(Email request to take web survey – survey link)
January 17, 2015

Dear Dr. Crockett,

You have been randomly selected to participate in a brief survey on the use of electronic health records in office-based practices. The National Center for Health Statistics (NCHS), a Federal Statistical Agency, collects data from physicians to help health services researchers and policy makers, as well as those in the private sector, understand changes in the environments physicians work in and emerging hot topics. These topics include the use of electronic health records and how it affects the delivery of health care in the United States.

You are not being asked to provide any patient information. Participation in this 30-minute survey is voluntary; you may discontinue your participation at any time. There will be no loss of benefits for not participating or discontinuing participation. We may carry out additional related health care research by linking your survey responses to administrative medical information and other related records. The NCHS Research Ethics Review Board has approved this research survey.

Data collection is authorized under Section 306 of the Public Health Service Act (42 U.S.C. 242k). NCHS is required to keep your survey data confidential in accordance with Section 308(d) of the Public Health Service Act (42 U.S.C. 242m(d)) and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, Title 5 of PL 107-347). Data collected will be used for statistical purposes only. In addition, NCHS complies with the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. §§ 151 & 151 note). See below for more information.

Conducting the survey over the Internet is the most efficient and easiest way to respond to our survey. You can access the survey through the following link: http://www.cdc.gov/nchs/nehrs/. The user ID and password for accessing the survey will be sent to you in a separate email. When prompted, enter the user ID and password provided in the separate email.

Your email address was obtained from a database of physicians. If you have any questions or comments regarding this study, please call the study coordinator at (xxx) xxx-xxxx. If you have questions about your rights as a research participant, please call the NCHS Research Ethics Review Board at (800) 223-8118.

Thank you in advance for your participation in this important study.

Sincerely,

Charles J. Rothwell
Director
National Center for Health Statistics

FAQ

1. WHO WILL SEE MY ANSWERS?

We take your privacy very seriously. The answers you give us are used for statistical research only. This means that your answers will be combined with other people's answers in a way that protects everyone's identity. As required by federal law, only those NCHS employees and our specially designated agents (such as the U.S. Census Bureau) who must use your personal information for a specific reason can see your answers.

Strict laws prevent us from releasing information that could identify you to anyone else without your consent. A number of federal laws require that all information we collect be held in strict confidence: Section 308(d) of the Public Health Service Act (42 U.S.C. 242m(d)), the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, Title 5 of Public Law 107-347), and the Privacy Act of 1974 (5 U.S.C. § 552a). Every NCHS employee, contractor, and agent has taken an oath to keep your information private. Anyone who willfully discloses ANY identifiable information could get a jail term of up to five years, a fine of up to $250,000, or both. In addition, NCHS complies with the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. §§ 151 & 151 note). This law requires the federal government to protect federal computer networks by using computer security programs to identify cybersecurity risks like hacking, internet attacks, and other security weaknesses. If information sent through government networks triggers a cyber threat indicator, the information may be intercepted and reviewed for cyber threats by computer network experts working for, or on behalf, of the government.

2. WHAT IS THE FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015?

The Federal Cybersecurity Enhancement Act of 2015 permits monitoring information systems for the purpose of protecting a network from hacking, denial of service attacks and other security vulnerabilities.[1] The software used for monitoring may scan information that is transiting, stored on, or processed by the system. If the information triggers a cyber threat indicator, the information may be intercepted and reviewed for cyber threats. The Cybersecurity Act specifies if any information that is scanned by the cybersecurity software programs is found to be suspicious, it may be reviewed for specific threats by computer network experts working for the government (or contractors or agents who have governmental authority to do so). The Act further specifies that such information may only be used for the purpose of protecting information and information systems from cybersecurity risks.

[1] "Monitor" means "to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system;" "information system" means "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information;" "cyber threat indicator" means "information that is necessary to describe or identify security vulnerabilities of an information system, enable the exploitation of a security vulnerability, or unauthorized remote access or use of an information system."

(Email request to take web survey – user ID and password)
January 17, 2015

Dear Dr. Crockett,

You have been randomly selected to participate in a brief survey on the use of electronic health records in office-based practices. The National Center for Health Statistics (NCHS), a Federal Statistical Agency, collects data from physicians to help health services researchers and policy makers, as well as those in the private sector, understand changes in the environments physicians work in and emerging hot topics. These topics include the use of electronic health records and how it affects the delivery of health care in the United States.

A separate email was sent to you containing the survey link which you can use to access the survey. When prompted, enter the user ID and password provided below.

User ID: [user-name-here]
Password: [6-char-password-here]

Data collection is authorized under Section 306 of the Public Health Service Act (42 U.S.C. 242k). NCHS is required to keep your survey data confidential in accordance with Section 308(d) of the Public Health Service Act (42 U.S.C. 242m(d)) and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, Title 5 of PL 107-347). Data collected will be used for statistical purposes only. In addition, NCHS complies with the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. §§ 151 & 151 note). See below for more information.

If you have any questions or comments regarding this study, please call the study coordinator at (xxx) xxx-xxxx. If you have questions about your rights as a research participant, please call the NCHS Research Ethics Review Board at (800) 223-8118.

Thank you in advance for your participation in this important study.

Sincerely,

Charles J. Rothwell
Director
National Center for Health Statistics

FAQ

1. WHO WILL SEE MY ANSWERS?

We take your privacy very seriously. The answers you give us are used for statistical research only. This means that your answers will be combined with other people's answers in a way that protects everyone's identity. As required by federal law, only those NCHS employees and our specially designated agents (such as the U.S. Census Bureau) who must use your personal information for a specific reason can see your answers.

Strict laws prevent us from releasing information that could identify you to anyone else without your consent. A number of federal laws require that all information we collect be held in strict confidence: Section 308(d) of the Public Health Service Act (42 U.S.C. 242m(d)), the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, Title 5 of Public Law 107-347), and the Privacy Act of 1974 (5 U.S.C. § 552a). Every NCHS employee, contractor, and agent has taken an oath to keep your information private. Anyone who willfully discloses ANY identifiable information could get a jail term of up to five years, a fine of up to $250,000, or both. In addition, NCHS complies with the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. §§ 151 & 151 note). This law requires the federal government to protect federal computer networks by using computer security programs to identify cybersecurity risks like hacking, internet attacks, and other security weaknesses. If information sent through government networks triggers a cyber threat indicator, the information may be intercepted and reviewed for cyber threats by computer network experts working for, or on behalf, of the government.

2. WHAT IS THE FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015?

The Federal Cybersecurity Enhancement Act of 2015 permits monitoring information systems for the purpose of protecting a network from hacking, denial of service attacks and other security vulnerabilities.[1] The software used for monitoring may scan information that is transiting, stored on, or processed by the system. If the information triggers a cyber threat indicator, the information may be intercepted and reviewed for cyber threats. The Cybersecurity Act specifies if any information that is scanned by the cybersecurity software programs is found to be suspicious, it may be reviewed for specific threats by computer network experts working for the government (or contractors or agents who have governmental authority to do so). The Act further specifies that such information may only be used for the purpose of protecting information and information systems from cybersecurity risks.

[1] "Monitor" means "to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system;" "information system" means "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information;" "cyber threat indicator" means "information that is necessary to describe or identify security vulnerabilities of an information system, enable the exploitation of a security vulnerability, or unauthorized remote access or use of an information system."

(LETTER in US Mail to take web survey)
September 24, 2015

John Doe, MD
Position (if provided, i.e. Director, Chief, etc)
Practice Name (if provided)
5 Smith Street
Nowhere, NC 99999-1111

Dear Dr. Doe,

You have been randomly selected to participate in a brief survey on the use of electronic health records in office-based practices. Results from the *Physician Experience with EHRs Survey*, which is affiliated with the National Ambulatory Medical Care Survey (NAMCS), will be used to inform health services researchers and policy makers, as well as those in the private sector, about the use of electronic health records and how it affects the delivery of health care in the United States.

All information we collect is voluntary and used for statistical purposes only. Participation in this 30-minute survey is voluntary; you may discontinue your participation at any time. There will be no loss of benefits for not participating or discontinuing participation. We may carry out additional related health care research by linking your survey responses to administrative medical information and other related records. You are not being asked to provide any patient information. The National Center for Health Statistics' Research Ethics Review Board has approved this research survey.

Data collection is authorized under Section 306 of the Public Health Service Act (42 U.S.C. 242k). We are required to keep your survey data confidential in accordance with Section 308(d) of the Public Health Service Act (42 U.S.C. 242m(d)) and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, Title 5 of PL 107-347). In addition, NCHS complies with the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. §§ 151 & 151 note). See reverse for more information.

Conducting the survey over the Internet is the most efficient and easiest way to respond to our survey. If you are interested in participating in this survey, please go to the following link: http://www.cdc.gov/nchs/nehrs/.

Enter the user ID and password provided below.

User ID: [user-name-here]
Password: [6-char-password-here]

We look forward to receiving your completed survey on this important public health issue. If you have any questions or comments regarding this study, please call the study coordinator at (xx) xxx-xxxx. If you have questions about your rights as a research participant, please call the Research Ethics Review Board at the National Center for Health Statistics at (800) 223-8118. General information on the survey may be obtained by visiting the NAMCS participant website at www.cdc.gov/namcs.

Thank you in advance for your participation in this important study.

Sincerely,

Charles J. Rothwell
Director
National Center for Health Statistics

FAQ

1. WHO WILL SEE MY ANSWERS?

We take your privacy very seriously. The answers you give us are used for statistical research only. This means that your answers will be combined with other people's answers in a way that protects everyone's identity. As required by federal law, only those NCHS employees and our specially designated agents (such as the U.S. Census Bureau) who must use your personal information for a specific reason can see your answers.

Strict laws prevent us from releasing information that could identify you to anyone else without your consent. A number of federal laws require that all information we collect be held in strict confidence: Section 308(d) of the Public Health Service Act

(42 U.S.C. 242m(d)), the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, Title 5 of Public Law 107-347), and the Privacy Act of 1974 (5 U.S.C. § 552a). Every NCHS employee, contractor, and agent has taken an oath to keep your information private. Anyone who willfully discloses ANY identifiable information could get a jail term of up to five years, a fine of up to $250,000, or both. In addition, NCHS complies with the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. §§ 151 & 151 note). This law requires the federal government to protect federal computer networks by using computer security programs to identify cybersecurity risks like hacking, internet attacks, and other security weaknesses. If information sent through government networks triggers a cyber threat indicator, the information may be intercepted and reviewed for cyber threats by computer network experts working for, or on behalf, of the government.

2. WHAT IS THE FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015?

The Federal Cybersecurity Enhancement Act of 2015 permits monitoring information systems for the purpose of protecting a network from hacking, denial of service attacks and other security vulnerabilities.[1] The software used for monitoring may scan information that is transiting, stored on, or processed by the system. If the information triggers a cyber threat indicator, the information may be intercepted and reviewed for cyber threats. The Cybersecurity Act specifies if any information that is scanned by the cybersecurity software programs is found to be suspicious, it may be reviewed for specific threats by computer network experts working for the government (or contractors or agents who have governmental authority to do so). The Act further specifies that such information may only be used for the purpose of protecting information and information systems from cybersecurity risks.

[1] "Monitor" means "to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system;" "information system" means "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information;" "cyber threat indicator" means "information that is necessary to describe or identify security vulnerabilities of an information system, enable the exploitation of a security vulnerability, or unauthorized remote access or use of an information system."

(First Mailing of Questionnaire)
September 24, 2015

John Doe, MD
Position (if provided, i.e. Director, Chief, etc)
Practice Name (if provided)
5 Smith Street
Nowhere, NC 99999-1111

Dear Dr. Doe,

About two weeks ago, we contacted you about participating in a brief survey. As of the date of this letter, we have not received your completed survey. Results from the enclosed *Physician Experience with EHRs Survey*, which is affiliated with the National Ambulatory Medical Care Survey (NAMCS), will provide information about the use of electronic health records and how it affects the delivery of health care in the United States. I request that you please take the time to answer the questions and return the questionnaire in the enclosed envelope.

This information will be used for statistical purposes only. Also, we intend to do additional health care research by linking your responses to this survey to available administrative medical information and other related records. The National Center for Health Statistics' Research Ethics Review Board has approved this research survey.

Data collection is authorized under Section 306 of the Public Health Service Act (42 U.S.C. 242k). We are required to keep your survey data confidential in accordance with Section 308(d) of the Public Health Service Act (42 U.S.C. 242m(d)) and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, Title 5 of PL 107-347). In addition, NCHS complies with the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. §§ 151 & 151 note). See reverse for more information.

We look forward to receiving your completed survey. If you are unable to complete the survey yourself, an office manager or another staff member familiar with your workload and experiences with your electronic health record system could complete the survey on your behalf. You are not being asked to provide any patient information for this mail survey and participation is voluntary. As survey participation is voluntary, you may discontinue your participation at any time. There will be no loss of benefits for not participating or discontinuing participation. If you choose not to participate, please answer Questions 2 and 4 on the form and return it to us in the enclosed envelope.

Please accept the enclosed pen as a token of our gratitude for completing this 30-minute research survey. We have routinely relied on the generosity of physicians like you to provide this much needed information to help policy makers, health services researchers, and medical associations understand the current issues with health care delivery in the United States. If you have any questions or comments regarding this study, please call the study coordinator at (xxx) xxx-xxx. If you have questions about your rights as a research participant, please call the Research Ethics Review Board at the National Center for Health Statistics at (800) 223-8118. Additional information on the survey may be obtained by visiting the NAMCS participant web site at www.cdc.gov/namcs.

Thank you for your valuable assistance with this worthy study.

Sincerely,

Charles J. Rothwell
Director
National Center for Health Statistics

FAQ

1. WHO WILL SEE MY ANSWERS?

We take your privacy very seriously. The answers you give us are used for statistical research only. This means that your answers will be combined with other people's answers in a way that protects everyone's identity. As required by federal law, only those NCHS employees and our specially designated agents (such as the U.S. Census Bureau) who must use your personal information for a specific reason can see your answers.

Strict laws prevent us from releasing information that could identify you to anyone else without your consent. A number of federal laws require that all information we collect be held in strict confidence: Section 308(d) of the Public Health Service Act (42 U.S.C. 242m(d)), the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, Title 5 of Public Law 107-347), and the Privacy Act of 1974 (5 U.S.C. § 552a). Every NCHS employee, contractor, and agent has taken an oath to keep your information private. Anyone who willfully discloses ANY identifiable information could get a jail term of up to five years, a fine of up to $250,000, or both. In addition, NCHS complies with the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. §§ 151 & 151 note). This law requires the federal government to protect federal computer networks by using computer security programs to identify cybersecurity risks like hacking, internet attacks, and other security weaknesses. If information sent through government networks triggers a cyber threat indicator, the information may be intercepted and reviewed for cyber threats by computer network experts working for, or on behalf, of the government.

2. WHAT IS THE FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015?

The Federal Cybersecurity Enhancement Act of 2015 permits monitoring information systems for the purpose of protecting a network from hacking, denial of service attacks and other security vulnerabilities.[1] The software used for monitoring may scan information that is transiting, stored on, or processed by the system. If the information triggers a cyber threat indicator, the information may be intercepted and reviewed for cyber threats. The Cybersecurity Act specifies if any information that is scanned by the cybersecurity software programs is found to be suspicious, it may be reviewed for specific threats by computer network experts working for the government (or contractors or agents who have governmental authority to do so). The Act further specifies that such information may only be used for the purpose of protecting information and information systems from cybersecurity risks.

[1] "Monitor" means "to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system;" "information system" means "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information;" "cyber threat indicator" means "information that is necessary to describe or identify security vulnerabilities of an information system, enable the exploitation of a security vulnerability, or unauthorized remote access or use of an information system."

(Second Mailing of Questionnaire)
September 24, 2015

John Doe, MD
Position (if provided, i.e. Director, Chief, etc)
Practice Name (if provided)
5 Smith Street
Nowhere, NC 99999-1111

Dear Dr. Doe,

About three weeks ago, we sent you a questionnaire from the *Physician Experience with EHRs Survey,* which is an important research study on the use of electronic health records in office-based practices. As of the date of this letter, we have not received your survey.

The National Center for Health Statistics collects data from physicians to help health services researchers and policy makers, as well as those in the private sector, understand changes in the environments physicians work in and emerging hot topics, including the use of electronic health records and how it affects the delivery of health care in the United States. Your participaton is extremely important to us and health policy researchers. The value of this study is dependent upon obtaining a good representation of physicians' unique insights and experiences. The data you provide are invaluable to track the adoption of electronic health records nationwide. The National Center for Health Statistics' Research Ethics Review Board has approved this research survey.

Data collection is authorized under Section 306 of the Public Health Service Act (42 U.S.C. 242k). We are required to keep your survey data confidential in accordance with Section 308(d) of the Public Health Service Act (42 U.S.C. 242m(d)) and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, Title 5 of PL 107-347). In addition, NCHS complies with the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. §§ 151 & 151 note). See reverse for more information.

You are not being asked to provide any patient information. All information will be used for statistical purposes only. Also, we intend to do additional health care research by linking your responses to this survey to available administrative medical information and other related records. We hope that you will take part in the study. Your participation is voluntary and you may discontinue your participation at any time. There will be no loss of benefits for not participating or discontinuing participation.

If you are unable to complete the survey yourself, an office manager or another staff member familiar with your workload and experiences with your electronic health record system could complete the survey on your behalf. If you are no longer in practice or do not provide care for ambulatory patients, please answer Question 2 on the survey and return it in the postage-paid envelope. If you choose not to participate, please answer Questions 2 and 4 on the form and return it in the envelope. I urge you to complete the survey and return it in the enclosed envelope.

Whether you have already mailed a completed survey, are planning to complete the 30-minute survey, or decided not to participate, we want to thank you very much for your time, effort, and contribution to this important study. If you have any questions or comments regarding this study, please do not hesitate to contact the study coordinator at (xxx) xxx-xxxx. If you have questions about your rights as a research participant, please call the Research Ethics Review Board at the National Center for Health Statistics at (800) 223-8118.

Sincerely,

Charles J. Rothwell
Director
National Center for Health Statistics

FAQ

1. WHO WILL SEE MY ANSWERS?

We take your privacy very seriously. The answers you give us are used for statistical research only. This means that your answers will be combined with other people's answers in a way that protects everyone's identity. As required by federal law, only those NCHS employees and our specially designated agents (such as the U.S. Census Bureau) who must use your personal information for a specific reason can see your answers.

Strict laws prevent us from releasing information that could identify you to anyone else without your consent. A number of federal laws require that all information we collect be held in strict confidence: Section 308(d) of the Public Health Service Act (42 U.S.C. 242m(d)), the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, Title 5 of Public Law 107-347), and the Privacy Act of 1974 (5 U.S.C. § 552a). Every NCHS employee, contractor, and agent has taken an oath to keep your information private. Anyone who willfully discloses ANY identifiable information could get a jail term of up to five years, a fine of up to $250,000, or both. In addition, NCHS complies with the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. §§ 151 & 151 note). This law requires the federal government to protect federal computer networks by using computer security programs to identify cybersecurity risks like hacking, internet attacks, and other security weaknesses. If information sent through government networks triggers a cyber threat indicator, the information may be intercepted and reviewed for cyber threats by computer network experts working for, or on behalf, of the government.

2. WHAT IS THE FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015?

The Federal Cybersecurity Enhancement Act of 2015 permits monitoring information systems for the purpose of protecting a network from hacking, denial of service attacks and other security vulnerabilities.[1] The software used for monitoring may scan information that is transiting, stored on, or processed by the system. If the information triggers a cyber threat indicator, the information may be intercepted and reviewed for cyber threats. The Cybersecurity Act specifies if any information that is scanned by the cybersecurity software programs is found to be suspicious, it may be reviewed for specific threats by computer network experts working for the government (or contractors or agents who have governmental authority to do so). The Act further specifies that such information may only be used for the purpose of protecting information and information systems from cybersecurity risks.

[1] "Monitor" means "to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system;" "information system" means "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information;" "cyber threat indicator" means "information that is necessary to describe or identify security vulnerabilities of an information system, enable the exploitation of a security vulnerability, or unauthorized remote access or use of an information system."

(Third mailing of Questionnaire)
September 24, 2015

John Doe, MD
Practice Name (if provided)
5 Smith Street
Nowhere, NC 99999-1111

Dear Dr. Doe,

We have been trying to reach you about an important research study on electronic health records in office-based practices. Results from the enclosed questionnaire will be used to inform health services researchers and policy makers, as well as those in the private sector, about the use of electronic health records and how it affects the delivery of health care in the United States. We are conducting this as a special *Physician Experience with EHRs Survey* to the National Ambulatory Medical Care Survey (NAMCS) which routinely collects information about office-based practices. You are not being asked to provide any patient information for this mail survey and participation is voluntary. All information will be used for statistical purposes only. Also, we intend to do additional health care research by linking your survey responses to available administrative medical information and other related records. The National Center for Health Statistics' Research Ethics Review Board has approved this research survey.

Data collection is authorized under Section 306 of the Public Health Service Act (42 U.S.C. 242k). We are required to keep your survey data confidential in accordance with Section 308(d) of the Public Health Service Act (42 U.S.C. 242m(d)) and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, Title 5 of PL 107-347). In addition, NCHS complies with the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. §§ 151 & 151 note). See reverse for more information.

This study period is drawing to a close, and one of our concerns is that physicians who have not responded to the survey may have different experiences from those who have returned surveys. In order to make statistically valid conclusions from the study, we need to hear from all types of physicians. If you are unable to complete the survey yourself within the next week, then an office manager or another staff member familiar with your workload and experiences with your electronic health record system could complete the survey on your behalf. I urge you to complete the survey and return it in the postage-paid envelope.

If you are no longer in practice or do not provide care for ambulatory patients, please answer Question 2 on the survey and return it in the postage-paid envelope. As survey participation is voluntary, you may discontinue your participation at any time. There will be no loss of benefits for not participating or discontinuing participation. If you choose not to participate, please answer Questions 2 and 4 on the form and return it to us in the enclosed envelope.

Whether you have already mailed a completed survey, are planning to complete the 30-minute survey, or decided not to participate, we want to thank you very much for your time, effort, and contribution to this important study. If you have any questions or comments regarding this study, please do not hesitate to contact the study coordinator at (xxx) xxx-xxxx. If you have questions about your rights as a research participant, please call the Research Ethics Review Board at the National Center for Health Statistics at (800) 223-8118.

Sincerely,

Charles J. Rothwell
Director
National Center for Health Statistics

FAQ

1. WHO WILL SEE MY ANSWERS?

We take your privacy very seriously. The answers you give us are used for statistical research only. This means that your answers will be combined with other people's answers in a way that protects everyone's identity. As required by federal law, only those NCHS employees and our specially designated agents (such as the U.S. Census Bureau) who must use your personal information for a specific reason can see your answers.

Strict laws prevent us from releasing information that could identify you to anyone else without your consent. A number of federal laws require that all information we collect be held in strict confidence: Section 308(d) of the Public Health Service Act (42 U.S.C. 242m(d)), the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, Title 5 of Public Law 107-347), and the Privacy Act of 1974 (5 U.S.C. § 552a). Every NCHS employee, contractor, and agent has taken an oath to keep your information private. Anyone who willfully discloses ANY identifiable information could get a jail term of up to five years, a fine of up to $250,000, or both. In addition, NCHS complies with the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. §§ 151 & 151 note). This law requires the federal government to protect federal computer networks by using computer security programs to identify cybersecurity risks like hacking, internet attacks, and other security weaknesses. If information sent through government networks triggers a cyber threat indicator, the information may be intercepted and reviewed for cyber threats by computer network experts working for, or on behalf, of the government.

2. WHAT IS THE FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015?

The Federal Cybersecurity Enhancement Act of 2015 permits monitoring information systems for the purpose of protecting a network from hacking, denial of service attacks and other security vulnerabilities.[1] The software used for monitoring may scan information that is transiting, stored on, or processed by the system. If the information triggers a cyber threat indicator, the information may be intercepted and reviewed for cyber threats. The Cybersecurity Act specifies if any information that is scanned by the cybersecurity software programs is found to be suspicious, it may be reviewed for specific threats by computer network experts working for the government (or contractors or agents who have governmental authority to do so). The Act further specifies that such information may only be used for the purpose of protecting information and information systems from cybersecurity risks.

[1] "Monitor" means "to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system;" "information system" means "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information;" "cyber threat indicator" means "information that is necessary to describe or identify security vulnerabilities of an information system, enable the exploitation of a security vulnerability, or unauthorized remote access or use of an information system."

Post Card Thank You/Reminder

Last week a questionnaire was mailed to you requesting your participation in an important research study of electronic health records in office-based practices.

If you have already returned the questionnaire, let me take this opportunity to thank you for your contribution to this research. If not, please do so today. Your participation in the study is critical to its success and to improving the understanding of the adoption of electronic health records systems in the United States.

If you did not receive the questionnaire, or if you have misplaced it, please call our toll-free number at (xxx) xxx-xxxx, and we will be happy to send you another one. If you have questions about your rights as a research participant, please call the Research Ethics Review Board at the National Center for Health Statistics at (800) 223-8118.

Thank you for your participation.

Charles J. Rothwell
Director
National Center for Health Statistics