persons to communicate, through social media sites must first ensure that it can retain records of those communications.
	FINRA Regulatory Notice 11-39	Capture and archive all communications by registered persons on social channels sent through personal devices.
	Investment Advisers Act, Rules 204(2) and 206(4)-1	Ensure that adequate records are kept across all communication and social channels in use.
	Commodity Futures Trading Commission (CFTC), 17 Final Rule, Parts 43, 45 and 49	Daily trading records of the swaps and all related records (including related cash or forward transactions) and electronic communications, including instant messages, for one year. This information needs to be stored safely and in a manner that allows for easy retrieval and review by regulators.

COUNTRY/REGION	REGULATION	DESCRIPTION
Canada 	IIROC Rule 29.7(5)	Retain advertisements and content for a period of two years, and ensure it is readily available for inspection.
	IIROC Notice 0349	Retain records of business activities, financial affairs, consumer transactions and communications, including "Facebook, Twitter, YouTube, blogs and chat rooms" as subject to the IIROC Dealer Member Rules.
United Kingdom 	FCA Policy Statement 08/1	All relevant electronic communications must be retained, including fax, email, Bloomberg mail, video conferencing, SMS, business to business devices, chat and instant messaging.
European Union 	European Securities and Markets Authority (ESMA), MiFID II Article 16(7)	Telephone conversations or electronic communications, including social media, relating to investment services such as the reception and transmission of orders, execution of orders on behalf of clients, and dealing on own account are required to be recorded.
Australia 	Australian Securities and Investments Commission (ASIC), Regulatory Guide 234, Advertising Financial Products and Services (Including Credit): Good Practice	Firms should capture and archive any advertisements, even those on social channels.
International 	IOSCO, Principles for Benchmark-Setting Processes, D.2 and D.3	Benchmark Calculation Agents need to document and keep records of all interactions with submitting parties, audit records of the data used for capturing the Benchmark and records of contracts with the Benchmark and make these available to Supervisory Authorities upon request.

Legal Requirements for Retention and Holds

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	Federal Rules of Civil Procedure (FRCP) 37	(FRCP) 37(e), a party must preserve documents and electronically stored information (ESI) when it reasonably anticipates litigation.

Healthcare

Policy and Procedures

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	Department of Health and Human Services, Health Insurance Portability and Accountability Act (HIPAA)	If there has been a breach of unsecured PHI or ePHI, the organization is obliged to provide notification of the breach to affected individuals, the Secretary of Health and Human Services, and in certain circumstances, to the media. Notification must occur within 60 days of the incident.
United Kingdom 	National Health Services (NHS)	Any organization that collects, analyzes, publishes or disseminates confidential health and care information must follow the Code of Practice on confidential information. It clearly defines the steps that organizations must, should and may take to ensure that confidential information is handled appropriately.
	Nursing and Midwifery Council (NMC)	NMC members should never put confidential or sensitive information on social networking sites, especially if it identifies patients. Should not accept friend requests from patients, or use social networks to build or pursue relationships with patients or clients, even if they are not in their care. Should not post pictures that have patients in them. Social media should not be used for whistle blowing or raising concerns. Should not discuss work online, especially about patients or colleagues.
	British Medical Association (BMA)	Members must adhere to the same legal and ethical duties of patient confidentiality on social media as in any other setting.
Australia 	Medical Board of Australia, Social Media Policy	Maintains the privacy and confidentiality of patient information. This applies even if the privacy settings used in a particular social medial channel are set at the highest setting (such as for a closed, “invisible” group). Section 133 of the National Law imposes limits on how health services delivered by registered health practitioners can be advertised. These limits apply to all forms of advertising, including through social media and on the internet. For example, the National Law prohibits the use of testimonials in advertising. The Advertising guidelines provide guidance about how the legal restrictions on advertising under the National Law and other relevant legislation apply to social media.
	Australian Medical Association, Guidelines on Social Media as a Joint Initiative of the AMA, NZMA, NZMSA and the AMSA	Doctors have an ethical and legal responsibility to maintain their patients’ confidentiality. This still applies when using any form of online tool, regardless of whether the communication is with other doctors, a specific group of people (for example, ‘friends’ on social networking sites), or the public (for example, a blog). The anonymity potentially afforded online is no excuse for unprofessional behavior. Before putting patient information online… you should inform the patient and gain their express consent, and acknowledge that the consent has been obtained in any online posts… In maintaining confidentiality, you must ensure that any patient or situation cannot be identified by the sum of information available online.
	Therapeutic Goods Administration Social Media Advertising Guide	Unsolicited testimonials for certain products and drugs if posted on social media and appear on the walls of a medical brand page or profile are an immediate violation of Therapeutic Goods Administration (TGA) guidelines in Australia and must be deleted.

Content

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	Department of Health and Human Services, Health Insurance Portability and Accountability Act (HIPAA)	Healthcare firms need to have procedures in place to properly authorize and supervise employees handling PHI and ePHI.
Australia 	Medical Board of Australia, Guidelines for Advertising Regulated Health Services	Practitioners advertising through social media, blogs, and websites should carefully review content regularly to make sure that all material complies with their obligations under the National Law. National Law requires advertising of regulated health services to contain factual information, not to be misleading, and not to contain offers or inducements to the consumer or testimonials.

Archive

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	Department of Health and Human Services, Health Insurance Portability and Accountability Act (HIPAA)	Healthcare firms need to capture, archive, secure, manage and make available the content from communications and social channels from the date of their creation or last effective date for six years, to storing disclosures of PHI or ePHI for three years. Firms are also charged with ensuring PHI and ePHI are securely stored.
	State Governments, The Affordable Care Act (ACA)	Requires organizations to adopt comprehensive recordkeeping practices (for example, health insurance issuers offering individual health insurance coverage including communications and social channels if they are in use) and to maintain records of all claims and notices associated with the internal claims and appeals process for six years. If a consumer completes a qualified health plan (QHP) selection using an agent or broker's internet website, the site is required to maintain related audit trails and records in an electronic format for at least ten years.
	Department of Labor, Employee Retirement Income Security Act (ERISA)	General guidance for record retention of journals, ledgers, checks, invoices, contracts, agreements, vouchers and worksheets, receipts, claim records, applicable resolutions and more. Actual records, not summaries, are required, although electronic versions are acceptable if certain standards for electronic retention are met. Companies planning to use social media need to ensure that their social media records are complete, secure and tamper-proof.

Legal Requirements for Retention and Holds

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	Federal Rules of Civil Procedure (FRCP) 37	(FRCP) 37(e), a party must preserve documents and electronically stored information (ESI) when it reasonably anticipates litigation.

Energy and Utilities

Policy and Procedures

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	Federal Energy Regulatory Commission (FERC), Order 71	Creation of ethical walls between the marketing and transmission functions of vertically integrated companies that distribute natural gas and electricity between states (the "No-Conduit" rule). Ensure that ethical walls are constructed and adhered to, so employees with potential conflicts of interest cannot communicate with each other across all communication and social channels.
	NERC Critical Infrastructure Protection (CIP) Standards, CIP-003-1	Requires the development and management of security management controls to protect critical networks and other assets. Must have the processes and technology in place to prevent data leakage and malware threats via communications and social channels.
	NERC Critical Infrastructure Protection (CIP) Standards, CIP-005-1	Requires the creation of an "Electronic Security Perimeter" that, among other things, must monitor and log access on a 24x7 basis, perform at least annual vulnerability assessments, including on social channels, and document changes in the network.

Archive

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	Department of Energy (DOE), 10 CFR 600.153	Retention of financial records, supporting documents, statistical records, and all other records pertinent to an award for three years, including records across all communications and social channels. These records must be captured and archived in secure WORM storage.
	Federal Energy Regulatory Commission (FERC), Order 717	Communications and social channels need to be retained for five years. If non-public information between transmission and marketing employees is shared, the fact that such an exchange took place must be made public immediately. Regulated firms that violate FERC Order 717 can be subject to a fine of up to $1 million per day for each violation of the order.
European Union 	European Agency for the Cooperation of Energy Regulators (ACER), European Union, REMIT (Regulation on Energy Market Integrity and Transparency)—No. 1227/2011	Record and retain for at least six months electronic communications (including social channels, emails, and instant messaging exchanges) made in connection with any transaction in wholesale energy products.

Legal Requirements for Retention and Holds

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	Federal Rules of Civil Procedure (FRCP) 37	(FRCP) 37(e), a party must preserve documents and electronically stored information (ESI) when it reasonably anticipates litigation.

Pharmaceutical

Policy and Procedures

COUNTRY/REGION	REGULATION	DESCRIPTION
United Kingdom 	Association of the British Pharmaceutical Industry, Code of Practice for the Pharmaceutical Industry 2021, Clause 26.2	States that companies providing information on social media must adhere to all principles set out in the Code, including restrictions on promotional activities. All information provided on social media must be factual, balanced and must not encourage members of the public to ask prescribers to prescribe a specific medicine. It must not constitute the advertising of prescription-only medicines to the public. Companies should not offer advice or information which properly should be in the domain of the doctor or prescriber.
	Association of the British Pharmaceutical Industry, Code of Practice for the Pharmaceutical Industry 2021, Clause 15.5	Email and other electronic communications can be used for promotional purposes only with the prior permission of the recipient. Each email sent by a company should inform the recipient about how to unsubscribe.

Content

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	Food and Drug Administration (FDA), Internet/Social Media Platforms with Character Space Limitations—Presenting Risk and Benefit Information for Prescription Drugs and Medical Devices	Outlines the FDA's policies for online microblog sites (such as Twitter) and paid "sponsored links." Regardless of character space constraints that may be present, firms that make product benefit claims should also incorporate risk information within the same character-space-limited communication. The firm should also provide a mechanism to allow direct access to a more complete discussion of the risks associated with its product.
United Kingdom 	Association of the British Pharmaceutical Industry, Code of Practice for the Pharmaceutical Industry 2021, Clause 26.2	Information on diseases and medicines may be provided to the public over social media so long as it does not constitute advertising of prescription-only medicines. If a company wants to promote a prescription-only medicine via social networks, it must ensure that the audience is restricted to health professionals and that the message is compliant with the Code. If a company facilitates a discussion forum on a third-party website or hosts one of its own, it is likely to be responsible under the Code for the content. Before undertaking such an activity, the company must be confident that it can moderate the site such that the only content to appear complies with the Code.

Supervision

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	Centers for Medicare & Medicaid Services (CMS) Physician Payment Sunshine Act, Final Rule (42 CFR Parts 402 and 403)	Pharmaceutical-related companies are required to report payments and other "transfers of value" made to physicians and teaching hospitals to CMS for inclusion in a publicly accessible database. Firms need to monitor communications and social channels for these payments. CMS may impose a penalty of $10,000 for each failure to report a payment. "Purposeful failure" to report is subject to a fine of up to $100,000 per violation.
United Kingdom 	Association of the British Pharmaceutical Industry, Code of Practice for the Pharmaceutical Industry 2021, Clause 26.5	Companies are obliged to collect adverse events, including monitoring communications and social channels, and report them if appropriate so any interaction must include plans for reviewing the site to meet vigilance requirements.

Archive

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	Food and Drug Administration (FDA), Code of Federal Regulations, Title 21 CFR Part 11	Mandates records of employee use of communications and social channels must be maintained; the content of records; whether signatures are required; how long records must be maintained. Subpart B states that the company's systems must be able to generate accurate and complete copies of records (specified in the predicate rules) in both human-readable and electronic form suitable for inspection, review, and copying by the agency.
	Food and Drug Administration (FDA), Prescription Drug Marketing Act (PDMA)	Recordkeeping requirement associated with marketing and advertising via communication or social channels should be captured and archived.
	Food and Drug Administration (FDA), Fulfilling Regulatory Requirements for Postmarketing Submissions of Interactive Promotional Media for Prescription Human and Animal Drugs and Biologics (Draft)	Firms wanting to use social media need to submit the material posted on social media to the FDA after the event.
	Food and Drug Administration (FDA), Guidance for Internet/Social Media Platforms: Correcting Independent Third-Party Misinformation About Prescription Drugs and Medical Devices (Draft)	Firms must keep records of corrections made should the FDA have questions. Adequate records of social media content must be captured and archived.
	Food and Drug Administration (FDA), Post-marketing reporting of adverse events, 21 CFR 314.80 and 21 CFR 600.8	Correspondence on communications and social channels relating to adverse events needs to be captured and archived for ten years.

Legal Requirements for Retention and Holds

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	Federal Rules of Civil Procedure (FRCP) 37	(FRCP) 37(e), a party must preserve documents and electronically stored information (ESI) when it reasonably anticipates litigation.

Education and Local Government

Policy and Procedures

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	United States Department of Education, 34 CFR Part 99—Family Educational Rights and Privacy Act	Parents of students who attend a school have the right to inspect and review the education records of that student, including electronic records and communications. Each educational agency or institution shall establish appropriate procedures for the granting of parents' requests for access to education records within a reasonable amount of time.
	United States Department of Education, 34 CFR Part 98—Protection of Pupil Rights Amendment	All instructional material – including teachers' manuals, films, tapes, electronic media or supplementary material – which will be used in connection with any research or experimentation program or project shall be available for inspection by the parents or guardians of the children engaged in the program.
	Florida Statute 286: The Sunshine Law on Open Government	Provides that any records made or received by any public agency in the course of its official business are available for inspection, unless specifically exempted by legislature. Public records include not just written documents but photographs, film, audio recordings, digital records and electronic communications.

Archive

COUNTRY/REGION	REGULATION	DESCRIPTION
Australia 	Public Records Act 2002	Public institutions including Universities are required to consistently capture, access, store and manage records as part of normal business practices. These records include but are not necessarily limited to student records, course materials, financial information and external communications including electronic correspondence.

Legal Requirements for Retention and Holds

COUNTRY/REGION	REGULATION	DESCRIPTION
United States 	Federal Rules of Civil Procedure (FRCP) 37	(FRCP) 37(e), a party must preserve documents and electronically stored information (ESI) when it reasonably anticipates litigation.

LEARN MORE

For more information, visit **proofpoint.com**.