

## Regulatory Challenges for Schools

Educators know that the Internet is a double-edged sword. While easy Internet access means students have a wealth of valuable information at their fingertips, the Internet also delivers material and unwanted agents that can harm both students and your school's networks.

When it comes to your school's Internet access and messaging protocols, regulatory compliance continues to be a particularly challenging issue, with schools subject to legislation such as CIPA (Child Internet Protection Act), and even HIPAA (Health Insurance Portability and Accountability Act). Complying with these regulations, while trying to provide an enriched learning experience for students, becomes even more difficult in the face of shrinking school budgets. That's why EdgeWave Secure Content Management solutions including iPrism Web Security, originally created for schools, EdgeWave Email Security and EdgeWave Email Archive offer the ideal combination of value, simplicity and performance that schools require.



## CIPA Compliance

Congress moved to protect students and schools with the Child Internet Protection Act (CIPA), passed in 1999. CIPA was created and tied to E-rate funds in order to induce elementary and secondary schools and libraries to take measures to filter and block unwanted Internet content from reaching students. The E-rate program helps schools and libraries pay for products and services such as Internet access, internal network connections and telecommunications and are an important funding adjunct to school budgets. Most schools are aware of CIPA requirements and have deployed a Web filter per this legislation's mandate. However, students' success in circumventing many filters by using anonymous browsing sites or non-sanctioned protocols can open schools to non-compliance and a loss of important e-rate funds.

## HIPAA Compliance

Many schools may not be aware that they are also subject to HIPAA compliance. The Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress in 1996 in response to several issues facing health care coverage, privacy, security, and fraud in the United States.

**Need for Uniformity** – Before HIPAA, rules and regulations varied by state and organization and there was no consistency. In addition there was no standard authority for enforcement of fraud and abuse that applied to state and federal health care programs.

**Need for Privacy and Security Standards** – Congress recognized the increased use of electronic technology, the potential for abuse or compromise, and the need to establish security and privacy standards for it. We have all heard news stories about electronic information being mistakenly lost, stolen, or inadvertently sent to the wrong place. The risks were much higher if electronic patient information were compromised considering the current communications environment. Schools might mistakenly think that because the Family Educations

Rights Privacy Act (FERPA) has jurisdiction over school health records, they are not subject to HIPAA rules. This is not the case. Because schools keep health records and may have healthcare workers on-site, such as a school nurse, they are in effect performing or assisting in the performance of an activity or function that involves the disclosure of protected health information. Examples include a physician or nurse working in conjunction with school officials to promote student health during the school day and sending protected health information about students to the school's district office. In this case, private health information has been transmitted and is covered by HIPAA regulations. In another example, you may be providing your staff and faculty with Flexx spending accounts for their medical coverage. Any health information transmitted as a result of these benefits would also be covered under HIPAA. Failure to comply with HIPAA regulations can result in severe fines and schools that are lax in this regard could be open to litigation.

## Internet-Based Threats

The Web is replete with threats that can cause direct and collateral damage to your school including the risk of non-compliance. The exposure of private student information via hacker exploits can have catastrophic consequence including non-compliance fines and convictions, lawsuits, network damage, student access to inappropriate content and more. iPrism Web Security, the secure Web gateway originally designed for schools offers the features and functionality you need to protect your students and networks from current and emerging Internet-based threats.

**Circumvention Attempts** – Circumvention techniques are becoming more sophisticated every day and easily accessible to your students. Circumventing school networks not only exposes students to inappropriate content, it can be a portal for damaging botnets and other criminal malware to enter your network.

**iPrism Circumvention Defense Network (CDN)** – iPrism’s CDN blocks attempts by circumvention tools to connect, rendering them harmless and protecting your school from opening the network to criminal malware designed to steal data. Once the circumvention threat has been blocked, iPrism’s Email Alerts and Real-Time Monitor features can be used to address the transgressors and take more serious action if required.

**Botnets, a New and Dangerous Trend** – Bots are autonomous applications created by cybercriminals for financial gain. Their creators form vast networks of these applications that can infect networks and do massive damage before they are detected. Botnets are created when bots “phone home” for instructions to a command and control center outside. These botnet networks, usually referred to as “zombies”, are controlled by hackers to do their bidding such as stealing private data.

**iPrism ThreatSTOP Botnet Technology** – iPrism Web Security leverages the ThreatSTOP Botnet Threat List to prevent bots from ‘phoning home’ and forming botnets. Bots that are unable to contact command and control outside your network, are never activated to do harm. Once a bot has been detected and blocked, users are alerted via email and Real-Time Monitor so they can remediate compromised endpoints, knowing that the immediate threat has been mitigated. iPrism on-box reporting will show compliance with regulations that protect users’ identities and data.

**iPrism Defense Against Viruses and Other Malware** – Even if you are already using an antivirus solution, our antivirus adds another layer of security by scanning all incoming HTTP traffic and blocking malware before it can reach your end-users. Our antivirus engine employs port-agnostic real-time scanning of web traffic for threats, known and unknown, on all allowed web pages using a unique four-factored system for dynamically detecting and blocking Internet-based viruses, worms and other malware.

**More Defense with Application Controls** – iPrism offers application controls that reduce the risks associated with unsanctioned application communications. These applications, which include popular IM and P2P protocols, not only erode productivity and drain bandwidth; they can open serious security gaps where bot-related malware and viruses can invade your network. iPrism allows you to monitor and block IM and P2P applications such as Skype and FTP with a simple set-and-forget check box.

## Email-Based Threats

Email is another access point that if not secured can undermine your efforts to stay compliant. Unfortunately, the technologies that make data easy to access and share also increase the risk of unauthorized disclosure and loss of sensitive, protected data. EdgeWave Email Security with optional Email Data Compliance includes the powerful tools you need to assure protection of private data of your students and staff and efficient delivery of legitimate mission-critical email. You can further bolster your email security with EdgeWave Secure Archive, which will retain all your email in an unalterable state should you ever need to retrieve it for compliance or legal issues.

**EdgeWave Email Data Compliance** – This optional service includes a content analysis and policy engine that uses proprietary technology

“With iPrism, our school not only meets, but exceeds compliance requirements for CIPA and state of Pennsylvania mandates. You can’t put a price on that kind of value add.”

— Michael White, Systems Administrator,  
Nueva Esperanza Academy

to detect private information transmitted via outgoing email. This data protection technology analyzes data in motion and using compliance-based rules, detects and blocks any sensitive private data from leaving your network. This solution is easily managed from the EdgeWave Email Security central dashboard and can be provisioned within hours to start protecting your organization with the powerful tools you need to comply with government regulations such as HIPAA and others. Email Data Compliance prevents the loss of all types of private data, including student healthcare information, social security numbers and credit card numbers.

**EdgeWave Criminal Malware Defense** – EdgeWave’s Zero-Minute Defense is a multi-layered approach that stops emerging threats before they can get near your network. Our technology incorporates real-time, session-level defenses against malware such as botnets, by employing a system that is automatic, adaptive and behaviorally-based. Our ability to keep these threats out of your email also conserves bandwidth, keeps mailboxes uncluttered, and because they are behaviorally based and key off the botnets’ known sending characteristics, virtually eliminates false-positives. The result is more efficiency and faster delivery of legitimate email.

**EdgeWave Secure Archive** – EdgeWave offers secure email archiving that is scalable to fit the requirements of any size school. All of your email is retained in an unalterable state to help you meet regulatory compliance requirements, possible litigation issues, or storage management needs. As an in-the-cloud solution, you are assured infinite scalability, no time limits on storage and easy retrieval whenever you need to access a message. EdgeWave’s secure data collection technology provides comprehensive interoperability with all messaging systems.

## EdgeWave Secure Content Management Solutions are Ideal for Schools

### iPrism Web Security Features

- **Easy-to-Use Technology** – Lowest TCO – iPrism, the Internet filtering appliance originally designed for schools, provides the low-cost, low-maintenance solution that meets your requirements for accurate and secure filtering while helping you maintain regulatory compliance. In two independent studies, iPrism was found to have the lowest total cost of ownership and lowest total cost of acquisition compared to leading competitors.
- **Maintenance-free, Self-Contained Solution** – iPrism requires no additional hardware or software and one low acquisition price includes everything needed for accurate monitoring, filtering and reporting. Once iPrism is up and running, it operates virtually maintenance-free. iPrism receives automatic database updates every night and in the case of critical security categories, updates can arrive hourly. Product upgrades are also automatically downloaded as they become available.

- **Enhanced Directory Integration** – iPrism authentication incurs no OS conflicts and integrates seamlessly with all major network directories including Novell Netware Directory Services (NDS), Windows Active Directory (including one-way outgoing trust support) for Window 7 and also Mac clients using AD 2003/2008 and Mac OSX Snow Leopard. In addition, as an LDAP variant, it is possible to integrate iPrism Web Filter with OSX Server Open Directory (LDAP v2/v3).
- **Hybrid Remote Filtering** – iPrism’s new Remote Filtering delivers powerful Web security to your remote users without using your VPN and without adding any hardware in your DMZ or requiring browser-specific PAC files.
- **Granular Policy Rules** – iPrism’s convenient central management console lets you create different groups and give them different levels of access, helping you create an environment where teachers, elementary students, high school or college-age students can have different access levels while assuring the safety of each audience and the security of your network.
- **Comprehensive Logging, Real-Time Monitoring and Reporting On-Box** – iPrism’s comprehensive on-box reporting requires no additional hardware or software and includes real-time monitoring and email alerts that give you highly accurate and timely visibility on Internet activity across your school. Reports can be flexibly scheduled and generated using a variety of templates or customized to suit your requirements. Email alerts are generated when security problems are detected allowing you to quickly mitigate threats before they cause damage.
- **ProCare Technical Support Services** – If there ever is a need to call EdgeWave Technical Support, you can count on a quick response. Because iPrism is a self-contained solution with its own hardened and optimized OS, you won’t spend time tracking down the origin of your problem as you would with a software only solution. With iPrism, you only have to make one call.

“The 100% human-review database is one of the primary reasons we chose iPrism. We can depend on the product to be consistently accurate, which is critical in an educational environment.”

— Sherry Hahn, District Technology Director,  
White Salmon Valley School District

## EdgeWave Email Security Features

- **No-Touch Email Protection** - We host the applications and infrastructure required to protect your organization from spam, malware, phishing, viruses and inappropriate content in email.
- **Proven Expertise** - We provide the technology expertise and front line defense required to fight emerging threats so you can focus on growing your business.
- **Easy Set-up and Zero Maintenance** - You can be setup within minutes to start protecting your networks and data, all that’s required is a simple MX path redirect. Nothing to install and zero maintenance - the ultimate in a no-touch solution that conserves your resources. Deployment options include hosted services or on-site managed appliances with Vx failover technology.
- **Infinite Scalability** - EdgeWave Hosted Services scale to fit any size school and can grow with you if your student and staff population increases.
- **160 Hour Email Spooling** – Ours is a fully redundant system backed up with multiple data centers and email spooling for up to 160 hours, so your email is never bounced or lost, in the event of any network problems.
- **Bandwidth Savings** - Eliminating the volume of spam hitting your servers increases your available bandwidth for other internet-based applications. EdgeWave helps reduce bandwidth costs, as well as lessen the burden on your email servers’ archive capacity.
- **Proactive Technical Support** - EdgeWave’s Security Operations Center is staffed around the clock with email experts and security specialists to handle your support needs. They provide proactive monitoring of any email threats to assure continuous service for all EdgeWave domains and users.

## EdgeWave Email Archive Features

- **Easy-to-Use Interface** – EdgeWave Email Archive is easy to set up and includes a role-based administrative dashboard and easy retrieval of all email using the simple end-user search tool.
- **Archiving of all Inbound and Outbound Messages** – All messages are saved in an immutable state, both internal and external, and available when needed to meet regulatory compliance or legal requirements.
- **Unlimited Storage and Time** – In-the-cloud storage means infinite scalability at no additional cost with no capacity or time limitations as long as you are a customer.
- **Complete Interoperability** – EdgeWave Email Archive is compatible with virtually all email systems so seamless integration is assured.

For more detailed information on EdgeWave Secure Content Management solutions, please access our product data sheets online:  
<http://www.edgewave.com/resources/>

### Contact Us

1-800-782-3762

[www.edgewave.com](http://www.edgewave.com)

### Corporate Office

15333 Avenue of Science, San Diego, CA 92128

Phone: 858-676-2277

Fax: 858-676-2299

Toll Free: 800-782-3762

Email: [info@edgewave.com](mailto:info@edgewave.com)