

GUIDE TO  
**GLOBAL DIGITAL  
COMMUNICATIONS  
COMPLIANCE**  
FOR REGULATED INDUSTRIES

# TABLE OF CONTENTS

- INTRODUCTION ..... 3**
- FINANCIAL SERVICES ..... 4**
  - Policy and Procedures ..... 4
  - Content..... 5
  - Supervision..... 6
  - Archive..... 7
- HEALTHCARE ..... 8**
  - Policy and Procedures ..... 8
  - Content..... 8
  - Supervision..... 9
  - Archive..... 9
- ENERGY AND UTILITIES ..... 10**
  - Policy and Procedures ..... 10
  - Archive..... 10
- PHARMACEUTICAL ..... 11**
  - Policy and Procedures ..... 11
  - Content..... 11
  - Supervision..... 12
  - Archive..... 12

# INTRODUCTION

Financial services, pharmaceuticals, healthcare, and energy are some of today's most regulated industries. And their compliance risks have only grown as modern business evolves. Your people work in more places, in more ways, across more channels. And you must comply with new rules that govern email, the web, social media, and more. Managing, supervising, and retaining it all has never been more complex—or critical—than ever.

Many regulated companies struggle to:

- Identify where their business communications are taking place
- Ensure that this content is captured and securely archived
- Search and retrieve content for audits quickly and cost-effectively
- Monitor and supervise workers who use these channels

This guide outlines global regulations for digital communications and social channels. It arranges the rules by industry and by country for easy lookup. It also shows how Proofpoint can help you stay compliant.

Proofpoint Digital Compliance is today's most powerful and complete digital compliance solution. It provides end-to-end digital communications compliance. That means you're covered from the moment content is posted to when it is indexed, archived, and retrieved.






Digital Compliance applies your regulatory policies automatically. So can be sure your digital engagement efforts comply with any communications and retention rules. With Digital Compliance, supervising, remediating (revising or removing), and archiving content is easier and less expensive.

No matter what regulations you face, Digital Compliance paves the way for digital engagement and social selling at scale.





# FINANCIAL SERVICES







## POLICY AND PROCEDURES

Country	Regulation	How Proofpoint Addresses Rule
United States 	<p><b>FFIEC Social Media Guidance</b> Draft social media policy tailored to the organization's use case for social media and incorporating goals and objectives.</p> <p><b>SEC Investment Advisors 206(4)-7</b> It is unlawful for an investment adviser to provide investment advice unless RIA firms have adopted and implemented written compliance policies and procedures reasonably designed to prevent violation of the Investment Advisers Act.</p> <p><b>FINRA Notice 10-06 &amp; 11-09</b> 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.</p> <p><b>FINRA Notice 07-59</b> 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.</p> <p><b>FINRA Notice 17-18</b> Reminds financial institutions that they must train and educate their associated persons regarding the differences between business and non-business communications.</p> <p><b>Bank Secrecy Act</b> Financial institutions must have compliance programs, training, and internal controls to ensure effective risk management and adherence to recordkeeping and reporting, including social media communications, requirements.</p> <p><b>Gramm-Leach-Bliley Act (GLBA)</b> 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.</p>	<ul style="list-style-type: none"> <li>• Provides financial services compliance best-practice policy templates for immediate enforcement</li> <li>• Delivers real-time monitoring and supervision to ensure policies are followed; enables firms to identify those who require additional training</li> <li>• End-to-end compliance platform that helps companies follow best practices</li> </ul>
Canada 	<p><b>IIROC Notice 11-0349; IIROC Dealer Member Rule 29.7</b> Requires policies and procedures to avoid misleading or false statements to clients.</p>	
United Kingdom 	<p><b>FCA SYSC 10.2</b> Firms must take reasonable steps to ensure that ethical walls remain effective and are adequately monitored, across all communications and social media channels.</p>	
Hong Kong 	<p><b>Securities and Futures Commission (SFC), Advertising Guidelines Applicable to Collective Investment Schemes Authorized under the Product Codes, Application of the Advertising Guidelines</b> Guidelines intended to apply to all forms of product advertisements, including the internet, interactive voice message systems, communications and social channels to which the advertising guidelines should be applied.</p> <p><b>Securities and Futures Commission (SFC), Corporate Regulation Newsletter, March 2016</b> 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.</p>	
Australia 	<p><b>Australian Securities &amp; Investments Commission (ASIC), Regulatory Guide 234 "Advertising financial products and services (including credit): Good Practice</b> Firms are urged to consider the channel used for advertisement as any such communication needs to be balanced.</p>	







# CONTENT

Country	Regulation	How Proofpoint Addresses Rule
United States 	<p><b>FFIEC Social Media Guidance</b> Create a content plan and defined review, approval process.</p> <p><b>FINRA 2210 and 2310</b> Communications with the public must be fair, balanced, and not misleading.</p> <p><b>FINRA Regulatory Notice 15-50</b> Amends FINRA Rule 2210 to require member firm's websites to include a readily apparent reference and hyperlink to BrokerCheck on affiliated web pages.</p> <p><b>Fair Debt Collection Practices Act (FDCPA)</b> Restricts debt collectors from inappropriately contacting consumers using social media to collect debts.</p> <p><b>Deposit Insurance or Share Insurance</b> Advertising requirement, including on social media, regarding FDIC or NCUA membership and deposit or share insurance. Must include "Member FDIC", "Federally insured by NCUA"; font must be legible.</p> <p><b>Electronic Fund Transfer Act, Regulation E</b> Customers must receive all required disclosures, including on social media, and disclosures must be "clear and conspicuous" and "readily understandable".</p> <p><b>Fair Credit Reporting Act</b> Sets standards for communication, including on social media, using eligibility information, responding to disputes and collecting medical information in connection with loan eligibility.</p>	<ul style="list-style-type: none"> <li>• Provides streamlined approval workflow for stakeholders to pre-approve static content, including profiles and ads</li> <li>• Delivers notifications about content and compliance infractions</li> <li>• Enables organizations to remediate problematic content right away</li> <li>• Provides a library of highly targeted content generated by both internal staff and third parties</li> </ul>
Canada 	<p><b>IIROC Dealer Member Rule 29.7</b> Requires pre-approval of social media content.</p>	

# SUPERVISION

Country	Regulation	How Proofpoint Addresses Rule
United States 	<p><b>FFIEC Social Media Guidance</b> Implement technology to monitor activity and ensure compliance with the established company policy.</p> <p><b>SEC Advisers Act Rule 206(4)-7</b> Prohibits use of testimonials or referrals as part of social media advertisements and promotions.</p> <p><b>FINRA Notice 10-06 and 11-39; 2210</b> Supervise static content and interactive communications.</p> <p><b>FINRA Regulatory Notice 11-39</b> Supervise business communications through personal devices.</p>	<ul style="list-style-type: none"> <li>• Provides financial services compliance best-practice policy templates for immediate enforcement</li> <li>• Delivers real-time monitoring and supervision to ensure policies are followed; enables firms to identify those who require additional training</li> </ul>
Canada 	<p><b>IIROC Rule 29.7; IIROC Dealer Member Rule 1300.1</b></p> <ul style="list-style-type: none"> <li>• Monitor content delivered to social networks</li> <li>• Requires a tool in place to monitor social media activity for non-compliant trigger words or phrases</li> <li>• Prohibits communication that constitute a recommendation.</li> </ul>	<ul style="list-style-type: none"> <li>• End-to-end compliance platform that helps companies follow best practices</li> </ul>
United Kingdom 	<p><b>FCA, FG15/4: Social media and customer communications</b> Clarifies that if the communication includes an invitation or inducement to engage in financial activity, it is considered a “financial promotion” and 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</p>	
Switzerland 	<p><b>Swiss Financial Market Supervisory Authority (FINMA) Operational Risks at Banks Circular 2008 (FINMA-Circ. 08/21)</b> Banks must diligently select, supervise (including monitoring content of staff communications sent on instant messaging, unified communications, social networks and so on), and train staff and third parties who have access to client-identifying data.</p>	
Singapore 	<p><b>MAS Guidelines on Risk Management Practices—Internal Controls Article 3.5.1</b> 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.</p> <p><b>MAS Technology Risk Management Guidelines, Article 9.1.4</b> Financial institutions should not use unsafe internet services such as social media sites, cloud-based internet storage sites, and web-based emails to communicate or store confidential information.</p>	
Australia 	<p><b>Australian Securities and Investments Commission (ASIC), Corporations Act, Section 912</b> Have procedures and systems to monitor employees with potential conflicts of interest so they cannot communicate with each other across all communications and social channels.</p>	




# ARCHIVE

Country	Regulation	How Proofpoint Addresses Rules
<p>United States</p> 	<p><b>FFIEC Social Media Guidance</b> Establish a recordkeeping system to archive activities.</p> <p><b>SEC 17a-3 and a-4</b> Preserve relevant communications for a period of not less than three years, the first two in an easily accessible place.</p> <p><b>FINRA Regulatory Notice 10-06 and 11-09</b> 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.</p> <p><b>SEC DFA Section 764 and CFTC SEA Section 15F(g)(1)</b> Daily trading communications, including email, instant messages, phone calls, and social media, of security-based swaps and all related records to be recorded for the period required by the Commission by rule or regulation.</p> <p><b>Investment Advisers Act, Rules 204(2) and 206(4)-1</b> Ensure that adequate records are kept across all communications and social channels in use.</p> <p><b>FINRA Regulatory Notice 11-39</b> Capture and archive all communications by registered persons on social channels sent through personal devices.</p> <p><b>Commodity Futures Trading Commission (CFTC), Dodd-Frank Act—Section 731</b> 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.</p>	<ul style="list-style-type: none"> <li>• Automatically adds messages to the archive with a single checkbox.</li> <li>• Proofpoint Digital Compliance and Archive allows firms to capture and securely archive digital content that constitutes a business communication.</li> <li>• Allows organizations to preserve digital content for a period of at least six years per requirements under the FINRA rules in SEA 17a-4.</li> <li>• Allows firms to capture and securely archive social content that constitutes advertising, sales literature, and correspondence.</li> <li>• Our unique grid-based storage architecture also ensures that information is available for immediate access by compliance</li> </ul>
<p>Canada</p> 	<p><b>IIROC Rule 29.7(5)</b> Retain advertisements and content for a period of two years, and ensure it is readily available for inspection.</p> <p><b>IIROC Notice 0349</b> Retain records of business activities, financial affairs, customer transactions and communications, including “Facebook, Twitter, YouTube, blogs and chat rooms, are subject to the IIROC Dealer Member Rules.”</p>	
<p>United Kingdom</p> 	<p><b>FCA Policy Statement 08/1</b> All relevant electronic communications must be retained, including fax, email, Bloomberg mail, video conferencing, SMS, business to business devices, chat, and instant messaging.</p>	
<p>European Union</p> 	<p><b>European Securities and Markets Authority (ESMA), MiFID II Article 16(7)</b> 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.</p>	
<p>Australia</p> 	<p><b>Australian Securities &amp; Investments Commission (ASIC), Regulatory Guide 234 “Advertising financial products and services (including credit): Good Practice</b> Firms should capture and archive any advertisements, even those on social channels.</p>	
<p>International</p> 	<p><b>IOSCO, Principles for Benchmark-Setting Processes, D.2 and D.3</b> Benchmark Calculation Agents need to document and keep records of all interactions with submitting parties, audit records of the data used for calculating the Benchmark and records of contacts with the Benchmark and make these available to Supervisory Authorities upon request.</p>	




# HEALTHCARE

## POLICY AND PROCEDURES


Country	Regulation	How Proofpoint Addresses Rule
United States 	<p><b>Department of Health and Human Services, Health Insurance Portability and Accountability Act (HIPAA)</b></p> <p>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.</p>	<ul style="list-style-type: none"> <li>• Provides healthcare compliance best-practice policy templates for immediate enforcement</li> <li>• Delivers real-time monitoring and supervision to ensure policies are followed; enables firms to identify those who require additional training</li> <li>• End-to-end compliance platform that helps companies follow best practices</li> </ul>
United Kingdom 	<p><b>National Health Services (NHS)</b></p> <p>Various Trusts have issued acceptable-use guidelines around electronic communications that fall under broadly similar areas. Employees are not allowed to use social media as part of their work except through the Trust’s official social media channels, for which content has to be pre-submitted and vetted.</p> <p><b>Nursing and Midwifery Council (NMC)</b></p> <p>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. Should not be used for whistle-blowing or raising concerns. Should not discuss work online especially about patients or colleagues.</p> <p><b>British Medical Association (BMA)</b></p> <p>Should not enter into informal relationships with patients on social networking sites to reduce the likelihood of inappropriate boundary transgressions.</p>	
Australia 	<p><b>Medical Board of Australia, Social Media Policy</b></p> <p>Maintains the privacy and confidentiality of patient information. This applies even if the privacy settings used in a particular social-media 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.</p> <p><b>Australian Medical Association has released guidelines on social media as a joint initiative of the AMA, NZMA, NZMSA and the AMSA</b></p> <p>Unsolicited testimonials for certain products and drugs if posted on social media and appear on the walls of a medical brand page or profile it is an immediate violation of Therapeutic Goods Administration (TGA) guidelines in Australia and must be deleted.</p>	

## CONTENT


Country	Regulation	How Proofpoint Addresses Rule
Australia 	<p><b>Medical Board of Australia, Guidelines for advertising regulated health services</b></p> <p>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 be misleading, and should not contain an offer or inducement to the consumer or testimonials.</p>	<ul style="list-style-type: none"> <li>• Provides streamlined approval workflow for stakeholders to pre-approve static content, including profiles and ads</li> <li>• Delivers notifications about content and compliance infractions</li> <li>• Enables organizations to remediate problematic content right away</li> <li>• Provides a library of highly targeted content generated by both internal staff and third parties</li> </ul>



## SUPERVISION

Country	Regulation	How Proofpoint Addresses Rule
United States 	<p><b>Department of Health and Human Services, Health Insurance Portability and Accountability Act (HIPAA)</b>            Healthcare firms need to have procedures in place to properly authorize and supervise employees handling PHI and ePHI.</p>	<ul style="list-style-type: none"> <li>• Continuously monitors digital communications and automatically identifies high-risk content; can remove it in seconds</li> <li>• Applies natural language processing and a wide range of compliance policies to accurately identify content that may pose a compliance risk</li> <li>• Out-of-the-box policy templates manage HIPAA compliance; no rule-writing or keyword lists needed</li> <li>• Monitors RIA social profile accounts and automatically identifies testimonials in both pre- and post-published content</li> <li>• Delivers notifications about content and compliance infractions</li> <li>• Content enforcement options that include log, notify, hide, and delete</li> </ul>


## ARCHIVE

Country	Regulation	How Proofpoint Addresses Rule
United States 	<p><b>Department of Health and Human Services, Health Insurance Portability and Accountability Act (HIPAA)</b>            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.</p> <p><b>State Governments, The Affordable Care Act (ACA)</b>            Requires organizations to adopt comprehensive recordkeeping practices (e.g. 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 a at least ten years.</p> <p><b>Department of Labor, Employee Retirement Income Security Act (ERISA)</b>            General guidance for record retention of journals, ledgers, checks, invoices, contracts, agreements, vouchers, 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.</p>	<ul style="list-style-type: none"> <li>• Automatically adds messages to the archive with a single checkbox.</li> <li>• Proofpoint Digital Compliance and Archive allows firms to capture and securely archive digital content that constitutes a business communication.</li> <li>• Allows organizations to preserve content for a period of at least six years per HIPAA requirements</li> <li>• Allows firms to capture and securely archive social content that constitutes advertising, sales literature, and correspondence.</li> <li>• Unique grid-based storage architecture also ensures that information is available for immediate access by compliance team or regulator.</li> </ul>





# ENERGY AND UTILITIES

## POLICY AND PROCEDURES

Country	Regulation	How Proofpoint Addresses Rule
United States 	<p><b>Federal Energy Regulatory Commission (FERC), Order 71</b>            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 communications and social channels.</p> <p><b>NERC Critical Infrastructure Protection (CIP) Standards, CIP-003-1</b>            Requires the development and management of security management controls to protect critical network and other assets. Have the processes and technology in place to prevent data leakage and malware threats via communications and social channels</p> <p><b>NERC Critical Infrastructure Protection (CIP) Standards, CIP-005-1</b>            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.</p>	<ul style="list-style-type: none"> <li>• Provides compliance best-practice policy templates for immediate enforcement</li> <li>• Delivers real-time monitoring and supervision to ensure policies are followed; enables firms to identify those who require additional training</li> <li>• End-to-end compliance platform that helps companies follow best practices</li> </ul>

## ARCHIVE

Country	Regulation	How Proofpoint Addresses Rule
United States 	<p><b>Department of Energy (DOE), 10 CFR 600.153</b>            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.</p> <p><b>Federal Energy Regulatory Commission (FERC), Order 717</b>            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.</p>	<ul style="list-style-type: none"> <li>• Automatically adds messages to the archive with a single checkbox.</li> <li>• Proofpoint Digital Compliance and Archive allows firms to capture and securely archive digital content that constitutes a business communication.</li> <li>• Allows organizations to preserve digital content for a period of at least five years per FERC requirements</li> </ul>
European Union 	<p><b>European Agency for the Cooperation of Energy Regulators (ACER), European Union, REMIT (Regulation on energy market integrity and transparency—No. 1227/2011)</b>            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.</p>	<ul style="list-style-type: none"> <li>• Allows firms to capture and securely archive social content that constitutes advertising, sales literature, and correspondence.</li> <li>• Unique grid-based storage architecture also ensures that information is available for immediate access by compliance team or regulator.</li> </ul>





# PHARMACEUTICAL



## POLICY AND PROCEDURES

Country	Regulation	How Proofpoint Addresses Rule
United Kingdom 	<p><b>The Association of the British Pharmaceutical Industry (ABPI) published guidelines instructing member organizations on how to use social media and online communications in ways that keep them compliant with ABPI's overall code of conduct on 1 Apr 2011.</b></p> <p>Clause 1.2 defines that promotion is any activity undertaken by a pharmaceutical company or with its authority which promotes the prescription, supply, sale or administration of its medicines, including a face-to-face meeting, through the distribution of paper-based or electronic promotional material, on a social networking site, in an online forum or by email.</p> <p><b>Association of the British Pharmaceutical Industry (ABPI)</b></p> <p>Clause 9.9 states that telephone, text messages, email and other electronic data communications must not be used for promotional purposes without prior permission of the recipient. Companies are required to provide information for recipient as to how to unsubscribe.</p>	<ul style="list-style-type: none"> <li>• Provides compliance best-practice policy templates for immediate enforcement</li> <li>• Delivers real-time monitoring and supervision to ensure policies are followed; enables firms to identify employees who require additional training</li> <li>• End-to-end compliance platform that helps companies follow best practices</li> </ul>


## CONTENT

Country	Regulation	How Proofpoint Addresses Rule
United States 	<p><b>Food and Drug Administration (FDA), Internet/ Social Media Platforms with Character Space Limitations—Presenting Risk and Benefit Information for Prescription Drugs and Medical Devices</b></p> <p>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.</p>	<ul style="list-style-type: none"> <li>• Provides streamlined approval workflow for stakeholders to pre-approve static content, including profiles and ads</li> <li>• Delivers notifications about content and compliance infractions</li> </ul>
United Kingdom 	<p><b>Association of the British Pharmaceutical Industry (ABPI)</b></p> <p>Information on taking medicines can be provided to the public over social media if it complies with the Code Clause 22. 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, in addition to any link to further information, complied 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.</p>	<ul style="list-style-type: none"> <li>• Enables organizations to remediate problematic content right away</li> <li>• Provides a library of highly targeted content—generated by both internal staff and third parties</li> </ul>

## SUPERVISION

Country	Regulation	How Proofpoint Addresses Rule
United States 	<b>Centers for Medicare &amp; Medicaid Services (CMS), Physician Payment Sunshine Act final rule (42 CFR Parts 402 and 403)</b> 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.	<ul style="list-style-type: none"> <li>Continuously monitors digital communication and automatically identifies high-risk content; can remove it in seconds</li> <li>Applies natural language processing and a wide range of compliance policies to accurately identify content that may pose a compliance risk</li> <li>Out-of-the-box policy templates manage compliance for HIPAA, FDA, and more; no rule-writing or keyword lists needed</li> </ul>
United Kingdom 	<b>Association of the British Pharmaceutical Industry (ABPI)</b> Clause 4.10—Reporting adverse events. 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.	<ul style="list-style-type: none"> <li>Monitors RIA social profile accounts and automatically identifies testimonials in both pre- and post-published content</li> <li>Delivers notifications about content and compliance infractions</li> <li>Content enforcement options that include log, notify, hide, and delete</li> </ul>

## ARCHIVE

Country	Regulation	How Proofpoint Addresses Rule
United States 	<b>Food and Drug Administration (FDA), Code of Federal Regulations, Title 21 CFR Part 11</b> 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 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.  <b>Food and Drug Administration (FDA), Prescription Drug Marketing Act (PDMA)</b> Recordkeeping requirement associated with marketing and advertising via communication or social channels should be captured and archived.  <b>Food and Drug Administration (FDA), Fulfilling Regulatory Requirements for Postmarketing Submissions of Interactive Promotional Media for Prescription Human and Animal Drugs and Biologics (Draft)</b> Firms wanting to use social media need to submit the material posted on social media to the FDA after the event.  <b>Food and Drug Administration (FDA), Draft Guidance for Internet/ Social Media Platforms: Correcting Independent Third-Party Misinformation About Prescription Drugs and Medical Devices</b> Firms must keep records of corrections made should the FDA have questions. Adequate records of social media content must be captured and archived.  <b>Food and Drug Administration (FDA), Post-marketing reporting of adverse events, 21 CFR 314.80 and 21 CFR 600.8</b> Correspondence relating to adverse events on communications and social channels need to be captured and archived for ten years.	<ul style="list-style-type: none"> <li>Provides compliance best-practice policy templates for immediate enforcement</li> <li>Delivers real-time monitoring and supervision to ensure policies are followed; enables firms to identify employees who require additional training</li> <li>End-to-end compliance platform that helps companies follow best practices</li> </ul>

## ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.