



# Panorama normativo in materia di messaggistica

Come conformarsi alle normative che regolamentano la  
conservazione e la supervisione di e-mail e instant message

## Indice

<b>Reperimento delle informazioni</b> .....	<b>1</b>
<b>Alla scoperta del Mondo Digitale</b> .....	<b>1</b>
<b>Le normative attualmente esistenti</b> .....	<b>2</b>
<b>L'esigenza di una governance aziendale</b> .....	<b>3</b>
<b>Scandali, multe e ancora multe</b> .....	<b>3</b>
<b>Quali tipi di documenti possono essere considerati documentazione aziendale e quali no?</b> ....	<b>4</b>
<b>Best practice in materia di conservazione delle e-mail</b> .....	<b>4</b>
Archiviazione e cancellazione di messaggi ai sensi delle leggi e delle politiche aziendali. ....	4
Ricerca e recupero di informazioni .....	5
Leggibilità .....	6
Integrità e verificabilità dei dati .....	6
Autenticità .....	6
Disponibilità .....	7
<b>La soluzione</b> .....	<b>7</b>
<b>Normative che regolamentano i servizi finanziari</b> .....	<b>8</b>
SEC 17a-4 .....	8
NASD 3010 e 3110 .....	11
Il Sarbanes-Oxley Act .....	12
Gramm-Leach-Bliley .....	14
FSA (Regno Unito) .....	14
PIPEDA (Canada) .....	15
Statuto IDA 29.7 (Canada) .....	15

UMIR Policy 7.1 (Canada) .....	16
<b>Normative regionali .....</b>	<b>17</b>
Normative sulle polizze di assicurazione .....	17
Florida Sunshine Laws .....	17
<b>Normative che regolamentano il sistema sanitario e farmaceutico .....</b>	<b>18</b>
HIPAA .....	18
Food and Drug Administration Enforcement Policy .....	19
<b>Normative che regolamentano il settore energetico .....</b>	<b>20</b>
FERC (CFR TITLE 18) .....	20
<b>Normative che regolamentano il settore militare e il governo federale .....</b>	<b>21</b>
DOD 5015.2 (US) .....	21
NARA GRS20 (US) .....	22
<b>Normative che regolamentano il settore delle telecomunicazioni ..</b>	<b>23</b>
UK Data Protection Act del 1998 .....	23
US Electronic Communications Act del 1996 .....	23
<b>Conclusione .....</b>	<b>24</b>
<b>Background societario .....</b>	<b>24</b>

## Elenco delle tabelle

<i>Tabella 1: SEC 17a-4</i>	9
<i>Tabella 2: NASD 3010 e 3110</i>	11
<i>Tabella 3: Sarbanes-Oxley</i>	12
<i>Tabella 4: Gramm-Leach-Bliley</i>	14
<i>Tabella 5: FSA (Regno Unito)</i>	14
<i>Tabella 6: PIPEDA (Canada)</i>	15
<i>Tabella 7: Statuto 29.7 (Canada)</i>	15
<i>Tabella 8: UMIR Policy 7.1 (Canada)</i>	16
<i>Tabella 9: Normative che regolano il sistema assicurativo</i>	17
<i>Tabella 10: Florida Sunshine Laws</i>	17
<i>Tabella 11: HIPAA</i>	18
<i>Tabella 12: FDA Enforcement Policy</i>	19
<i>Tabella 13: FERC</i>	20
<i>Tabella 14: DOD 5015.2</i>	21
<i>Tabella 15: NARA GRS20</i>	22
<i>Tabella 16: UK Data Protection Act</i>	23
<i>Tabella 17: US Electronic Communications Act</i>	23

## Reperimento delle informazioni

Alla luce dell'impennata dei volumi e della dipendenza da posta elettronica, circa il 70% delle informazioni business-critical viene conservato all'interno di sistemi di messaggistica aziendali<sup>1</sup>. La posta elettronica si è affermata come strumento mission-critical, e molte aziende considerano i server di posta elettronica alla stregua di depositari dell'intelligenza aziendale - scopo per il quale non sono stati concepiti. La prospettiva di conservare e recuperare e-mail è scoraggiante dato che il volume effettivo di e-mail scambiate tra aziende è sbalorditivo.

Flussi di e-mail in rapida espansione, normative statali, maggiori responsabilità aziendali e controversie legali sempre più frequenti sono alcune delle minacce a cui molte organizzazioni devono oggi far fronte. La posta elettronica è un bene aziendale di vitale importanza e come tale deve essere trattata. Le organizzazioni chiedono strumenti per la gestione, l'accesso e la ricerca di contenuto specifico, il che implica l'esigenza di reperire informazioni.

## Alla scoperta del Mondo Digitale

Una ricerca ha dimostrato che solo negli Stati Uniti esistono oltre 10.000 leggi e normative redatte da enti legislativi statali e regionali che hanno in comune il fatto di regolamentare "documenti" - ovvero informazioni che assumono molte delle forme citate in precedenza. Queste normative, inoltre, regolamentano il processo che prevede la creazione, l'archiviazione, l'accesso, l'aggiornamento e la conservazione di tali documenti per periodi di tempo sempre più lunghi, in alcuni casi addirittura per periodi superiori alla vita di un essere umano. La conformità con tali disposizioni interessa l'intera organizzazione e supera i confini che delimitano l'aspetto IT e quello commerciale di un'azienda, compresi gli stakeholder che notoriamente non prendono parte al processo decisionale, come ad esempio gli uffici legali o i chief compliance officer<sup>2</sup>. Nell'ultimo decennio la tecnologia ha giocato un ruolo fondamentale nel passaggio dai documenti cartacei come supporto informativo ai documenti elettronici, che comprendono fogli elettronici, presentazioni, documenti di word processing, e-mail e instant message. Mentre in passato i documenti cartacei rappresentavano il mezzo più diffuso per la trasmissione di informazioni, la tecnologia lo ha sublimato alla dimensione on-line. Secondo un'analisi condotta dalla UC Berkeley, attualmente il 93% di tutte le informazioni viene creato in formato elettronico<sup>3</sup>.

Oggi giorno le organizzazioni si affidano principalmente a informazioni digitali/elettroniche. La maggior parte di queste informazioni viene divulgata internamente o esternamente per mezzo della posta elettronica che è diventata il principale metodo di comunicazione per qualsiasi azienda.

1 Enterprise Strategy Group

2 Enterprise Strategy Group, Impact Report: Compliance, May 2003

3 Osterman Research, Inc., How to Evaluate and Choose A Messaging Archiving Solution

Quando per la prima volta la posta elettronica si è affermata come principale strumento utilizzato dalle aziende, pochi erano i controlli o le politiche deputati alla regolamentazione dell'uso e della conservazione di questi messaggi. Questi sistemi si imposero senza politiche e controlli sulla gestione dei dati dal momento che si riteneva che la posta elettronica costituisse semplicemente un nuovo metodo di comunicazione reciproca. L'e-mail non era stato concepito per essere un documento, così come il server di posta elettronica non era stato concepito per fungere da "depositario" delle conoscenze di un'organizzazione. Tuttavia questi sistemi di messaggistica aziendali si sono trasformati in qualcosa di ben diverso da un semplice strumento di comunicazione.

## Le normative attualmente esistenti

In linea di massima tutte le organizzazioni sono tenute a soddisfare i requisiti di conservazione di documenti statutari, compresi requisiti più generali quali il Sarbanes-Oxley Act, l'Americans with Disabilities Act, l'Age Discrimination in Employment Act e l'Occupational Safety and Health Act; nonché svariati requisiti regionali e di altra natura. Le aziende regolamentate dalla SEC (Securities and Exchange Commission, la Commissione di Vigilanza della Borsa americana), dalla NASD (National Association of Securities Dealers, Associazione nazionale degli operatori in titoli) o dalle normative UMIR per i mercati canadesi (Universal Market Integrity Rules for Canadian Marketplaces) devono attenersi a rigorose linee guida in materia di conservazione dei dati. Le aziende che operano nel settore sanitario devono attenersi a politiche sulla conservazione dei dati stabilite da vari enti normativi e a vari statuti, quali l'Health Insurance Portability and Accountability Act (HIPAA), le Medicare Conditions of Participation e la Food and Drug Administration (FDA). Le agenzie governative devono conformarsi ad un'ampia gamma di requisiti in materia di conservazione dei dati, compresi quelli stabiliti dalla NASA (National Aeronautics and Space Administration), dal Ministero della Difesa, oltre a varie disposizioni sancite nell'United States Code, nel National Archives of Canada e da altre agenzie e statuti. Molti requisiti in materia di conservazione dei documenti impongono specifici requisiti in materia di e-mail e instant message, quali ad es. il SEC 17a-4 oppure fanno riferimento a documenti elettronici in cui possono rientrare e-mail e IM.

Le autorità competenti hanno sempre chiesto alle società di salvare e conservare documenti importanti, sebbene si riferissero perlopiù a documenti cartacei. Molti enti normativi, specialmente quelli legati al settore finanziario – SEC e NASD – hanno ravvisato la diffusione e l'importanza dei documenti elettronici. Le autorità competenti operanti in diversi settori hanno raccolto il testimone dal settore dei servizi finanziari e hanno recentemente dichiarato che e-mail e instant message sono documenti che devono essere conservati prestando la stessa attenzione riservata ai documenti cartacei. Queste autorità si sono rese conto che nei server di posta elettronica è conservata una considerevole quantità di documenti aziendali e di altra natura e per questo motivo è necessario provvedere alla conservazione di tali documenti.

Dal momento che e-mail e instant message si sono trasformati in canali preferenziali di comunicazione, le società sono sotto stretta osservazione e sentono maggiormente il peso della pressione normativa che li obbliga a conservare i messaggi nella loro forma originale affinché siano a disposizione degli auditor a scopo di controllo su richiesta – l'accesso ai dati, l'archiviazione e il recupero di dati, la supervisione delle comunicazioni, la protezione dei dati e gli audit trail sono tutti aspetti che vengono minuziosamente verificati. L'esigenza di conformità alle varie normative governative e di settore, nonché l'esigenza di una governance aziendale delle regole interne, significa adottare un approccio proattivo a qualsiasi livello aziendale che consenta di gestire tutte queste problematiche IT e di conformità.

## L'esigenza di una governance aziendale

Oltre alla conformità con le normative, le organizzazioni iniziano anche ad avvertire l'esigenza di implementare politiche interne in materia di e-mail e instant message. Per evitare di essere perseguite per osservazioni discreditanzi o per distribuzione di materiale offensivo, nonché per evitare la condivisione di informazioni riservate o inopportune via e-mail e instant message, le società devono poter essere in grado di controllare i messaggi dei propri utenti al fine di identificare eventuali contenuti sospetti. Ciò consente alle organizzazioni di condurre indagini interne che potrebbero coinvolgere non solo entità esterne ma anche i dipendenti.

## Scandali, multe e ancora multe

Molte aziende hanno spesso adottato la politica del "vada come vada" per quanto riguarda l'archiviazione di messaggi per lunghi periodi di tempo, sostenendo che sia meno costoso vivere nel rischio e pagare, se necessario, le eventuali multe. Tuttavia le autorità competenti si sono fatte più severe in materia di applicazione di tali requisiti e si è registrata un'impennata sia nel numero di aziende multate, che nel numero di multe pecuniarie. Sebbene non vi sia una ragione normativa per l'archiviazione delle e-mail, vi è ancora un elevato rischio pecuniario per chi non conserva questi messaggi alla luce delle possibili controversie che questi potrebbero innescare. Le aziende che non si conformano ai requisiti di conservazione delle e-mail corrono inoltre il rischio di incorrere in difficoltà organizzative e perdita di credibilità.

Le porte dello scandalo si sono spalancate nel 2001, con il gravissimo caso Enron. In questi scandali, i tentativi di eliminare sia i documenti cartacei, che le e-mail sono riconducibili ad un disperato depistaggio delle indagini da parte di queste società. Questi scandali aprono la strada a importanti nuove leggi e normative, la più significativa delle quali è il Sarbanes-Oxley (SOX) Act del 2002. Il SOX e la nuova legislazione di "corporate governance" non solo hanno imposto alle società rigorosi controlli e nuovi requisiti ma hanno sancito anche l'importanza di procedure di conservazione e tutela di documenti, comprese le e-mail. Molte di queste nuove disposizioni adottano un approccio applicativo estremamente rigoroso, e nel caso del Sarbanes-Oxley Act hanno indicato i senior executive – quali Amministratore Delegato e Responsabile Amministrativo – come personalmente e penalmente responsabili della conformità.

Nel gennaio 2003, la Commissione di vigilanza della Borsa americana ha multato 5 importantissime aziende di Wall Street per un totale di 8,2 milioni di dollari per inadempienza alla Regola 17a-4. Laddove molte aziende erano prima in dubbio sull'entità dell'adempimento della 17a-4 in materia di messaggistica elettronica, questo provvedimento e altri simili esemplificano l'obiettivo delle autorità competenti che chiedono di tenere in seria considerazione questi statuti. La SEC ha scoperto che alcune aziende conservavano su nastri vecchi messaggi e-mail che erano stati eliminati o sovrascritti prima del termine previsto di 3 anni.

Nel luglio 2004, un colosso dell'industria del tabacco, la Philip Morris USA e la sua casa madre, la Altria Group Inc., sono state multate per un totale di 2,7 milioni di dollari per aver cancellato e-mail ritenute potenzialmente rilevanti per la causa intentata dal governo contro l'industria del tabacco.

## Quali tipi di documenti possono essere considerati documentazione aziendale e quali no?

La "rete normativa" in materia di messaggi è stata ampiamente stabilita ed è ancora in evoluzione. Inizialmente, tutta l'attenzione era concentrata sulle e-mail. Ora, grazie a direttive più esplicite da parte delle autorità competenti, quali il NASD, e ad una nuova casistica giudiziaria, anche gli instant message (IM) sono considerati documenti. I messaggi e i documenti che rientrano nelle attuali normative sono:

- Messaggi e-mail e relativi allegati
- Documenti elettronici quali Microsoft Word, Excel, Powerpoint, ecc.
- File log degli instant message
- Collaboration repository, quali cartelle pubbliche di Microsoft Exchange e database di IBM/Lotus Notes

Non tutte le e-mail devono essere archiviate in quanto non tutte sono rilevanti per l'azienda. È chiaro che non è necessario salvare uno spam in quanto non costituisce documento aziendale e quindi non risponde ai requisiti normativi di conservazione delle informazioni. Molte delle e-mail aziendali utilizzate per scopi personali non devono essere archiviate. Ad esempio, uno scambio di messaggi personali tra amici che discutono di una partita di calcio non ha rilevanza ai fini dell'attività di un'organizzazione. Altre e-mail quali promemoria di incontri o notifiche del tipo "Non sono in ufficio" potrebbero non essere rilevanti ai fini dell'archiviazione. La problematica maggiore è stabilire quali e-mail è necessario archiviare e per quanto tempo.

## Best practice in materia di conservazione delle e-mail

Esistono molti tratti comuni tra la moltitudine di normative che regolamentano la conservazione di documenti da parte di società che operano in settori specifici e di società pubbliche in generale.

### Archiviazione e cancellazione di messaggi ai sensi delle normative e regole aziendali

Le normative prevedono che le organizzazioni conservino messaggi in entrata, in uscita e interni e che archivino questi messaggi per un determinato periodo di tempo a seconda di quanto previsto dalla normativa. La maggior parte di queste normative specifica che per quanto riguarda le e-mail, queste devono essere conservate per almeno tre anni fino ad un massimo di sette. Tuttavia, per alcuni documenti i tempi di conservazione si allungano. L'OSHA, ad esempio, richiede la conservazione di documenti per un periodo di trent'anni.

In molti casi, specialmente nel caso di aziende che dipendono da agenzie governative quali la SEC, si richiede di conservare il contenuto delle e-mail in un formato sicuro e di sola lettura ai fini della conformità legale. I formati WORM (Write Once Read Many - Scrivi una volta leggi più volte) assicurano l'impossibilità che il contenuto possa essere sovrascritto o modificato e che tale contenuto possa essere conservato per un determinato periodo di tempo, mantenendo inalterata la propria autenticità e soddisfacendo i requisiti normativi e specifici di controversie legali.

La possibilità di stabilire flessibili politiche di cancellazione dei documenti rientra in una più ampia soluzione di gestione della conservazione dei documenti. È infatti necessario poter garantire una sicura distruzione dei documenti al termine del periodo di conservazione, in modo che le organizzazioni non debbano rispondere a questioni di conformità una volta concluso il periodo di conservazione richiesto.

## Ricerca e recupero di informazioni

I dati conservati devono essere consultabili e recuperabili in caso di audit normativo o processo giudiziario. I dati elettronici devono essere archiviati in modo regolamentato affinché sia possibile trovare, accedere, organizzare, controllare e presentare le e-mail.

L'utilizzo di nastri di backup per il recupero delle e-mail pone molti problemi. I nastri di backup non sono concepiti per la ricerca e il recupero di informazioni specifiche. Si tratta quindi di una procedura inutile che fa perdere tempo prezioso. Il tempo richiesto per il recupero di e-mail da nastri di backup è notevole, tanto che alcune organizzazioni hanno trascorso settimane e mesi nel tentativo di presentare dati pertinenti e a questo scopo hanno speso milioni di dollari oppure non sono state in grado di soddisfare tale richiesta e sono state quindi multate. Secondo un'indagine condotta da Osterman Research, Inc., al 75% delle organizzazioni è stato chiesto di cercare e recuperare nei nastri di backup una o più e-mail in risposta ad una richiesta del proprio ufficio legale, dell'ufficio delle risorse umane o di qualche altro ente, mentre a circa il 40% delle società è stato ordinato da un tribunale o da un ente normativo di presentare le e-mail dei dipendenti<sup>4</sup>. Le soluzioni implementate devono poter garantire ricerche nell'intero archivio a prescindere dalle dimensioni e dal tipo dei supporti di memorizzazione utilizzati. L'indicizzazione delle voci, che identifica persone, società, numeri di conto e molte altre voci, è un modo pratico per lanciare una prima ricerca. I risultati della ricerca dovranno essere conservati in cartelle definite dall'utente dove potranno essere sottoposti a ulteriori migliorie e analisi. Gli utenti devono avere la possibilità di condividere questi risultati con altri utenti autorizzati. Gli utenti possono scegliere di consentire ad altri l'accesso e assegnare loro vari livelli di visualizzazione, o come utenti a pieno diritto o come utenti "ospiti". Ciò comprende la possibilità di consentire ad un organismo esterno la consultazione di archivi e risultati.

Per condurre ricerche più dettagliate si possono utilizzare i criteri di ricerca full-text e booleano per tutti i messaggi presenti in archivio. Alcune soluzioni consentono di automatizzare ulteriormente il processo di ricerca grazie alla possibilità di caricare un file contenente tutti i principali termini di ricerca. Altre funzioni avanzate comprendono opzioni di ricerca quali Fuzzy, Stemming e Phonic. La ricerca Fuzzy trova una parola, anche se scritta non correttamente (ad es., la ricerca della parola "mela" troverà anche mella). Lo Stemming amplia la ricerca alle variazioni grammaticali di una parola (ad es. la ricerca della parola "applicare" troverà anche applicato, applicando, applica). La ricerca di tipo Phonic individua una parola che ha lo stesso suono della parola che si sta cercando e che inizia con la stessa lettera (ad es. la ricerca di "Smith" troverà anche Smithe e Smythe).

4 Osterman Research, Inc., How to Evaluate and Choose A Messaging Archiving Solution

## Leggibilità

Una volta soddisfatti i requisiti di una semplice e rapida individuazione dei documenti necessari, è fondamentale che questi documenti siano leggibili. Dato il ritmo accelerato dell'innovazione tecnologica, si richiede compatibilità con formati e applicazioni tradizionali e, possibilmente, compatibilità con quelli futuri. Alcune normative (ad es. l'HIPAA) impongono la conservazione dei dati per decenni, sebbene la maggior parte dell'infrastruttura IT sia organizzata in tempistiche significativamente più brevi. Molte autorità e tribunali richiedono la presentazione dei dati recuperati in risposta ad una richiesta nel formato elettronico originale.

## Integrità e verificabilità dei dati

Una volta soddisfatte le richieste di recupero e leggibilità, è imperativo fare in modo che i documenti di conformità vengano gestiti nel massimo rispetto della privacy. Tuttavia, è sempre più importante equilibrare questo aspetto con la possibilità di consentire ad un ente normativo o a terzi autorizzati di controllare sia il procedimento mediante il quale si creano e conservano documenti, sia fornire accesso ai documenti di conformità stessi a scopo di controllo.

La maggior parte delle normative si concentra su misure di sicurezza da adottare al fine di tutelare i documenti archiviati contro eventuali alterazioni, danni o cancellazioni nel corso del periodo di conservazione richiesto. Queste regole stabiliscono in genere funzioni di sicurezza standard – tra cui controlli sugli accessi, autenticazione e log di audit. Una sicura architettura di archiviazione, quindi, deve prevedere misure cautelative quali l'autenticazione mediante password e il controllo sugli accessi a livello di applicazioni, sistema di file e storage.

Solo poche normative si spingono oltre richiedendo funzioni specifiche di memorizzazione per l'integrità dei dati, quali la Regola 17a-4 della SEC che prescrive che i dati relativi alla compravendita di titoli siano conservati nei supporti di memorizzazione in formato non riscrivibile e non cancellabile, noto anche come processo di memorizzazione WORM. L'archiviazione di messaggi su supporti di memorizzazione WORM è una garanzia maggiore per l'autenticità del documento e-mail. I dispositivi di memorizzazione WORM non consentono agli utenti di sovrascrivere o manomettere alcun documento archiviato. Tuttavia, per garantire l'integrità dei messaggi e degli allegati archiviati è necessario adottare misure supplementari.

## Autenticità

La Sezione SEC: 240.17a-4 (f) (3) (v) stabilisce che le aziende che si occupano di servizi finanziari devono implementare un software di audit che ne documenti la veridicità. Questi risultati devono essere a disposizione in qualsiasi momento nel corso del periodo di conservazione dei documenti e-mail. L'audit trail deve essere conservato per l'intera vita utile del messaggio e/o dell'allegato, ovvero non dovrà essere cancellato prima del termine del periodo di conservazione e prima della cancellazione dall'archivio del messaggio stesso.

I log di audit devono specificare informazioni quali data e ora, quando è stato esaminato, da chi, quale provvedimento è stato adottato in merito al messaggio (in termini di conformità le opzioni potrebbero essere: documento approvato, rifiutato, inserito in una cartella temporanea in attesa di decisioni future, ecc.). L'utente che visiona o prende provvedimenti in merito ad un messaggio deve essere identificabile mediante uno User ID. Un altro modo per garantire l'autenticità è disporre di un numero di serie univoco per ogni messaggio archiviato e apporre la bollatura oraria su questi messaggi elaborati. Il numero di serie e la bollatura oraria diventano parte integrante dei metadati associati al messaggio.

La Sezione 301(4) del SOX richiede ai comitati di revisione interna delle società pubbliche di stabilire procedure per la ricezione, la conservazione e il trattamento di reclami relativi a truffe, contabilità, controlli di contabilità interni o questioni di revisione contabile. Occorre definire un meccanismo per la conservazione e la bollatura oraria di suggerimenti o reclami e un audit trail che fornisca una risposta. Le soluzioni software esistenti sono in grado di individuare, apporre la bollatura oraria e contrassegnare automaticamente messaggi e allegati contenenti reclami e fornire un audit trail di conformità. Quindi non solo il messaggio viene individuato, ma può essere categorizzato e conservato per un adeguato periodo di tempo unitamente all'audit trail a testimonianza della conformità.

## Disponibilità

Garantire sempre la massima accessibilità e disponibilità dei dati è assolutamente essenziale, specialmente in considerazione dei requisiti necessari per una rapida presentazione di prove in caso di controversia. Le organizzazioni che adottano una strategia di disponibilità dei dati che si affida ad un unico dispositivo hardware rischiano di perdere l'accesso ai dati in caso di malfunzionamento di tale dispositivo. Le infrastrutture ridondanti dotate di protezione da failover garantiscono una maggiore disponibilità e integrità dei dati in quanto trasferiscono un servizio dati di un supporto non disponibile su un altro dispositivo del cluster. Spesso il trasferimento di un servizio dati è un processo trasparente per utenti e applicazioni finali e quindi il recupero del servizio dati è rapido e non comporta alcuna interruzione degna di nota dell'attività aziendale. È necessario che la disponibilità dei dati dell'archivio e-mail attive sia pari al 99,99% in modo da non perdere dati business-critical e non interrompere o rallentare le ricerche di dati.

## La soluzione

Assentor offre alle organizzazioni una soluzione ottimale per la definizione e l'implementazione di processi di conservazione e conformità finalizzati a soddisfare i requisiti Sarbanes-Oxley, SEC, NASD e altri requisiti normativi e di governance aziendale. In qualità di soluzione all'avanguardia per la sorveglianza e la supervisione di messaggi e-mail in entrata, in uscita e interni, nonché degli instant message, Assentor offre alle aziende la possibilità di ridurre i rischi legati al libero flusso di corrispondenza elettronica scansionando in modo intelligente il contenuto di ogni e-mail, allegato e instant message.

Soluzione più completa rispetto alla semplice ricerca di parole-chiave o frasi, Assentor utilizza la sofisticata tecnologia Natural Language Processing (NLP) combinata ad un sistema lessicale aperto per l'analisi del contenuto dei messaggi e-mail.

*Ad esempio, Assentor è in grado di cogliere le differenze tra i vari utilizzi del termine "sue": "sue" è la minaccia di un'azione legale, mentre "Sue" è il nome proprio. Assentor è inoltre in grado di capire che il termine "sue" può essere scritto in molti modi diversi quali "I'm going to take legal action against you", ovvero "Ho intenzione di intraprendere un'azione legale contro di lei". L'uso di "sue" come parola-chiave non consentirebbe di cogliere quest'accezione.*

Grazie alla tecnologia NLP e ad un sistema lessicale aperto, Assentor fornisce il meglio di entrambi gli aspetti, potendo offrire i più accurati e affidabili metodi di identificazione e contrassegno del contenuto dei messaggi potenzialmente a rischio di violazione di politiche interne o normative federali (vale a dire SEC, NASD, NYSE, Sarbanes-Oxley, HIPAA, ecc.). Assentor offre inoltre una gestione centralizzata delle politiche relative al contenuto e conserva una documentazione permanente dei risultati e di tutti gli eventi associati.

Assentor è inoltre in grado di contrassegnare contenuti sospetti in modalità pre- o post-ricezione. In modalità pre-ricezione, quando si rileva la presenza di contenuto inaccettabile o sospetto, Assentor blocca tale contenuto all'interno del flusso di e-mail della società e indirizza il messaggio in una coda di messaggi "in quarantena" dove verrà controllato da un apposito supervisore o amministratore, e solo dopo essere stato approvato verrà immesso nel flusso dei messaggi di posta. In modalità post-ricezione, quando si rileva la presenza di contenuto sospetto, Assentor indirizza il messaggio ad un supervisore dopo che il messaggio è già stato spedito. Le modalità pre- e post-ricezione possono essere implementate a livello di direzione, azienda, gruppo e giù giù fino al singolo individuo.

Per soddisfare molti requisiti statali in materia di conservazione dei documenti, Assentor archivia i messaggi su dischi WORM (Write Once Read Many) oppure su supporti on-line quali IBM Total Storage DR 450, NetApp SnapLock, EMC Centera Compliance Edition e Permabit Permeon.

Assentor è stata la prima soluzione nel suo genere ad essere lanciata sul mercato nel 1998, e il suo livello qualitativo e la sua esperienza stanno aiutando le aziende a conformarsi a queste esigenze normative. Noto come standard del settore per la conformità SEC, NASD e NYSE, Assentor supporta inoltre le nuove normative quali Sarbanes-Oxley e altre. La tecnologia avanzata NLP e il sistema lessicale aperto di Assentor - soluzione completa per la supervisione del flusso di lavoro con funzioni flessibili di conservazione dei documenti e supporto integrato per la gestione del contenuto e mass storage - è in grado di gestire una vasta gamma di normative in continuo aggiornamento in aree quali servizi finanziari, sanità e settore farmaceutico, settore energetico, pubblica amministrazione, settore militare e telecomunicazioni.

## **Normative che regolamentano i servizi finanziari**

### **SEC 17a-4**

La Regola SEC 17a-4 si rivolge a tutte le società che si occupano di servizi finanziari e indica a intermediari, banche e altri enti finanziari quali supporti utilizzare e per quale periodo di tempo conservare i documenti elettronici. Un emendamento alla Regola 17a-4 spiega che la SEC non obbliga intermediari e rivenditori a conservare tutte le e-mail e le comunicazioni internet, ma solo quelle che riguardano la comunicazione di informazioni importanti relative ad affari interni "intermediario-rivenditore" con i propri clienti e con il pubblico in generale. L'Instant Messaging (IM) rientra nella categoria di ciò che la SEC definisce "Comunicazioni Internet" e pertanto richiede di conservare i documenti IM allo stesso modo delle e-mail aziendali.

La SEC 17a-4 richiede alle società di conformarsi alle seguenti linee guida in materia di posta elettronica. La mancata osservanza di queste linee guida comporta una serie di sanzioni che non si limitano al pagamento di ingenti multe, ma anche alla sospensione o revoca della licenza:

**Tabella 1: SEC 17a-4**

Requisiti SEC 17a-4	Come Assentor Enterprise garantisce la conformità
Sezione: 240.17a-4 (f) (2) (ii) (A) Conservazione di tutti i documenti elettronici esclusivamente in formato non riscrivibile e non cancellabile.	Assentor supporta una vasta gamma di dischi (NetApp SnapLock, EMC Centera), dispositivi ottici e su nastro con funzioni WORM (Write Once Read Many).
Sezione: 240.17a-4 (f) (2) (ii) (B) Possibilità di verificare automaticamente la qualità e l'accuratezza del processo di registrazione dei supporti di memorizzazione.	Assentor garantisce la scrittura e la verifica del contenuto del messaggio prima che il messaggio venga considerato opportunamente archiviato.
Sezione: 240.17a-4 (f) (2) (ii) (C) Serializzare i supporti di memorizzazione originali e specificare data e ora delle informazioni per il periodo di conservazione richiesto.	Assentor crea un numero di serie univoco per ciascun messaggio e appone una bollatura oraria su ogni messaggio elaborato. Il numero di serie e l'orario diventano parte integrante dei metadati associati al messaggio.
Sezione: 240.17a-4 (f) (2) (ii) (D) Possibilità di scaricare tempestivamente indici e documenti conservati sui supporti.	La ricerca e il recupero di messaggi e allegati dall'archivio Assentor sono operazioni che possono essere effettuate facilmente mediante una schermata di ricerca web-based in Assentor Archive o in Assentor Discovery. Assentor Discovery viene utilizzato principalmente in caso di controversie o ricerche su ingenti volumi di dati per indagini interne o richieste normative di messaggi e allegati. I messaggi e gli allegati recuperati vengono salvati in alcune directory a scopo di analisi e/o creazione del corrispettivo set di messaggi nel formato richiesto. A seconda delle necessità, i messaggi e gli allegati possono essere stampati in blocco oppure salvati in formato PDF, TIF e nell'originale formato e-mail. Gli indici vengono salvati nel database Assentor e possono essere inoltrati al DTPP (Designated Third Party Provider - Terza parte di fiducia designata) o ad altri mediante il dump del database o invio di un nastro di backup.
Sezione: 240.17a-4 (f) (3) (i) Capacità di presentare documenti in ogni momento per un'immediata revisione da parte SEC/SRO.	Come accennato sopra, Assentor Discovery viene utilizzato per garantire la disponibilità immediata dei documenti a scopo di revisione da parte SEC/SRO.
Sezione: 240.17a-4 (f) (3) (iii) Conservazione in un luogo a parte di una copia di ciascun documento.	Assentor crea due copie di tutti i messaggi su supporti, dischi separati, ecc. e fa in modo che entrambe le copie vengano scritte e verificate prima che il messaggio venga considerato opportunamente archiviato. Uno dei due supporti finali viene generalmente inviato al DTPP (DTPP - Designated Third Party Provider) che ne verifica la conformità ai sensi dei requisiti sanciti dalla Regola SEC 17a-4.f.3.viii.

Requisiti SEC 17a-4	Come Assentor Enterprise garantisce la conformità
Sezione: 240.17a-4 (f) (3) (iv) Disponibilità di un indice accurato sia sull'originale che sul duplicato del documento.	Assentor crea un indice "intelligente" di tutti i messaggi che vengono archiviati. L'indice contiene tutte le voci (nomi di persone, luoghi, nomi di società, numeri di conto, ecc.) che la tecnologia Natural Language Content Analysis (NLCA) trova nel corpo del messaggio e negli allegati. Anche le informazioni che compaiono nell'intestazione del messaggio (data, ora, mittente e destinatario) vengono inserite nell'indice. L'indice è uno strumento efficiente e richiede molto meno spazio di memorizzazione rispetto agli indici "full-text", inoltre consente ai clienti di trovare rapidamente qualsiasi messaggio anche in presenza di notevoli quantità di dati all'interno dell'archivio. Questi indici vengono salvati nel database Assentor e possono essere inoltrati al DTPP o ad altri mediante il dump del database o invio di un nastro di backup. L'indice compare su entrambe le copie del messaggio salvato su supporti o dischi WORM.
Sezione: 240.17a-4 (f) (3) (iv) (A) Tenere sempre a disposizione l'indice per controlli da parte SEC/SRO.	L'indice Assentor può essere tempestivamente richiamato dal database Assentor in qualsiasi momento e può essere mostrato a qualunque incaricato dei controlli.
240.17a-4 (f) (3) (iv) (B) Creazione di un duplicato dell'indice e conservazione in un luogo diverso da quello dell'originale.	I dump di backup periodici del database soddisfano questa esigenza in quanto i nastri di backup vengono generalmente conservati in un luogo diverso ai fini di "disaster recovery". Inoltre, gli amministratori del sistema possono creare dump dell'indice da Assentor in qualsiasi momento.
Sezione: 240.17a-4 (f) (3) (iv) (C) Conservazione dell'indice per l'intera durata del periodo richiesto.	Assentor conserva l'indice di ogni messaggio per tutto il tempo in cui il messaggio rimane in archivio. Allo scadere del periodo di conservazione del messaggio e non appena il messaggio viene cancellato, anche l'indice viene cancellato.
Sezione: 240.17a-4 (f) (3) (v) Implementazione di un software di revisione per documentare la contabilità.	Assentor crea un audit trail completo che riporta nel dettaglio la cronologia e i provvedimenti adottati nel corso della vita di un messaggio. Qualsiasi addetto alla conformità o supervisore che esamini un messaggio viene registrato nell'audit trail.
240.17a-4 (f) (3) (v) (A) Disponibilità dei risultati per SEC/SRO in qualsiasi momento.	Assentor crea report standard che ne testimoniano la conformità qualora SEC o SRO desiderino esaminarli. Assentor conserva statistiche di tutti i messaggi archiviati, esaminati, approvati, respinti ecc. nonché dettagli sullo stato dei messaggi per persona, gruppo e società.
240.17a-4 (f) (3) (v) (B) I risultati della revisione devono restare a disposizione in qualsiasi momento nel corso del periodo di conservazione del documento.	Assentor conserva l'audit trail per l'intera vita del messaggio. Non viene eliminato per nessun motivo prima dello scadere del periodo di conservazione previsto e della cancellazione del messaggio.
240.17a-4(f) (3) (vi) Tempestiva possibilità di accesso a documenti e indici da parte di SEC/SRO.	È sempre possibile accedere in qualsiasi momento alle informazioni relative a messaggi, indici e audit conservate in Assentor. Videate e report standard forniscono tali informazioni in modo rapido e semplice. Inoltre è possibile recuperare in qualsiasi momento messaggi e allegati con i rispettivi metadati. Le informazioni relative a indici e audit trail possono essere facilmente recuperate su richiesta dal database Assentor.

Requisiti SEC 17a-4	Come Assentor Enterprise garantisce la conformità
240.17a-4(f) (3) (vii) Consentire ad una terza parte o più l'accesso a indici e documenti e il download di documenti su supporti accettabili a scopo di revisione da parte SEC/SRO.	Assentor fornisce servizi DTTP per tutte le implementazioni Assentor. Prevede inoltre la possibilità di inviare a terzi la seconda copia dei supporti o nastri unitamente ai nastri di backup del database. Assentor non prevede ulteriori costi di licenza per altre terze parti a scopo di accesso ai messaggi, ecc. in caso di richieste normative o legali.

## NASD 3010 e 3110

Le Regole NASD 3010 e 3110 si riferiscono in linea di massima a tutte le società che operano nel settore titoli sul territorio statunitense. Sotto la giurisdizione del NASD rientrano ben 5.300 società di brokeraggio, oltre 94.000 filiali e oltre 664.000 operatori in titoli registrati. Le Regole NASD 3010 e 3110 trattano i requisiti di supervisione e i periodi obbligatori di archiviazione della corrispondenza elettronica. Alle società viene richiesto di stabilire e gestire un sistema di supervisione con procedure scritte, controlli regolari della corrispondenza elettronica in entrata e in uscita, con una revisione di tutte le prassi dell'intera organizzazione e del suo adempimento alle regole in vigore e relative normative almeno una volta all'anno.

NASD 3010 e 3110 richiedono alle società di conformarsi alle seguenti linee guida in materia di posta elettronica:

**Tabella 2: NASD 3010 e 3110**

Requisiti NASD 3010 e 3110	Come Assentor Enterprise garantisce la conformità
NASD 3010(a) (2) Approvazione della corrispondenza dell'operatore registrato da parte di un superiore autorizzato designato.	Assentor applica politiche documentate in materia di controlli di supervisione di corrispondenza e-mail e Instant Messaging. Assentor Compliance supporta un processo di supervisione dell'organizzazione consentendo all'azienda di stabilire gruppi organizzativi di persone all'interno del sistema e assegnando a ciascun gruppo un Compliance Reviewer (CR) autorizzato. Solo ai CR autorizzati è consentito esaminare i messaggi delle persone che compongono il/i gruppo/i loro assegnato/i e sono le uniche persone a poter decidere se approvare o respingere messaggi che il sistema di quarantena Assentor ha giudicato come presunte violazioni delle regole SEC. L'organizzazione può personalizzare a proprio piacimento le procedure di revisione del contenuto dei messaggi Assentor per ciascun gruppo e/o persona a seconda del livello di verifica previsto dalla politica di supervisione dell'azienda. Inoltre, questa personalizzazione può essere applicata anche alla tipologia dei messaggi (interni, in uscita o in entrata). Assentor è in grado di gestire tutti i messaggi e-mail e allegati in entrata, in uscita e interni; conversazioni in Instant Messaging (in collaborazione con i nostri partner IM); nonché e-mail e allegati Bloomberg. Questa soluzione prevede la completa ispezione del contenuto di tutto il testo dei messaggi e degli allegati, nonché la possibilità di ispezionare a caso e in modo manuale messaggi "puliti" a proprio piacimento. Assentor si adatta praticamente a qualsiasi flusso di lavoro che un'azienda sceglie di implementare alla luce della propria politica e delle procedure di supervisione.

Requisiti NASD 3010 e 3110	Come Assentor Enterprise garantisce la conformità
NASD 3010 (d) (1) Conservazione sistematica di prove relative a procedure e applicazione, messa a disposizione di tali prove su richiesta.	La documentazione relativa ai controlli è sempre disponibile e può essere mostrata su richiesta agli addetti al momento del controllo.
La Regola NASD 3110 sancisce che tutte le aziende che fanno capo ad essa sono tenute a conservare tutti i documenti e la corrispondenza e a conformarsi ai requisiti relativi a conservazione e supporti di memorizzazione stabiliti dalle Regole SEC 17a-3 e 17a-4.	Assentor supporta una vasta gamma di dischi (NetApp SnapLock, EMC Centera, Permabit Permeon), dispositivi ottici e su nastro con funzioni WORM (Write Once Read Many). Assentor prevede la possibilità di stabilire politiche flessibili in materia di conservazione dei documenti che soddisfano i requisiti SEC 17-a4 o altri.

## Il Sarbanes-Oxley Act

Diventato legge nel giugno 2002, il Sarbanes-Oxley Act (SOX) è stato concepito per garantire maggiore trasparenza alle attività delle società quotate in borsa e degli enti finanziari. Tutte le società quotate in borsa che sono tenute a conformarsi alle normative SEC devono generalmente soddisfare anche altri requisiti, stabiliti dal Sarbanes-Oxley Act, in materia di conservazione di e-mail.

Il SOX è costituito da svariati componenti in quanto si occupa di governance aziendale, reporting e divulgazioni di natura finanziaria, auditing finanziario e di verificare l'adeguatezza dei controlli interni finalizzati a garantire l'accuratezza e l'integrità dei risultati finanziari divulgati. La legge prevede inoltre significative sanzioni legali in caso di inadempienza in quanto ritiene gli amministratori aziendali penalmente responsabili delle attività di una società. Le penali per il mancato rispetto della conformità alla certificazione e ai requisiti di conservazione dei documenti comprendono multe fino a 25 milioni di dollari per le aziende e 5 milioni di dollari per i responsabili, che possono anche rischiare fino a 20 anni di carcere.

Il Sarbanes-Oxley richiede alle società di conformarsi alle seguenti linee guida in materia di posta elettronica:

**Tabella 3: Sarbanes-Oxley**

Requisiti Sarbanes-Oxley relativi a comunicazioni e documenti	Come Assentor Enterprise garantisce la conformità
La sezione 103(a) richiede alle società contabili pubbliche registrate di conservare i documenti di revisione e le relative informazioni per 7 anni.	Assentor permette periodi di conservazione flessibili ed è in grado di archiviare messaggi e-mail e allegati, instant message e documenti.
La sezione 801(a) stabilisce che la documentazione pertinente comprenda fogli di lavoro, documenti principali di una revisione, appunti, corrispondenza e comunicazioni.	Assentor permette periodi di conservazione flessibili ed è in grado di archiviare messaggi e-mail e allegati, instant message e documenti.

Requisiti Sarbanes-Oxley relativi a comunicazioni e documenti	Come Assentor Enterprise garantisce la conformità
<p>La sezione 104(a) stabilisce che la Commissione di Vigilanza delle società pubbliche ha la possibilità di estendere la tipologia di documenti che le società contabili devono conservare.</p>	<p>Assentor permette periodi di conservazione flessibili ed è in grado di archiviare messaggi e-mail e allegati, instant message e documenti.</p>
<p>La sezione 501(a) richiede la separazione degli analisti di borsa dagli intermediari/rivenditori in base ad "appropriate partizioni informative" e impone l'autorizzazione alla pre-pubblicazione di una relazione di ricerca da parte di banche d'affari. Può succedere che prima della pubblicazione di una relazione alle banche d'affari venga chiesto di fornire documentazione relativa a qualsiasi scambio di e-mail tra le 2 parti.</p>	<p>Assentor MailWall offre la possibilità di stabilire e applicare politiche relative alle comunicazioni interne tra singoli, gruppi e uffici. Una volta spedito, il messaggio di posta elettronica viene esaminato da Assentor MailWall e approvato o respinto ai sensi della politica vigente. Questa possibilità di blocco risulta particolarmente utile nel settore dei servizi finanziari dove, ad esempio, un'azienda può decidere di bloccare un messaggio e-mail indirizzato ad un membro del gruppo Investimenti da un membro del gruppo Ricerca e viceversa.</p>
<p>La sezione 105(b) stabilisce che a qualsiasi cliente di una società contabile pubblica può essere richiesto di presentare documenti relativi a controlli o indagini.</p>	<p>Assentor MailWall annota e registra qualsiasi tentativo di comunicazione tra le parti bloccate e respinge al mittente il messaggio originale con un messaggio personalizzato. L'opzione di recupero e contenziioso di Assentor è in grado di svolgere una rapida ed efficiente ricerca nell'archivio, a prescindere dalle sue dimensioni o volume, di messaggi pertinenti e dispone di funzioni di ricerca full text per ricerche più approfondite.</p>
<p>La sezione 301(4) richiede agli addetti alla revisione interna delle società quotate in borsa di stabilire procedure per la ricezione, la conservazione e il trattamento di contestazioni relative a contabilità, controlli di contabilità interni o questioni di revisione contabile. Occorre definire un meccanismo per la conservazione e la bollatura oraria di suggerimenti o reclami e accertarsi che siano a prova di manomissione.</p>	<p>Tutti i messaggi catturati da Assentor dispongono di log di audit antimanomissione e bollatura oraria e possono essere conservati su una vasta gamma di dispositivi WORM.</p>
<p>La sezione 404 richiede alle società quotate in borsa di relazionare in merito ai propri controlli interni nei bilanci annuali. L'ultima regola a definire la sezione 404 riporta alcune note secondo le quali "nella conduzione di una simile valutazione e nello sviluppo dei criteri di efficacia dei controlli interni sul reporting finanziario, una società deve conservare elementi probatori - documentazione compresa - in grado di garantire ragionevole sostegno a favore della valutazione da parte dei quadri direttivi dell'efficacia dei controlli interni della società sul reporting finanziario."</p>	<p>Poiché la posta elettronica è al centro delle discussioni tra dipendenti e addetti ai controlli su tali argomenti, essa rappresenta un elemento cruciale dell'intera documentazione aziendale. Assentor permette periodi di conservazione flessibili ed è in grado di archiviare messaggi e-mail e allegati, instant message e documenti.</p>

## Gramm-Leach-Bliley

Il Financial Modernization Act del 1999, noto anche come il Gramm-Leach-Bliley Act, contiene indicazioni per la tutela delle informazioni finanziarie personali dei clienti in possesso di istituti finanziari. Questa legge regola la raccolta e la divulgazione di informazioni finanziarie personali dei clienti da parte degli istituti o delle società finanziarie che ricevono tali informazioni.

Il Gramm-Leach-Bliley richiede alle società di conformarsi alle seguenti linee guida in materia di posta elettronica:

**Tabella 4: Gramm-Leach-Bliley**

Requisiti Gramm-Leach-Bliley relativi a comunicazioni e informazioni personali	Come Assentor Enterprise garantisce la conformità
Richiedono a tutti gli istituti finanziari di studiare, implementare e applicare misure di sicurezza finalizzate a tutelare le informazioni dei clienti.	Assentor è in grado di identificare informazioni personali grazie alla tecnologia NLCA e mette automaticamente in quarantena presunte violazioni al Gramm-Leach-Bliley Act che l'addetto alla conformità provvederà a riesaminare.

## FSA (Regno Unito)

La Financial Services Authority (FSA) è un ente indipendente non governativo che si occupa di tutelare e sostenere i mercati finanziari e assicurativi del Regno Unito. Ai sensi del Money Laundering Act (legge anti-riciclaggio), la FSA richiede a tutti gli istituti finanziari di conservare documenti pertinenti (cartacei ed elettronici) per un minimo di 5 anni, compresi quei documenti di identificazione dei clienti (al termine del rapporto con un cliente); documenti relativi a ciascuna transazione completata per un cliente; documenti relativi a clienti insolventi - documenti relativi all'insolvenza e provvedimenti adottati per recuperare un credito; documenti di reporting interni ed esterni.

Le linee guida FSA richiedono alle società di conformarsi alle seguenti linee guida in materia di posta elettronica:

**Tabella 5: FSA (Regno Unito)**

Requisiti FSA	Come Assentor Enterprise garantisce la conformità
Richiedono a tutti gli istituti finanziari di conservare documenti elettronici pertinenti per un minimo di 5 anni.	Assentor Enterprise garantisce periodi di conservazione flessibili ed è in grado di archiviare messaggi e-mail e allegati, instant message e documenti, offrendo la possibilità di creare un indice intelligente di tutte le voci che compaiono all'interno dei messaggi o di altro contenuto presente in archivio.

## PIPEDA (Canada)

Questa normativa canadese è simile a SOX e GLB per aziende operanti in territorio canadese. Richiede alle aziende di tutelare i dati personali.

Per conformarsi alla normativa canadese PIPEDA, le società devono soddisfare i seguenti requisiti:

**Tabella 6: PIPEDA (Canada)**

Requisiti PIPEDA	Come Assentor Enterprise garantisce la conformità
La legge tutela i dati personali di individui, dipendenti, clienti o contatti. Queste informazioni includono qualsiasi informazione di identificazione personale presente in documenti cartacei/elettronici o e-mail. PIPEDA tutela tutti gli indirizzi di abitazioni private o indirizzi e-mail presenti in curriculum o documenti del personale, file dipendenti, qualsiasi tipo di documento tra cui: informazioni creditizie, prestiti, documentazione medica, fedina penale, situazione fiscale, ecc. Tutte le organizzazioni pubbliche, private e senza fini di lucro canadesi devono conformarsi alle normative PIPEDA, specialmente nell'uso della posta elettronica.	Assentor offre un'efficace analisi del contenuto con oltre 3.000 modelli "pronti all'uso" in grado di identificare quei messaggi e-mail che contengono un certo numero di elementi (ad es. numeri di conto, numeri di serie) o classi di contenuto compresi dati personali non di dominio pubblico. Le aziende possono inoltre bloccare messaggi e-mail in uscita che contengono questo tipo di dati utilizzando uno strumento di gestione flessibile, che può essere personalizzato in base ai singoli gruppi o addirittura al singolo dipendente.

## Statuto IDA 29.7 (Canada)

Gli emendamenti allo Statuto IDA (Associazione dei promotori finanziari canadesi) 29.7 stabilisce che le aziende sono tenute ad archiviare e monitorare tutta la corrispondenza. Con il termine corrispondenza si definisce "qualsiasi comunicazione scritta o in formato elettronico inerente l'attività aziendale redatta allo scopo di essere inviata ad un singolo cliente attuale o potenziale, e non allo scopo di essere divulgata a molteplici clienti o al grande pubblico." In virtù di questa definizione, è necessario archiviare e monitorare anche i messaggi e-mail e gli instant message.

Per conformarsi allo Statuto canadese IDA 29.7, le società devono soddisfare i seguenti requisiti:

**Tabella 7: Statuto 29.7 (Canada)**

Requisiti Statuto IDA 29.7	Come Assentor Enterprise garantisce la conformità
La sezione 29.7(3) richiede che la revisione e la supervisione della corrispondenza vengano eseguite mediante autorizzazione pre- e post-utilizzo e campionamento post-utilizzo, a seconda del tipo di materiale.	La scansione dei messaggi può essere eseguita nelle modalità pre-verifica, post-verifica o post-elaborazione. Assentor Compliance mette in quarantena i messaggi a seconda della modalità di elaborazione scelta dall'azienda: In modalità <b>pre-verifica</b> , Assentor Compliance elabora le e-mail in tempo reale ed è in grado di ritardarne o impedirne il recapito se un messaggio è scritto in una lingua sospetta. In questo caso, prima di poter inviare il messaggio un addetto alla conformità dovrà adottare i dovuti provvedimenti. In modalità <b>post-verifica</b> , Assentor Compliance elabora le e-mail in tempo reale ma non ne impedisce il recapito. In questo caso, l'addetto alla conformità deve ancora verificare il messaggio e adottare i dovuti provvedimenti. In modalità <b>post-elaborazione</b> , Assentor Compliance elabora copie di messaggi che sono già stati recapitati.

Requisiti Statuto IDA 29.7	Come Assentor Enterprise garantisce la conformità
La sezione 29.7(5) richiede che tutta la corrispondenza e la documentazione relativa agli interventi di supervisione venga conservata e che sia sempre disponibile per l'ispezione da parte della IDA. Tutta la corrispondenza e i relativi documenti devono essere conservati per un periodo di cinque (5) anni dalla data di creazione.	Tutti i messaggi catturati da Assentor dispongono di log di audit anti-manomissione e bollatura oraria e possono essere conservati su una vasta gamma di dispositivi WORM. La documentazione relativa ai controlli è sempre disponibile e può essere mostrata su richiesta agli addetti al momento del controllo. Assentor Enterprise garantisce periodi di conservazione flessibili ed è in grado di archiviare messaggi e-mail e allegati, instant message e documenti, offrendo la possibilità di creare un indice intelligente di tutte le voci che compaiono all'interno dei messaggi o di altro contenuto presente in archivio.

### UMIR Policy 7.1 (Canada)

Le normative UMIR per i mercati canadesi (Universal Market Integrity Rules for Canadian Marketplaces) 7.1 richiedono l'implementazione di una supervisione della conformità e un sistema di protezione. Questa normativa interessa le aziende che si occupano di fondi di investimento e i promotori registrati che rientrano nella giurisdizione della IDA.

Per conformarsi alle disposizioni della normativa UMIR 7.1, le società devono soddisfare i seguenti requisiti:

**Tabella 8: Normativa UMIR 7.1 (Canada)**

Requisiti Normativa UMIR 7.1	Come Assentor Enterprise garantisce la conformità
Alle aziende viene richiesta l'implementazione di un sistema di supervisione costituito da politiche e procedure finalizzate a impedire eventuali violazioni, e da procedure di conformità finalizzate all'individuazione di violazioni, laddove queste si verificano.	Assentor Compliance impedisce che messaggi con contenuto sospetto giungano al destinatario, fornisce una gestione centralizzata delle politiche relative al contenuto e conserva una documentazione permanente dei risultati e di tutti gli eventi associati. Oltre alla sofisticata tecnologia NLP, Assentor consente alle aziende di creare il proprio lessico personalizzato e categorie di problemi garantendo così alle aziende precisione e flessibilità. La scansione dei messaggi può essere eseguita nelle modalità pre-verifica, post-verifica o post-elaborazione. Assentor Compliance mette in quarantena i messaggi in base alla modalità di elaborazione scelta dall'azienda.
Controllo del sistema di revisione almeno una volta all'anno al fine di verificare che continui ad essere adeguatamente impostato per prevenire e rilevare eventuali violazioni dei requisiti. Potrebbero essere necessari controlli più frequenti se in occasione di controlli precedenti sono stati rilevati problemi di supervisione e conformità. I risultati di questi controlli devono essere conservati per almeno cinque anni.	Assentor offre dettagliate funzioni di reporting e auditing al fine di garantire un efficace lavoro di monitoraggio e supervisione.
Conservazione dei risultati di tutti i controlli di conformità per almeno cinque anni.	Tutti i messaggi catturati da Assentor dispongono di log di audit anti-manomissione e bollatura oraria e possono essere conservati su una vasta gamma di dispositivi WORM. La documentazione relativa ai controlli è sempre disponibile e può essere mostrata su richiesta agli addetti al momento del controllo.

## Normative regionali

### Normative sulle polizze di assicurazione

Ciascuno dei 50 stati degli Stati Uniti dispone di normative che regolamentano la vendita e la promozione di assicurazioni, nonché di limitazioni su chi può dire cosa in termini di polizze assicurative. Il CARFRA sta tentando di stabilire normative federali in materia di assicurazione, ma il processo è tuttora in corso.

Le normative regionali in merito alla vendita e alla liquidazione delle assicurazioni richiedono alle società di conformarsi alle seguenti linee guida in materia di posta elettronica:

**Tabella 9: Normative che regolano il sistema assicurativo**

Requisiti assicurativi	Come Assentor Enterprise garantisce la conformità
Ciascuno stato dispone di indicazioni e normative su chi può parlare a chi (certificazione), di che cosa (promotori finanziari), in che termini questi possono descrivere determinate polizze (terminologia della polizza e metro di paragone). Tutti gli stati si attengono a precise normative sulla tempistica da adottare nel rispondere ad eventuali contestazioni. I "viatical settlement" e i "guarantee funds" sono rigorosamente regolamentati in tutti gli stati.	Grazie all'impiego della tecnologia NLA allo stato dell'arte, Assentor è in grado di identificare potenziali violazioni delle polizze di assicurazione in oltre 15 categorie.

### Florida Sunshine Laws

Nel 1909, la Florida fu il primo stato ad approvare quella che è diventata famosa come la "Public Records Law," Capitolo 119 dello Statuto della Florida. Questa legge sancisce che qualsiasi documento redatto o ricevuto da una qualsiasi agenzia pubblica nel corso della sua attività ufficiale deve essere conservato a scopo di ispezione, salvo specifica esenzione da parte della legislatura. Nel corso degli anni, la definizione di "documenti pubblici" è arrivata a includere non solo i tradizionali documenti scritti quali carte, mappe e libri, ma anche nastri, fotografie, film, registrazioni con sonoro e documenti conservati nei computer ed e-mail. Molti altri stati hanno adottato leggi simili in materia di conservazione delle e-mail per lunghi periodi di tempo.

Le Florida's Sunshine Laws richiedono alle società di conformarsi alle seguenti linee guida in materia di posta elettronica:

**Tabella 10: Florida Sunshine Laws**

Requisiti Florida Sunshine Laws	Come Assentor Enterprise garantisce la conformità
Stabiliscono che le e-mail spedite o ricevute da dipendenti statali sono documenti pubblici e come tali sono soggetti a divulgazione pubblica, salvo specifica esenzione. La legge sancisce inoltre che "un documento pubblico può essere distrutto o eliminato in altro modo solo in conformità dei piani di conservazione stabiliti dalla Division of Library and Information Services del Dipartimento di Stato."	La ricerca e il recupero di messaggi e allegati dall'archivio Assentor possono essere eseguiti agevolmente grazie ad una ricerca sul web. Assentor supporta una vasta gamma di dischi (IBM DR 450, NetApp SnapLock, EMC Centera, Permabit Permeon), dispositivi ottici e su nastro con funzioni WORM (Write Once Read Many). Assentor prevede la possibilità di stabilire politiche flessibili in materia di conservazione dei documenti.

## Normative che regolamentano il sistema sanitario e farmaceutico

### HIPAA

L'Health Insurance Portability and Accountability Act del 1996 (HIPAA) stabilisce standard di privacy per il trattamento dei dati personali dei cittadini e delle loro cartelle mediche, fornendo ai pazienti maggiore accesso alla propria documentazione medica e l'autorità di decidere come le organizzazioni sanitarie possono utilizzare le loro informazioni personali.

L'HIPAA richiede alle società di conformarsi alle seguenti linee guida in materia di posta elettronica:

**Tabella 11: HIPAA**

Requisiti HIPAA	Come Assentor Enterprise garantisce la conformità
La normativa sulla privacy tutela tutte le "informazioni sanitarie riconducibili a singoli" in possesso o comunicate da un'entità soggetta o da aziende associate, in qualsiasi forma o supporto, sia in formato elettronico, cartaceo o verbale.	Assentor Enterprise è in grado di identificare informazioni personali grazie alla tecnologia NLCA e mette automaticamente in quarantena presunte violazioni alla normativa HIPAA che l'addetto alla conformità provvederà a riesaminare.
Garantisce una migliore conservazione e organizzazione della documentazione medica, compresi documenti e-mail a beneficio dei pazienti.	L'archivio Assentor dispone della tecnologia NLCA e prevede la possibilità di creare un'efficace e utile indicizzazione dell'intestazione e del corpo dei messaggi e di tutti gli allegati al fine di identificare tutti gli elementi significativi che contribuiscono ad una rapida ricerca e recupero dei dati.

## Food and Drug Administration (FDA) Enforcement Policy

La "Enforcement Policy 21 CFR Part 11; Electronic Records: Electronic Signatures (CPG 7135.17)" USDA stabilisce che i documenti aziendali creati e conservati in formato elettronico devono essere conformi agli stessi requisiti di archiviazione dei documenti cartacei (compresi audit trail, sicurezza di sistema, autotest del sistema, ecc.). Diventata legge nel 1997, questa normativa prevede che in determinate circostanze, i documenti elettronici devono essere considerati alla stregua di documenti cartacei, e le firme elettroniche come aventi lo stesso valore legale delle firme scritte a mano.

Le linee guida della FDA Enforcement Policy richiedono alle società di conformarsi alle seguenti linee guida in materia di posta elettronica:

**Tabella 12: FDA Enforcement Policy**

Requisiti della FDA Enforcement Policy	Come Assentor Enterprise garantisce la conformità
I documenti aziendali creati e conservati in formato elettronico devono essere conformi agli stessi requisiti di archiviazione dei documenti cartacei (compresi audit trail, sicurezza del sistema, autotest del sistema, ecc.).	Assentor Enterprise permette periodi di conservazione flessibili ed è in grado di archiviare messaggi e-mail e allegati, instant message e documenti. L'archivio Assentor dispone della tecnologia NLCA e prevede la possibilità di creare un'efficace e utile indicizzazione dell'intestazione e del corpo dei messaggi e di tutti gli allegati al fine di identificare tutti gli elementi significativi che contribuiscono ad una rapida ricerca e recupero dei dati. Assentor supporta una vasta gamma di dischi (NetApp SnapLock, EMC Centera), dispositivi ottici e su nastro con funzioni WORM.

## Normative che regolamentano il settore energetico

### FERC (CFR TITLE 18)

Il Federal Energy Regulatory Committee (FERC) attraverso il Dipartimento dell'Energia richiede specificatamente periodi di conservazione per determinati tipi di corrispondenza.

FERC richiede alla società di conformarsi alle seguenti linee guida in materia di posta elettronica:

**Tabella 13: FERC**

Requisiti FERC	Come Assentor Enterprise garantisce la conformità
Articolo 18 Capitolo 23 Corrispondenza e documentazione relativi alla creazione di tariffe e conformità delle stesse, classificazioni, division sheet e circolari inerenti al trasporto di beni. Devono essere conservati per i 2 anni successivi l'annullamento della tariffa.	Assentor combina la sua capacità di stabilire periodi flessibili di conservazione con le funzioni Natural Language in grado di identificare significati pertinenti all'interno di un messaggio (e-mail, IM o altro).

## Normative che regolamentano il settore militare e il governo federale

### DOD 5015.2 (Stati Uniti)

Il Dipartimento della Difesa si avvale di comprovate linee guida che regolamentano il software per la gestione dei documenti elettronici, "5015.2", che costituisce una serie di indicazioni DOD sulle modalità di conservazione dei documenti elettronici. L'articolo 5015 specifica che i documenti da conservare comprendono e-mail, documenti di pianificazione, documenti di distruzione, audit di sistema e altri. Tutti i documenti conservati devono poter essere accessibili per ricerche e stampa e presentare un indice che tenga conto dei seguenti elementi: data dell'eliminazione, distruzione, posizione, trasferimento o posizione di accesso, revisione di documenti importanti e data o durata del ciclo di aggiornamento, identificatore della categoria di documenti, identificatore univoco della cartelle e campi definibili dall'utente.

Le linee guida DOD 5015.2 richiedono alle società di conformarsi alle seguenti linee guida in materia di posta elettronica:

**Tabella 14: DOD 5015.2**

Requisiti DOD 5015.2	Come Assentor Enterprise garantisce la conformità
Indicano la posta elettronica come un tipo di documento.	IBM DB2 Content Manager for Data Retention Compliance, guidato da Assentor, offre la possibilità di classificare un messaggio o un documento come documento aziendale, che in quanto tale sarà soggetto al completo processo di gestione per tutto il suo ciclo di vita.
Tutti i documenti conservati devono poter essere accessibili per ricerche e stampa e presentare un indice che tenga conto dei seguenti elementi: data dell'eliminazione, distruzione, posizione, trasferimento o posizione di accesso, revisione di documenti importanti e data o durata del ciclo di aggiornamento, identificatore della categoria di documenti, identificatore univoco della cartelle e campi definibili dall'utente.	Tutti i documenti conservati in IBM DB2 Content Manager for Data Retention Compliance possono essere oggetto di ricerche, stampati e sono presentati sotto forma di indice, cosa che consente quindi di condurre ricerche federate. Questo sistema assegna al documento in questione appropriate regole di conservazione e distruzione e darà inizio alla distruzioni o al trasferimento dei messaggi in questione all'interno dell'applicazione aziendale. La stessa infrastruttura e gli stessi procedimenti che regolamentano la conservazione dei documenti vengono utilizzati per la gestione dei tradizionali documenti cartacei aziendali, l'individuazione di cartelle e caselle, l'applicazione di codici a barre e la gestione dello spazio di memoria fisico. Le funzioni Declare, Classify e di gestione del ciclo di vita incorporate in questa applicazione ne fanno una soluzione conforme a US DoD 5015.2.

## NARA GRS20 (US)

La National Archives and Records Administration (NARA), un'agenzia federale indipendente che sovrintende alla gestione di tutti i documenti federali, si occupa dello sviluppo del General Record Schedule (GRS). Si tratta di un sistema utilizzato dalla NARA in cui l'eliminazione dei documenti elettronici (compresi e-mail, documenti di word processing, fogli di calcolo, ecc.) è possibile solo dopo che questi sono stati copiati su carta, microfilm o su un sistema elettronico di conservazione dei documenti.

Le linee guida NARA GRS20 richiedono alle società di conformarsi alle seguenti linee guida in materia di posta elettronica:

**Tabella 15: NARA GRS20**

Requisiti NARA GRS20	Come Assentor Enterprise garantisce la conformità
Richiede che i documenti elettronici, e-mail comprese, vengano conservati fin quando non saranno stati copiati su carta, microfilm o su un sistema di conservazione dei documenti.	Assentor permette periodi di conservazione flessibili ed è in grado di stabilire norme di archiviazione e cancellazione per messaggi e-mail e allegati, instant message e documenti.

## Normative che regolamentano il settore delle telecomunicazioni

Le società di telecomunicazioni che operano in territorio statunitense si debbono attenere alla normativa federale CFR Articolo 47, Parte 42 che richiede alle società di conservare i documenti relativi a tutte le comunicazioni elettroniche con i propri clienti.

Le leggi statali riportate di seguito vengono applicate nello specifico a ISP e ad altri fornitori di servizi.

### UK Data Protection Act del 1998

Questa legge britannica è in vigore dal marzo 2000. Il suo obiettivo è tutelare dati personali sensibili garantendo ai singoli il diritto di accedere ai propri documenti personali.

Il UK Data Protection Act richiede alle società di conformarsi alle seguenti linee guida in materia di posta elettronica:

**Tabella 16: UK Data Protection Act**

Requisiti UK Data Protection Act	Come Assentor Enterprise garantisce la conformità
Richiede ai fornitori di servizi di conservare documenti completi e organizzati dei dati dei propri clienti.	L'archivio Assentor dispone della tecnologia NLCA e prevede la possibilità di creare un'efficace e utile indicizzazione dell'intestazione e del corpo dei messaggi e di tutti gli allegati al fine di identificare tutti gli elementi significativi che contribuiscono ad una rapida ricerca e recupero dei dati. Assentor offre la possibilità di condurre ricerche più dettagliate grazie alle funzioni di ricerca full-text e di organizzare grandi quantità di dati in diverse cartelle.

### US Electronic Communications Act del 1996

Questa legge comprende una sezione sul diritto di sequestro, da parte di organismi che tutelano l'applicazione della legge, di e-mail lette e non lette conservate da un fornitore di servizi per un massimo di un anno.

L'US Electronic Communications Act richiede alla società di conformarsi alle seguenti linee guida in materia di posta elettronica:

**Tabella 17: US Electronic Communications Act**

Requisiti dell'US Electronic Communications Act	Come Assentor Enterprise garantisce la conformità
Conservazione delle e-mail per un massimo di un anno.	Assentor permette periodi di conservazione flessibili ed è in grado di archiviare messaggi e-mail e allegati, instant message e documenti.

## Conclusione

"Ciò che accomuna tutte le normative è l'esigenza di garantire massima sicurezza e privacy nonché tutelare le informazioni per tutto il loro ciclo di vita, partendo dalla loro creazione, passando attraverso il periodo di utilizzo attivo fino ad arrivare alla fase di archiviazione e conservazione a lungo termine. Il fatto che le organizzazioni regolamentate siano soggette a controlli sulle loro soluzioni e prassi di conformità implica l'esigenza di un'efficiente individuazione e recupero dei documenti rilevanti. Sebbene il valore e la frequenza di accesso ad un particolare documento si riducano nel tempo, il rischio di inadempienza a causa di un trattamento non conforme dei documenti è di gran lunga troppo elevato per essere ignorato."

La sostanziale crescita nell'uso della posta elettronica e di caselle di posta aziendali, parallela alla proliferazione di nuove normative, pone nuove e sempre maggiori pressioni sulle organizzazioni IT. La conformità non è un'opzione – al contrario è fondamentale, in quanto funge da forza motrice alla base della creazione e della conservazione di più tipi di informazioni e documenti. I procedimenti e le tecnologie attuali devono essere rivisti e in molti casi aggiornati/sostituiti per poter sostenere la richiesta di memorizzazione di un maggior numero di documenti per periodi di tempo più lunghi e l'esigenza di dover recuperare e dimostrare su richiesta l'autenticità dei documenti. Assentor Enterprise fornisce la soluzione e le capacità necessarie a soddisfare le richieste di queste normative.

Per maggiori informazioni su come adeguarsi alle conformità normative, rivolgersi a CA, iLumin Division al numero +1-703-880-1347, e-mail [info@ilumin.com](mailto:info@ilumin.com) oppure visitare il nostro sito web all'indirizzo [www.ilumin.com](http://www.ilumin.com).

## Background societario

CA International, Inc. (NYSE:CA), la più grande società produttrice di software di gestione al mondo, offre soluzioni software per la gestione di sicurezza, storage, ciclo di vita e servizi in grado di ottimizzare le performance e l'efficienza degli ambienti IT aziendali. Per maggiori informazioni visitare il sito web [ca.com](http://ca.com).

## Proprietà e riservatezza

Le informazioni contenute nel presente documento sono riservate e di proprietà di CA International, Inc. È vietato divulgare a terzi tanto l'esistenza del documento quanto le informazioni ivi contenute senza previo consenso scritto da parte di CA. Il presente documento potrebbe non venire utilizzato per altro scopo, se non quello di strumento di valutazione interna della tecnologia CA.

CA, iLumin Division 1881  
Campus Commons Drive, Suite 400, Reston, VA 20191 USA  
(Tel) 703-481-8627 | (Fax) 703-481-8672  
[www.ilumin.com](http://www.ilumin.com)

<sup>5</sup> Enterprise Strategy Group