General HIPAA Implementation FAQ

What is HIPAA?

Signed into law in August 1996, the Health Insurance Portability and Accountability Act ("HIPAA") was created to provide better access to health insurance, limit fraud and abuse and reduce administrative costs in the health care industry. HIPAA included several sections, including one titled Administrative Simplification. Under Administrative Simplification, Congress created a process whereby its legislative authority would be delegated in 1999 if it did not establish national standards for transmitting electronic health care transactions, protecting patient privacy, and ensuring the security of individually identifiable health information. By 1999, Congress had not established these national standards so it delegated rule-making authority to the U.S. Department of Health and Human Services ("HHS"). The product of this Congressional delegation of rule-making authority, which is the focus of this document, includes three regulatory sets: 1) Standards for Electronic Transactions, (45 C.F.R. §§ 160 & 162), 2) Standards for Privacy of Individually Identifiable Health Information, (45 C.F.R. §§ 160 & 164), and 3) Security and Electronic Signature Standards, (45 C.F.R. §§ 160 & 142). These three regulatory sets are referred to collectively as the "HIPAA regulations" throughout this FAQ document.

- Standards for Electronic Transactions: This set of regulations addresses electronic interactions among health care providers, health plans, and health care clearinghouses. Transaction standards are intended to standardize the mechanisms of electronic exchange by establishing a format and set of codes for covered transactions.

- Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"): The Privacy Rule establishes standards to protect individually identifiable health information, including:

    - Limiting the nonconsensual use and disclosure of protected health information

    - Describing the individual's rights with respect to uses and disclosures of their protected health information

    - Giving patients the right to access their medical information and to know who else has accessed their health information

    - Restricting most disclosures of protected health information to the minimum necessary for the intended purpose

    - Establishing criminal and civil sanctions for violating the rule

- Security Standards: These regulations set a security standard for protecting health information. They address the following three categories of system security requirements:

  Administrative safeguards – documented, formal policies and procedures that are intended to manage the selection and execution of security measures to protect data and manage the conduct of personnel in relation to the protection of data.

  Physical safeguards – the protection of physical computer systems and the buildings holding such systems from natural and environmental hazards and inappropriate intrusion or removal

  Technical safeguards – processes put in place to protect information, authenticate users, and control individual access to information.

Who has to comply with the HIPAA?

The HIPAA regulations apply to "covered entities," groups that include health plans, health care clearinghouses, and health care providers. Under the Standards for Electronic Transactions and the Standards for Privacy of Individually Identifiable Health Information covered entities include health plans, health care clearinghouses, and health care providers that transmit any health information in electronic form in connection with a standard transaction. Under the Security Standards covered entities include health plans, health care clearinghouses when transmitting and receiving a standard transaction, and health care providers when transmitting an electronic transaction. Through these covered entities the HIPAA regulations also reach other non-covered entities called "business associates" and "trading partners." Business associates are contractors who assist or perform functions on behalf of covered entities and trading partners are entities that transmit health information in standardized electronic form with covered entities. Oftentimes, a covered entity's business associates are also its trading partners, but this is not always the case. Sometimes, an entity may be a covered entity, business associate and trading partner of another covered entity, but these determinations are fact intensive and should be made independently. Regardless of an entity's classification under HIPAA, the HIPAA regulations require covered entities that interact with business associates and trading partners to enter into contracts called business associate and trading partner agreements. To satisfy the HIPAA regulations, these agreements must contain specific provisions, including (but not limited to) the following:

- A description of the permitted uses and disclosures of an individual's health information
- Appropriate safeguards of records
- Reports of any unauthorized disclosures to the covered entity

- An agreement that protected health information will be available for inspection, amendment, and accounting by patients

- An agreement that a business associate's books and records related to its functions performed on behalf of a covered entity are available for inspection by HHS.

- A requirement that protected health information related to the covered entity be either destroyed or returned to the covered entity at the time of termination of the contract.

Since the HIPAA regulations directly apply only to covered entities, only covered entities are subject to the enforcement jurisdiction of the Office of Civil Rights, the government entity charged with enforcing the HIPAA regulations. Consequently, covered entities may be held accountable for the non-compliant acts of their business associates and trading partners. According to the HIPAA regulations, this liability may be appropriate when the covered entity knew that there was a pattern of violations by the business associate or trading partner and failed to take reasonable steps to resolve the violation.

What are Express Scripts' obligations under HIPAA?

Express Scripts has more than one role under the HIPAA regulations. While Express Scripts' mail service and Specialty Distribution Services (SDS) may be covered entities in their capacity as health care providers, its Pharmacy Benefits Management (PBM) business serves as a business associate and trading partner of many covered entity clients. Consequently, Express Scripts recognizes that appropriate processes, procedures, and technical changes must be made to ensure timely compliance.

Express Scripts aims to comply with all aspects of HIPAA that relate to us as a health care provider, business associate and trading partner by the applicable compliance dates. While we will communicate with our clients as we integrate HIPAA requirements into our business processes, both parties are independently responsible for complying with all laws and regulations applicable to their respective businesses, including laws and regulations regarding patient data and confidentiality.

When will Express Scripts comply with the HIPAA Regulations?

The three regulatory sets (privacy, security, and electronic transactions) promulgated under the Administrative Simplification provision of HIPAA each have unique requirements and applicable compliance dates. In order to better serve its members and clients, Express Scripts is actively involved in a process to ensure that it will comply with the HIPAA regulations by the required dates indicated below.

HIPAA Timelines

HIPAA Regulation	Express Scripts' Anticipated Compliance Date
Electronic Transactions	October 2002 (PBM Component) October 2003 (Provider Components)

Privacy	April 2003 (All Express Scripts' Components)
Security	April 2005 (All Express Scripts' Components)

When will Express Scripts implement systems changes?

The Express Scripts PBM component became compliant with the Standards for Electronic Transactions before the October 2002 compliance date and is now capable of accepting and transmitting applicable Standard Transactions. However, Express Scripts is aware that the Administrative Simplification Compliance Act allowed covered entities to file for a one-year compliance date extension. For this reason, Express Scripts will accommodate transactions from both filing and non-filing covered entities. Express Scripts hopes maintaining this dual functionality will ease pharmacies and clients' transition toward compliance.

What investments is Express Scripts making to ensure timely compliance with HIPAA?

Compliance with HIPAA is an approved corporate initiative. Express Scripts has a full time project management team, including an overall project manager, business requirements project manager and full time managers for privacy and security.

In order to ensure a smooth transition to compliance, Express Scripts created a HIPAA Steering Committee comprised of management personnel who are technical experts in the areas of regulatory compliance, security, and information systems architecture. Through a coordinated effort with the Express Scripts HIPAA Project Management Office, the Steering Committee works to resolve issues and develop appropriate policies and procedures in order to ensure timely compliance. The Steering Committee is chaired by Express Scripts' Vice President and Chief Compliance Officer.

Will the Explanation of Benefits form (EOB) be provided in a HIPAA-compliant format?

Explanation of Benefit (EOB) documents will not need any material alterations. Under HIPAA, EOB correspondence may be sent to a policyholder for purposes of payment even if it discloses PHI about another individual. Express Scripts sends EOBs to the address on file for the policyholder.

Who can I contact with more HIPAA questions?

Please contact your Account Manager with questions.

Standards for Electronic Transactions FAQ

Which standard transactions will Express Scripts support?

Express Scripts will support the following transactions and their associated implementation specification:

- NCPDP Version 5.1 – Pharmacy Claims
- NCPDP Version 5.1 – Eligibility Verification (request from retail pharmacies)
- ASC X12N 835- Payment and Remittance Advice
- ASC X12N 834 – Benefit Enrollment and Maintenance

Will Express Scripts mandate enrollment information from its health plan clients be sent using the ASC X12N 834 transaction?

Express Scripts will ask its clients what their intentions are with regard to the electronic transmission of enrollment information since the client usually is the covered entity who is responsible to determine whether supporting the ASC X12N 834 transaction is required. Express Scripts will accept the ASC X12N 834 transaction if its clients determine that the 834 transaction format must be used to send enrollment data to Express Scripts.

Will Express Scripts process the medical data codes sets named in HIPAA; ICD-9CM, CPT-4, HCPCS, and NDC codes?

The only medical data codes set named in HIPAA which Express Scripts processes is the NDC. Other code sets continue to be utilized as applicable per the standard implementation guides.

Have you identified the gaps between the data content currently required and that required by HIPAA?

Express Scripts has conducted a gap analysis and has implemented the changes necessary to make our systems HIPAA compliant. Express Scripts does not anticipate that clients will be required to collect new or different data.

How has Express Scripts been involved in testing the Standards for Electronic Transactions?

Express Scripts has followed the Strategic National Implementation Process (SNIP) testing schedule for transaction standards. Express Scripts is an active member of WEDI/SNIP and NCPDP and has participated in the PDX/NHIN testing initiative, an initiative that facilitated testing between multiple pharmacy and PBM organizations. In addition, Express Scripts has performed testing for the remaining standard transactions with some of our clients and pharmacy partners.

How will Express Scripts ensure that there is no substantial decline in the level of processing time during the implementation of the standards for electronic transactions?

Express Scripts does not anticipate its clients will experience any substantial disruptions in transactional processing time as a result of its HIPAA implementation efforts. Express Scripts has made significant allocations of business and information systems resources to ensure timely compliance with the HIPAA regulations and to minimize any client service disruptions.

What industry groups or Designated Standards Maintenance Organizations (DSMOs) is Express Scripts involved with?

Aside from its internal compliance efforts, Express Scripts participates in the Workgroup for Electronic Data Interchange/Strategic National Implementation Process (WEDI/SNIP) workgroup on HIPAA. Express Scripts is also an active member of the National Council for Prescription Drug Programs (NCPDP) and the X12 organization to insure our involvement in the development of industry standards.

What is the Compliance Act passed by Congress?

In response to concerns raised by many covered entities, the United States Congress passed a statute entitled, "the Administrative Simplification Compliance Act." This statute enables covered entities to file for a one year compliance extension, which means that these filing covered entities will have until October 2003 to comply with the Standards for Electronic Transactions, provided there is proper compliance with the filing requirements.

Did Express Scripts file a Compliance Plan to extend the compliance date of the Standards for Electronic Transactions?

Express Scripts' mail service, Specialty Distribution Service (SDS), and specialty care pharmacies are covered entities and, therefore, were eligible to file for an extension. Express Scripts has already filed an extension for each of these covered entity components. Having done so, these components are not required by law to transmit standard transactions until October 2003.

How long will Express Scripts accept both NCPDP Version 3.2 and 5.1 claims?

Express Scripts plans to support both NCPDP Versions 3.2 and 5.1 until the October 2003 final compliance date.

STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION FAQ

What issues have Express Scripts identified to ensure that member PHI is adequately protected? How will Express Scripts identify and address these issues?

Express Scripts has finalized policies and procedures to ensure the requirements of the Privacy Rule are met. A specialized multi-disciplinary HIPAA implementation team was formed to address organizational issues involving the privacy and protection of health information. This team has collaborated with additional unit personnel to identify and address privacy issues. The HIPAA Team will continue to work with business units, account managers, and others to ensure implementation milestones are achieved in a comprehensive and timely fashion.

How will the Privacy Rule impact the data sharing necessary to implement and maintain a carved-out pharmacy benefit, particularly if integration with health plan data is desired?

The Privacy Rule regulates the manner in which covered entities use and disclose certain types of health information. In addition, the Privacy Rule requires covered entities that share protected health information with other entities to enter into business associate agreements that delineate the rights and responsibilities of both parties with regard to protected health information. Express Scripts intends to meet all Privacy Rule requirements relevant to the services it provides for its members and clients. Although the Privacy Rule impacts the sharing of health information, Express Scripts will work with its clients to ensure that its pharmacy benefit can be appropriately integrated and implemented.

Will Express Scripts enter into a Business Associate Agreement with clients in accordance with the requirements of HIPAA?

Express Scripts has developed a HIPAA contract addendum to its standard PBM Agreement. This addendum has appropriate business associate and trading partner language, and details the rights and responsibilities of each party to protect individually identifiable health information. This addendum also addresses the other mandates of the Privacy Rule. This addendum can be accessed on our web site at www.express-scripts.com.

Will Express Scripts distribute a Notice of Privacy Practices for the proposed plan year?

Yes. Express Scripts' mail service, SDS, and specialty care pharmacies will provide a Notice of Privacy Practices to members who utilize these services and will make a good faith effort to obtain a written acknowledgement of receipt of this Notice. In its role as a PBM, Express Scripts does not anticipate providing a Notice of Privacy Practices on behalf of its covered entity health plan clients. Additionally, Express Scripts does not anticipate assisting clients in the development or distribution of the client's Notice of Privacy Practices.

Will any utilization review, appeals, care management or other plan design applications be affected by the Privacy Rule?

Express Scripts does not anticipate its core business processes will be affected significantly by implementation of the Privacy Rule. Express Scripts is hopeful that HIPAA mandates can be integrated into current business practices without altering the structure and delivery of its pharmacy benefit services. If changes become necessary, clients will be contacted as appropriate.

Does Express Scripts have any internal policies and procedures concerning the privacy of health information?

Express Scripts has finalized policies and procedures necessary to ensure the requirements of the Privacy Rule are met. These policies and procedures reflect HIPAA mandates and are designed to protect health information throughout its storage, maintenance, and transmittal.

Will Express Scripts make its internal policies and practices relating to the Privacy of Individually Identifiable Health Information available to its clients?

For those clients entering into a Business Associate Agreement with Express Scripts, Express Scripts will agree to make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Express Scripts on behalf of, the client available to the client within ten business days, or at the request of the client or the Secretary of HHS, to the Secretary in a time and manner directed by the Secretary, for the purposes of the Secretary determining the client's compliance with the HIPAA Rules. For clients that have asked Express Scripts to enter into a unique or client-specific Business Associate Agreement, the specific requirements of this provision may vary.

Does Express Scripts have a Privacy Officer? What does this person do within Express Scripts?

Yes, Express Scripts has a Privacy Officer. The Privacy Officer is responsible for establishing policies and procedures related to the protection of health information, implementing employee education and training protocols, handling member privacy-related complaints, and performing other activities to ensure HIPAA mandates are met.

Does Express Scripts plan, by April 14th 2003, to satisfy all applicable privacy requirements of HIPAA?

Express Scripts intends to be in compliance with all applicable mandates of HIPAA, including but not limited to, the following privacy specific provisions:

- Erection of physical and electronic barriers to safeguard individually identifiable health information
- Receipt of authorizations from individuals as needed
- Ability to make available to HHS internal books and records for purposes of determining client compliance with HIPAA Privacy requirements
- Establishment of mechanisms to report to clients any improper uses and disclosures of individually identifiable health information
- Establishment of processes to provide individuals with access to their individually identifiable health information and the right to amend that information
- Creation of a process for individuals to lodge complaints and a system for resolving complaints
- Establishment of processes allowing members to exercise other individual rights granted them by HIPAA.

To what extent will Express Scripts disclose information to vendors and subcontractors? How will Express Scripts protect this information under HIPAA?

Potential uses and disclosures of PHI are addressed by Express Scripts' Business Associate Agreement. This agreement details the rights and responsibilities of the parties to use and disclose plan member PHI. In its pharmacy benefit management role, Express Scripts will protect PHI contractually by entering into confidentiality agreements with outside vendors and contractors. Covered entity components of Express Scripts will enter into Business Associate Agreements with those entities that perform services on its behalf.

The Privacy Rule requires covered entities to have the capability to provide an accounting of disclosures to certain individuals. Will Express Scripts provide this accounting of disclosures?

Yes. Express Scripts will maintain an accounting of disclosures as required by the Privacy Rule. Members may request an accounting of disclosures after April 14th 2003 by submitting a written request to Express Scripts.

Does Express Scripts have a procedure for allowing members to request copies or amendments to their protected health information? How will Express Scripts ensure that PHI is available to clients to implement HIPAA's individual rights requirements?

Express Scripts has finalized policies and procedures designed to allow members to inspect, copy, and amend their PHI. Express Scripts' Business Associate Agreement details the rights of a health plan client to access PHI held by Express Scripts on behalf of the client. In this agreement, Express Scripts agrees to provide access, at the request of client (upon reasonable notice and during Express Scripts normal business hours), to PHI in a Designated Record Set (as defined in the HIPAA Rules), to the client or, as directed by the client, to a member, in order to meet the requirements under HIPAA.

What will Express Scripts disclose if a subscriber's spouse or other family member calls requesting explanation of benefit information on behalf of the subscriber?

Member benefit information will be sent only to the subscribing member (i.e., the cardholder). Even in the event a spouse or other dependent family member requests such information, benefit statements will be sent exclusively to the subscribing member.

What changes will be made to on-line service functions to verify user identity?

Express Scripts has finalized policies and procedures regarding member access and verification of requestors. These procedures will encompass establishing the identity of the requestor and verifying authority to access the information requested. In some instances, members may need to provide more information (e.g. date of birth, prescription number) than has been required by past on-line verification practices.

What are Express Scripts' internal privacy audit procedures? Will the audit program be changed in response to HIPAA Privacy?

Express Scripts understands that comprehensive systematic oversight and monitoring is necessary to ensure the effective implementation of any organizational initiative. To provide this oversight and monitoring, Express Scripts will perform ongoing audit functions designed to ensure PHI is protected throughout its storage, maintenance, and transmittal. Organization-wide audits will reflect HIPAA mandates and will test the physical, operational, and technical integrity of our business and information systems.

Will Express Scripts' standard reporting or large case–high dollar reporting packages change as a result of HIPAA?

Express Scripts does not anticipate implementing significant alterations in its current reporting practices across benefit design. If reporting alterations are needed, they will be dealt with on a client-specific basis.

Does Express Scripts anticipate implementing procedures in response to state laws that are more stringent than the federal HIPAA privacy regulation?

It is impossible to know at the moment of the privacy "event" which state law might apply. Express Scripts is a national company with operational sites in several states. Express Scripts contracts with 60,000 pharmacies in 50 states. Express Scripts' clients and their members and members' physicians are in 50 states, and not necessarily the same states. There are numerous privacy "events" that may happen involving multiple states, business associates, provider covered entities and health plan covered entities. Express Scripts' position is that HIPAA is the base level for privacy and there are generally recognized laws or rules in some states that require

"less" disclosure (e.g., HIV information in New York). Express Scripts designed its policies and procedures to allow for the generally applicable and universally recognized stricter rules, but have also informed its practices with a philosophy of the safety and health of members and patients, as well as a respect for the professionals caring for its members.

Will Express Scripts require members to sign individual authorizations before using or disclosing their PHI?

Subject to certain important exceptions (e.g., uses and disclosures for treatment, payment, or health care operations), the HIPAA regulations require covered entities to obtain a written authorization from individuals before using or disclosing the PHI of that individual. In implementing HIPAA, Express Scripts has made every effort to ensure that all uses and disclosures of an individual's PHI are made under circumstances expressly excepted from, or permitted by, the HIPAA regulations. Because of this, Express Scripts does not anticipate making a use or disclosure requiring an individual's authorization. If a use or disclosure of PHI requiring an authorization should become necessary in the future, ESI will obtain a written authorization from affected members in compliance with the HIPAA regulations before making such use or disclosure.

Will Express Scripts provide citations to all State laws and legislation that require more stringent privacy policies and procedures than those required by the federal HIPAA privacy regulation?

Express Scripts does not have a list of citations of State privacy laws. Express Scripts has seen compilations from time to time that appear to refer to thousands of possible provisions. Express Scripts keeps apprised of privacy trends and from time to time clients may bring specific rules to Express Scripts' attention. Express Scripts designs its systems and programs consistent with HIPAA, although Express Scripts understands that reasonable minds can and do differ as to what may or may not be restricted, used or disclosed. HIPAA went into effect April 2003. Express Scripts, along with the entire healthcare industry, employers and other sponsors of health plans, are constantly determining, sometimes on a daily basis, how HIPAA requires such organizations to act. Express Scripts is committed to the privacy, health and respect of its members, and compliance with HIPAA.

SECURITY STANDARDS FAQ

How will Express Scripts comply with the Security Standards?

Express Scripts is dedicating significant resources to ensure that it complies with the newly finalized Security Standards. It will take all appropriate steps to adequately ensure the confidentiality, integrity, and availability of all electronic protected health information it creates, receives, maintains, or transmits. Technical, administrative, and physical safeguards are being reviewed and implemented to assure that electronic member PHI transmitted to us by our sponsors and members is protected. Many of the required and addressable implementation specifications of the Security Standard are considered "good practices" by members of the information system security industry. Because of this, Express Scripts has already addressed, to varying degrees, many security issues raised by the Security Standards.

Does Express Scripts have a Security Officer? What does this individual do?

Yes. Express Scripts has appointed an Information System Security Officer. This individual is tasked with overseeing the successful implementation of appropriate security mechanisms designed to safeguard electronic PHI. The Information System Security Officer will effectuate the creation and deployment of security protocols and policies, train members of the workforce, and monitor the overall status of corporate security compliance efforts. Additionally, to ensure that appropriate mechanisms are utilized to address security requirements, Express Scripts has employed several individuals who are Certified Information System Security Professionals (CISSPs).

If open networks are used, what security measures protect transmitted information?

Encryption options are currently under analysis while network hardware configurations are being standardized to provide a secure environment. In addition, network monitoring is being enhanced to detect potential security incidents.

When was the most recent systems penetration test performed at Express Scripts?

Express Scripts has contracted with external consultants in the past several years to locate, identify and remediate security vulnerabilities in our networks and systems. In the past two years, Express Scripts has acquired the security tools and experienced personnel to perform this function in-house and regularly tests its systems and networks. Evaluations of our systems and network technical security have been a part of the services performed by external consultants.

Has Express Scripts conducted a risk assessment regarding the security of protected health information?

Yes. An outside consulting firm was engaged by Express Scripts in 2001 to provide an assessment of our systems and procedures as they relate to security of protected health information.

Does Express Scripts have a contingency/disaster plan in place to prevent unauthorized access to protected health information?

Yes. Express Scripts has a contingency/disaster plan to prevent unauthorized access to electronic protected health information.

How often does Express Scripts conduct security awareness training?

Security awareness training is conducted upon hire and as needed, according to the individual's job function. Additional security awareness items are provided to system users periodically.

Does Express Scripts have documented physical security processes and procedures?

Yes. Express Scripts already has many documented administrative, physical, and technical security processes and procedures. Additional processes and procedures reflecting the requirements of the Security Standard are currently under development.

Will Express Scripts implement entity authentication?

Yes. Express Scripts currently utilizes several levels of entity authentication and plans to enhance its entity authentication capabilities.

BUSINESS ASSOCIATE AND TRADING PARTNER AGREEMENTS FAQ

How will Express Scripts handle business associate and trading partner agreements?

Express Scripts' clients can find the Express Scripts' Business Associate Agreement form on our web site at www.express-scripts.com. This agreement contains appropriate business associate and trading partner language and was drafted in conformity with Express Scripts' standard PBM Agreement forms. Clients should execute the agreement and return it to their Account Manager. Due to its large client base and the difficulty associated with negotiating many client-specific Business Associate Agreements, Express Scripts encourages clients to execute Express Scripts' agreement as written. Please understand that if clients want to modify the form, the Legal review time will be very protracted.