HCISPP^{SM}

HealthCare Information Security and Privacy Practitioner

At the Forefront of Healthcare Security & Privacy

HealthCare Information Security and Privacy Practitioners (HCISPP^{SM}) are at the forefront of protecting patient health information. These are the practitioners whose foundational knowledge and experience unite healthcare information security and privacy best practices and techniques under one credential to protect organizations and sensitive patient data against emerging threats and breaches.

As the rapidly evolving healthcare industry faces increasing challenges to keeping personal health information protected – including growing volumes of electronic health records, new government regulations, and a more complex IT security landscape – there is a growing need to ensure knowledgeable and credentialed security and privacy practitioners are in place to protect this sensitive information.

HCISPPs provide the frontline defense in protecting health information. Backed by (ISC)$^{2®}$, a global not-for-profit organization that delivers the gold standard for information security certifications, the HCISPP credential confirms a practitioner's core knowledge and experience in security and privacy controls for personal health information.

WHY BECOME A HCISPP

The HCISPP Helps You:

- Validate your experience, skills, and commitment as a healthcare practitioner.
- Demonstrate your qualifications to implement, manage, or assess the appropriate security and privacy controls for your healthcare organization.
- Advance your career with the only certification that establishes your foundational practitioner knowledge, experience, and competency in health information security and privacy best practices.
- Differentiate and enhance your credibility and marketability as a health information security and privacy practitioner with a credential backed by (ISC)^{2}, the globally recognized Gold Standard in information security certification.
- Affirm your commitment to continued competence in the most current security and privacy practices through (ISC)^{2}'s continuing professional education (CPE) requirement.

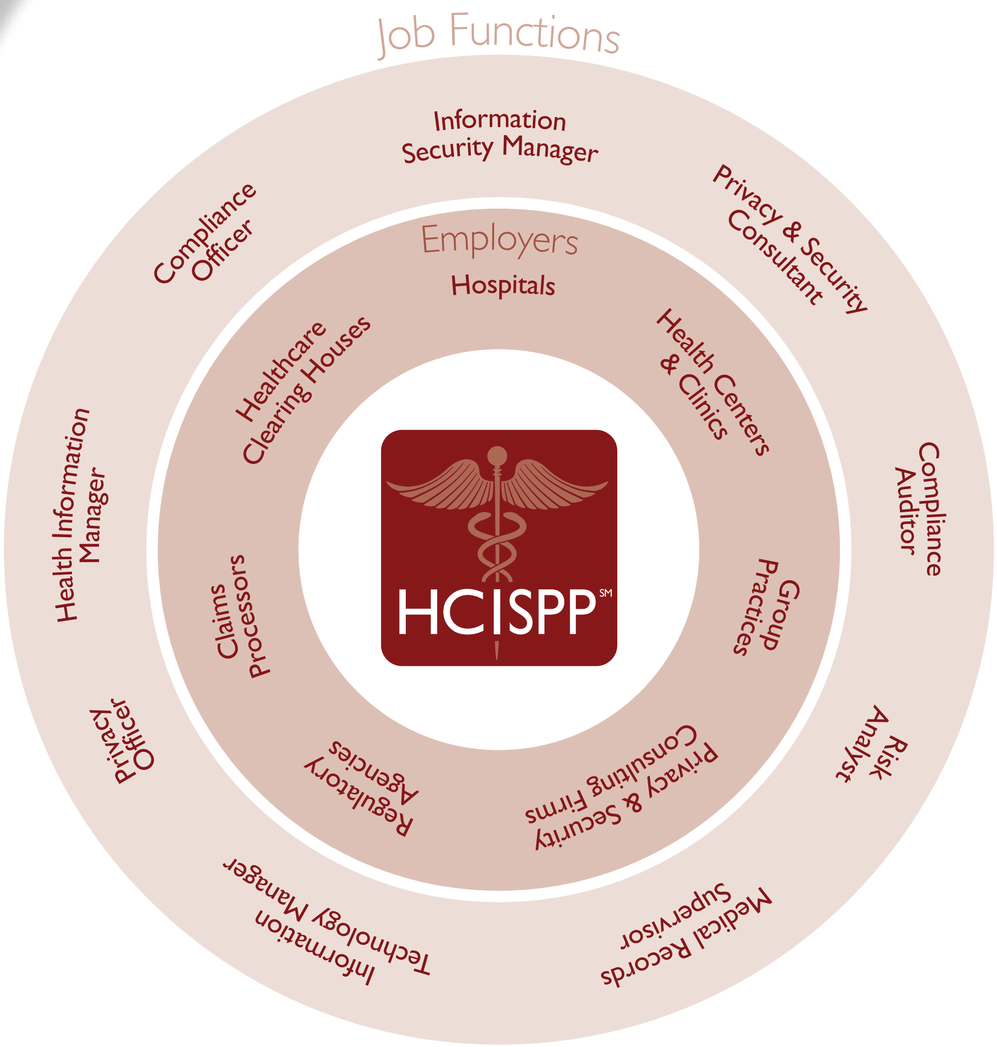
The HCISPP Helps Employers:

- Solidify frontline defense with qualified, experienced, and credentialed healthcare information security and privacy practitioners.
- Demonstrate the organization's proactive commitment to minimizing the risk of breaches.
- Increase confidence that job candidates and employees can do the job right.
- Mitigate risk by exchanging Protected Health Information (PHI) with 3rd parties that employ HCISPPs.
- Increase credibility of the organization when working with clients and vendors.
- Ensure privacy and security personnel are current and capable through HCISPP's CPE credits requirement.

> *"Healthcare organizations face significant and evolving challenges for the proper design, implementation, and administration of effective privacy and security protection programs. The HCISPP will benefit organizations by having a much greater chance for success in tackling these and other opportunities because they will have a contextual understanding for the appropriate application of essential practices and controls that meet organizational, legislative, and directive mandates for the correct handling, processing, and securing of healthcare information. Additionally, this shows that the healthcare practitioner is serious about enhancing their career path and it provides greater confidence and assurance of their skills in their chosen profession."*
>
> **Marc Schandl**, CISSP-ISSAP, ISSMP, CSSLP
> Enterprise Architect with Blue Cross and Blue Shield of Minnesota

WHO SHOULD OBTAIN AN HCISPP

HCISPPs are instrumental to a variety of job functions and employers:


Job Functions
Information Security Manager
Privacy & Security Consultant
Compliance Auditor
Risk Analyst
Medical Records Supervisor
Information Technology Manager
Privacy Officer
Health Information Manager
Compliance Officer
Employers
Hospitals
Health Centers & Clinics
Group Practices
Privacy & Security Consulting Firms
Regulatory Agencies
Claims Processors
Healthcare Clearing Houses
HCISPP SM

EXPERIENCE REQUIRED FOR AN HCISPP

HCISPP candidates must have a minimum of two years of cumulative paid full-time work experience in one domain of the HCISPP credential with the exception that one year of cumulative experience must be in any combination of the following three domains:

Domain 1: Healthcare Industry
Domain 2: Regulatory Environment in Healthcare
Domain 3: Privacy and Security in Healthcare

The remaining one year of experience can be optionally in any of the remaining three domains and does not have to be related to the Healthcare Industry:

Domain 4: Information Governance and Risk Management
Domain 5: Information Risk Assessment
Domain 6: Third Party Risk Management

In addition, as with all (ISC)² credentials, candidates must agree to abide by the (ISC)² Code of Ethics.

THE HCISPP CBK

The HCISPP^{SM} domains are drawn from various privacy and security topics within the (ISC)$^{2®}$ HCISPP CBK®. Updated annually, the domains reflect the most up-to-date best practices worldwide, while establishing a common framework of terms and principles to discuss, debate and resolve in matters pertaining to the profession.

The HCISPP CBK consists of the following six domains:

- **Healthcare Industry –** understand diversity of healthcare industry, types of technologies, flow of information and levels of protection.
  - Healthcare Environment
  - Third-Party Relationships
  - Health Data Management Concepts

- **Regulatory Environment –** entails identifying and understanding relevant legal and regulatory requirements and ensuring organization's policies and procedures are in compliance.
  - Applicable Regulations
  - International Regulations and Controls
  - Internal Practices Compared to New Policies and Procedures
  - Compliance Frameworks, Generally Accepted Privacy Principles

- **Privacy & Security in Healthcare –** basic understanding of security and privacy concepts and principles, types of information to protect.
  - Security Objectives / Attributes
  - General Security Concepts
  - General Privacy Principles
  - Relationship Between Privacy & Security
  - Disparate Nature of Sensitive Data and Implications

- **Information Governance & Risk Management –** how organizations manage information risk through security and privacy governance, risk management lifecycles, principle risk activities likely to support.
  - Security & Privacy Governance
  - Basic Risk Management Methodology
  - Information Risk Management Lifecycles
  - Risk Management Activities

- **Information Risk Assessment –** understand risk assessment concepts, identify and participate in risk assessment practices and procedures.
  - Understand Risk Assessment
  - Identify Control Assessment Procedures
  - Risk Assessment Consistent with Role
  - Efforts to Remediate Gaps

- **Third Party Risk Management –** identify third parties based on use of information, help manage third-parties relationships, determine when additional security and privacy assurances are required.
  - Healthcare Definition of Third Parties
  - Third-Party Management Standards
  - Third-Party Assessments & Audits
  - Security/Privacy Events
  - Third-Party Connectivity
  - Third-Party Requirements
  - Remediation Efforts

Download the HCISPP Exam Outline at **www.isc2.org/exam-outline**.

ENGAGE WHILE OBTAINING EXPERIENCE

Associate of (ISC)²®

For those who not yet have acquired the necessary experience to qualify for the HCISPP credential, (ISC)² will confer an "Associate of (ISC)²" status after successfully passing the HCISPP examination. The Associate status may be especially useful to those experienced information security professionals looking to move into healthcare. Or, recent graduates who have worked hard to acquire the knowledge but have not yet gained the needed experience. Become an Associate of (ISC)², and you're already part of a reputable and credible organization, earning recognition from employers and peers for the industry knowledge you've already gained.

Participation Requirements

Associate of (ISC)² status is available to those knowledgeable in key areas of industry concepts but lacking the work experience. As a candidate, you may successfully pass the HCISPP examination and subscribe to the (ISC)² Code of Ethics, however to earn the HCISPP credential you will have to acquire the necessary years of pertinent work experience, provide proof and be endorsed by a member of (ISC)² in good standing. If you are working towards this credential, you will have a maximum of three years from your exam pass date to acquire the necessary two years of professional experience. An Annual Maintenance Fee (AMF) of US$35 applies and 10 Continuing Professional Education (CPE) credits must be earned each year to remain in good standing.

For more information on how you can become an Associate of (ISC)², visit **www.isc2.org/associate**.

THE NEED FOR THE HCISPP CERTIFICATION

The privacy and security of personal health information has become a globally recognized issue and priority. While countries around the world have attempted to manage the issue and improve the effectiveness of security and privacy controls through numerous laws, regulations and best practice frameworks, very little progress has been made in reducing the number of breaches. When combined with the severe penalties agencies are now imposing – including heavy fines and sometimes criminal prosecution – the magnitude of risk borne by entities handling patient health information is resulting in even more diligent and vigorous efforts to protect the information.

Unfortunately, the task is becoming even more complex and challenging with the advent of electronic health records, mandated electronic exchange of records, and ever-growing IT environment complexity. While these advances in technology have greatly advanced healthcare, they have also accelerated and broadened the exposure of organizations adopting them.

Even though technology has increased organizations' risk, human error remains the leading cause of health information breaches. With this in mind, employers across the globe recognize the criticality of mitigating risk through improved hiring and training practices to ensure their security and privacy practitioners are qualified to do their jobs well. Until now, there has been no credentialing program to validate a practitioner's core knowledge, skills, and qualifications to protect and keep secure vital healthcare information. The HCISPP aims to do just that.

HEALTHCARE PRIVACY INSIGHTS

The cost of healthcare security & privacy breaches continues to mushroom:

- Ponemon Institute's December 2012 study "Patient Privacy & Data Security" estimates that "the average annual cost to the healthcare industry could potentially be as high as almost $7 billion"
- The Ponemon study also calculates that "the average cost for the organizations represented in this benchmark study is $2.4 million over a two-year period"
- The Study also reveals that "the top three causes for a data breach are: lost or stolen computing devices, employee mistakes and third-party snafus"

For recent examples of penalties visit
www.isc2.org/healthcare-data-breaches

> *"Recent trends towards stronger enforcement of security regulations have begun to change the healthcare industry's perception of information security. There is a growing need in the industry for qualified professionals to help mature the current state of healthcare information security and improve regulatory compliance. (ISC)²'s HCISPP will help organizations streamline their hiring process by ensuring prospective candidates have a basic level of knowledge about the healthcare industry, the security and privacy concerns specific to healthcare, and the general risk management principles and concepts required of a healthcare information protection professional."*
>
> **Dr. Bryan Cline**, CISSP-ISSEP
> CISO and VP, CSF Development & Implementation, HITRUST

EDUCATION DELIVERED YOUR WAY

Official (ISC)$^{2®}$ HCISPP^{SM} CBK® Training Seminar

This official training seminar is the most comprehensive, complete review of healthcare security and privacy concepts and industry best practices, and the only training course endorsed by (ISC)^2. As your exclusive way to review and refresh your knowledge of the domains and sub-domains of the HCISPP CBK, the seminar will help you identify areas you need to study and includes:

- 100% up-to-date material
- Three days of comprehensive review of topics related to healthcare security and privacy
- Contributions from HCISPPs, (ISC)^2 Authorized Instructors and subject matter experts

The Official HCISPP CBK Training Seminar is offered in the following formats:

- **Classroom** Delivered in a multi-day, classroom setting. Course material focuses on covering the six HCISPP domains. Available throughout the world at (ISC)^2 facilities and (ISC)^2 Official Training Providers.
- **Private On-site** Host your own Training Seminar on- or off-site. Available for larger groups, this option often saves employee travel time and expense. Group pricing is also available to organizations with 15 or more employees planning to sit for the exam.
- **Live OnLine** Educate yourself from the convenience of your computer. Live OnLine brings you the same award winning course content as the classroom-based or private on-site seminars and the benefit of an (ISC)^2 Authorized Instructor.

Visit **www.isc2.org/hcispp-training** for more information or to register.

Exam Outline - Free

Your primary resource in your study efforts to become an HCISPP. The Exam Outline contains a blueprint that details the major topics and subtopics within the domains, a suggested reference list for further study, exam information, and registration/administration policies and instructions. **www.isc2.org/exam-outline**

OFFICIAL TRAINING PROVIDERS

Official (ISC)^2 CBK Training Seminars are available throughout the world at (ISC)^2 facilities and through (ISC)^2 Official Training Providers. Official (ISC)^2 CBK Training Seminars are conducted only by (ISC)^2 Authorized Instructors who are experts in their field and have demonstrated their mastery of the covered domains.

Be wary of training providers that are not authorized by (ISC)^2. Be certain that your educator carries the (ISC)^2 Official Training Provider logo to ensure that you are experiencing the best and most current programs available.

2013 SC Magazine Award Winner – Best Professional Training Program, (ISC)^2 Education

CHECKLIST FOR CERTIFICATION

✓ **Obtain the Required Experience** - For the HCISPP certification, candidates must have a minimum of two years of cumulative paid full-time work experience in one knowledge area of the credential that includes security, compliance & privacy. Legal experience may be substituted for compliance, and/or information management experience may be substituted for privacy. One year of the two-year experience requirement must be in healthcare. If you do not have the required experience, you may still sit for the exam and become an Associate of (ISC)^2 until you have gained the required experience.

✓ **Study for the Exam** - Utilize these optional educational tools to learn the HCISPP CBK.

- Exam Outline
- Official Training Seminar

✓ **Register for the Exam**

- Visit **www.isc2.org/certification-register-now** to schedule an exam date
- Submit the examination fee

✓ **Pass the Exam** - Pass the HCISPP examination with a scaled score of 700 points or greater. Read the Exam Scoring FAQs at **www.isc2.org/exam-scoring-faqs**.

✓ **Complete the Endorsement Process** - Once you are notified that you have successfully passed the examination, you will have nine months from the date you sat for the exam to complete the following endorsement process:

- Complete an Application Endorsement Form
- Subscribe to the (ISC)^2 code of ethics
- Have your form endorsed by an (ISC)^2 member

The credential can be awarded once the steps above have been completed and your form has been submitted.* Get the guidelines and form at **www.isc2.org/endorsement**.

✓ **Maintain the Certification** - Recertification is required every three years, with ongoing requirements to maintain your credentials in good standing. This is primarily accomplished through earning 60 Continuing Professional Education (CPE) credits every three years, with a minimum of 10 CPEs earned each year after certification. If the CPE requirements are not met, HCISPPs must retake the exam to maintain certification. HCISPPs must also pay an Annual Maintenance Fee (AMF) of US$65.

For more information on the HCISPP visit **www.isc2.org/hcispp**.

**Audit Notice - Passing candidates will be randomly selected and audited by (ISC)^2 prior to issuance of any certificate. Multiple certifications may result in a candidate being audited more than once.*

MEMBER BENEFITS

FREE:

(ISC)^2 One-Day SecureEvents
Industry Initiatives
Certification Verification
Chapter Program
(ISC)^2 Receptions/Networking Opportunities
(ISC)^2 Global Awards Program
Online Forum
(ISC)^2 e-Symposium Webinars
ThinkTANK
Global Information Security Workforce Study
InfoSecurity Professional Magazine
Safe and Secure Online Volunteer Opportunities
InterSeC

DISCOUNTED:

(ISC)^2 Security Congress
(ISC)^2 Local Two-Day Secure Events
Industry Conferences
The (ISC)^2 Journal

Maintain the certification with required CPEs and AMF

US$ 65 amf

60 cpes

3 years

Formed in 1989 and celebrating its 25th anniversary, (ISC)^{2}® is the largest not-for-profit membership body of certified information and software security professionals worldwide, with nearly 100,000 members in more than 135 countries. Globally recognized as the Gold Standard, (ISC)^2 issues the Certified Information Systems Security Professional (CISSP®) and related concentrations, as well as the Certified Secure Software Lifecycle Professional (CSSLP®), the Certified Cyber Forensics Professional (CCFP^{SM}), Certified Authorization Professional (CAP®), HealthCare Information Security and Privacy Practitioner (HCISPP^{SM}), and Systems Security Certified Practitioner (SSCP®) credentials to qualifying candidates. (ISC)^2's certifications are among the first information technology credentials to meet the stringent requirements of ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel. (ISC)^2 also offers education programs and services based on its CBK®, a compendium of information and software security topics. More information is available at **www.isc2.org**.