Leaking Beeps:

Unencrypted Pager Messages in the Healthcare Industry

Stephen Hilt and Philippe Lin
Trend Micro Forward-Looking Threat Research

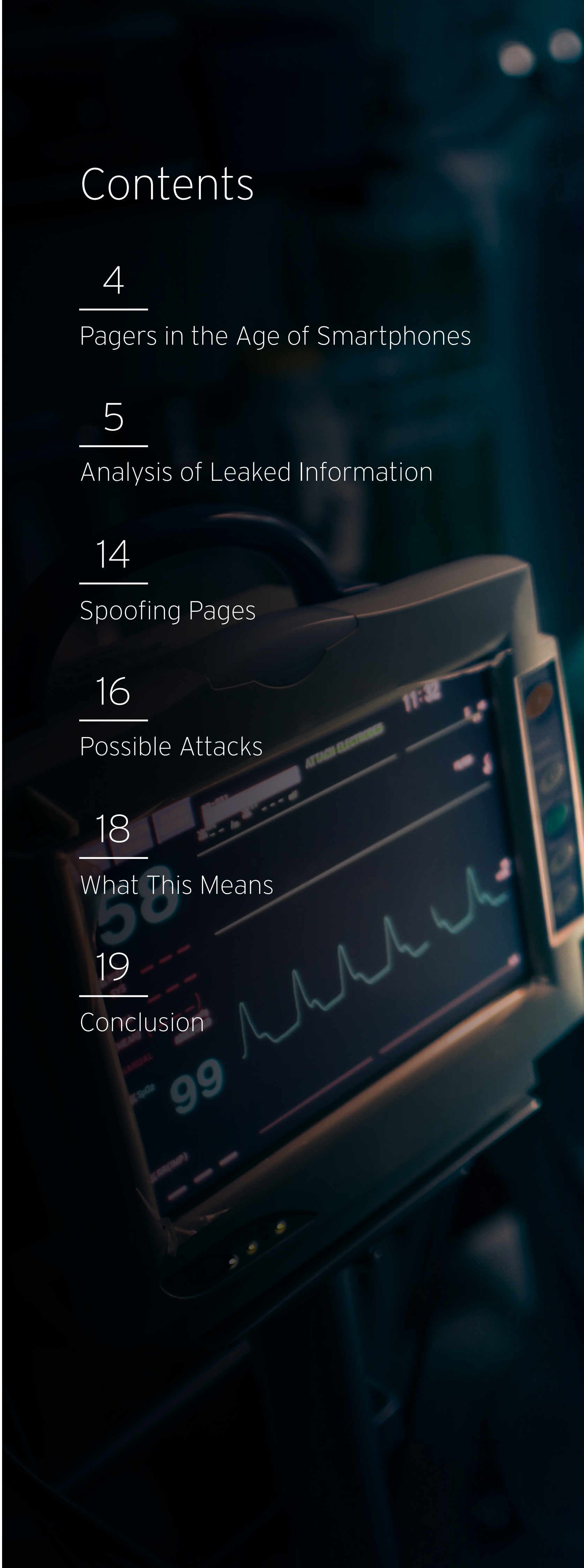
A **TrendLabs**SM Research Paper

TREND MICRO LEGAL DISCLAIMER

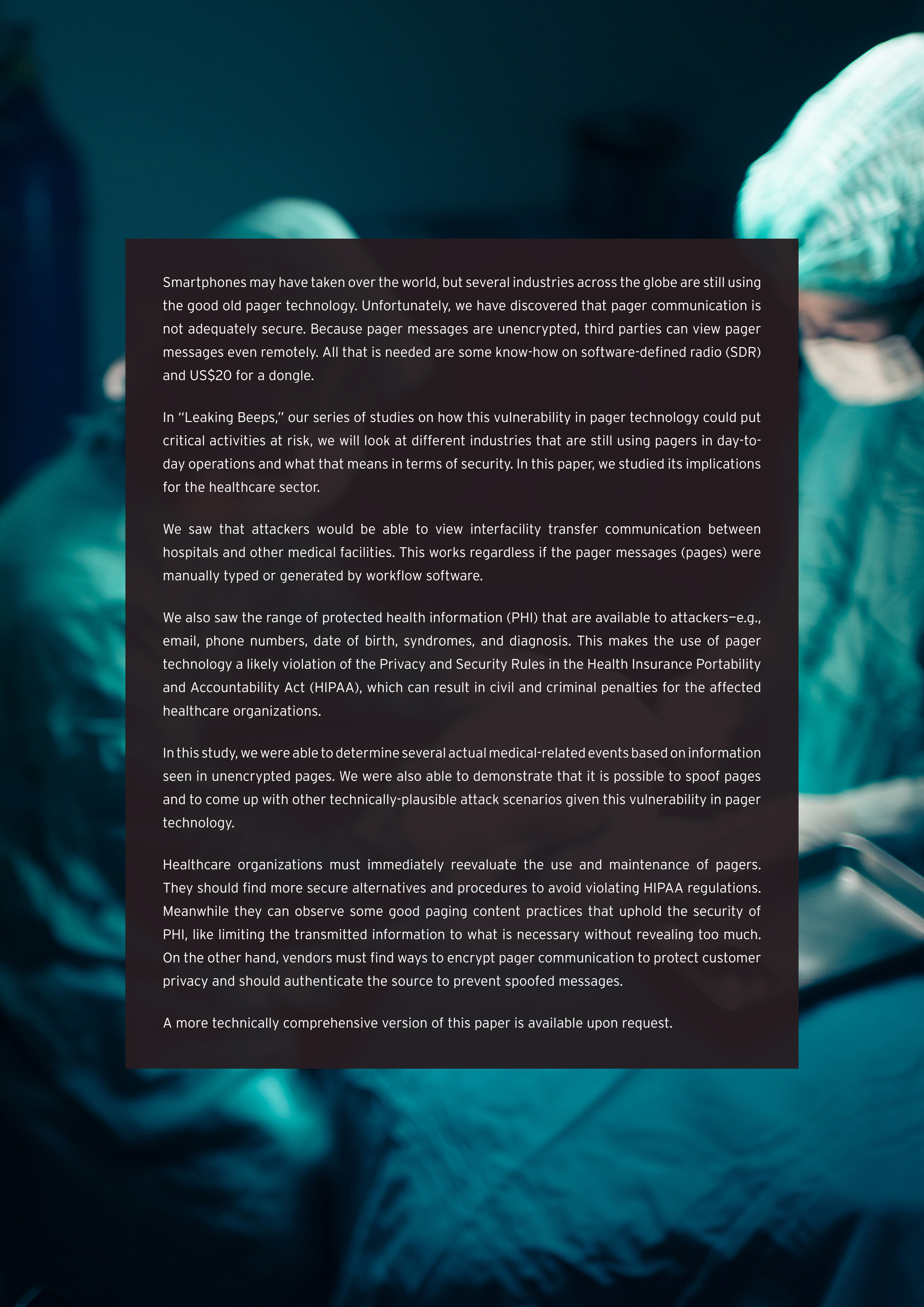
The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.



Contents



Smartphones may have taken over the world, but several industries across the globe are still using the good old pager technology. Unfortunately, we have discovered that pager communication is not adequately secure. Because pager messages are unencrypted, third parties can view pager messages even remotely. All that is needed are some know-how on software-defined radio (SDR) and US$20 for a dongle.

In "Leaking Beeps," our series of studies on how this vulnerability in pager technology could put critical activities at risk, we will look at different industries that are still using pagers in day-to-day operations and what that means in terms of security. In this paper, we studied its implications for the healthcare sector.

We saw that attackers would be able to view interfacility transfer communication between hospitals and other medical facilities. This works regardless if the pager messages (pages) were manually typed or generated by workflow software.

We also saw the range of protected health information (PHI) that are available to attackers—e.g., email, phone numbers, date of birth, syndromes, and diagnosis. This makes the use of pager technology a likely violation of the Privacy and Security Rules in the Health Insurance Portability and Accountability Act (HIPAA), which can result in civil and criminal penalties for the affected healthcare organizations.

In this study, we were able to determine several actual medical-related events based on information seen in unencrypted pages. We were also able to demonstrate that it is possible to spoof pages and to come up with other technically-plausible attack scenarios given this vulnerability in pager technology.

Healthcare organizations must immediately reevaluate the use and maintenance of pagers. They should find more secure alternatives and procedures to avoid violating HIPAA regulations. Meanwhile they can observe some good paging content practices that uphold the security of PHI, like limiting the transmitted information to what is necessary without revealing too much. On the other hand, vendors must find ways to encrypt pager communication to protect customer privacy and should authenticate the source to prevent spoofed messages.

A more technically comprehensive version of this paper is available upon request.

Pagers in the Age of Smartphones

Since the 1950s, physicians have been using pagers (also called beepers) that could receive pages up to 25 miles away from a single transmitter tower.[1] In the 1960s, the technologies used in walkie-talkies and automobile radios were combined to create the first transistorized pagers. It wasn't until the 1990s that the general public began using pager technology. However, its wider adoption was cut short as it was quickly replaced by current cellular technologies such as text messages or Short Message Service (SMS).

Pagers are still utilized today in many different sectors, mostly because they need at least one communication device to alert and inform an end user. IT departments, industrial automation, restaurants, and big hotels use pagers to deliver messages in a closed system within a limited distance. One of its primary uses seen today is within the healthcare sector—e.g., hospitals and large doctor offices. Most people who have been to hospitals recognize that the doctors and nurses still carry around pagers to help in the performance of their daily functions around facilities in many countries.

Cellular coverage can be weak or nonexistent inside a large hospital complex and mobile phone signals are thought to interfere with sensitive medical equipment. In Australia, Canada, European countries, Japan, and other countries, cellphones are still prohibited in specified areas in hospitals.[2]

As doctors and nurses need to receive messages in wards and operating rooms, pagers and Personal Handy-phone System (PHS) for medical facilities serve as an alternative means of communication.[3] In Japan, pagers or emergency radio using paging protocol are legally adopted as backup communication lines in cases of disasters.[4]

It doesn't take much power to transmit pages over long distances. Since it only requires a pre-defined wattage to be sent, pages were received even from tens of kilometers away from their transmitting facilities.

This research only focuses on the unencrypted pages that are sent over the air from medical facilities such as hospitals and large doctor offices.

Note that Trend Micro's passive observation of certain clear text message content in the course of its security research was not the result of any attempt by Trend Micro to intercept or procure any such communications, and we strongly advise against any attempt to do so, as most countries prohibit this by law and severe criminal and/or civil penalties may result (see, e.g., 18 U.S.C. 2511).

Analysis of Leaked Information

Pagers were designed before security was even a concern and privacy standards were just coming about. HIPAA was enacted in 1996 during the height of pager technologies.[5] Pagers are rarely encrypted and pages are sent over the airwaves unencrypted. Through technical means, we were able to decode pager messages using software-defined radio (SDR) and a USB dongle as cheap as $20.

After setting up our equipment and software to observe pager messages, we began analyzing what types of information are being passed along in the clear. We did this to determine how well pager technology—a relatively outdated means of communication—stands against today's attackers, who have easy access to decoding tools as well.

The pager contents themselves are varied in form. This pie chart shows the distribution of data types seen in this research:

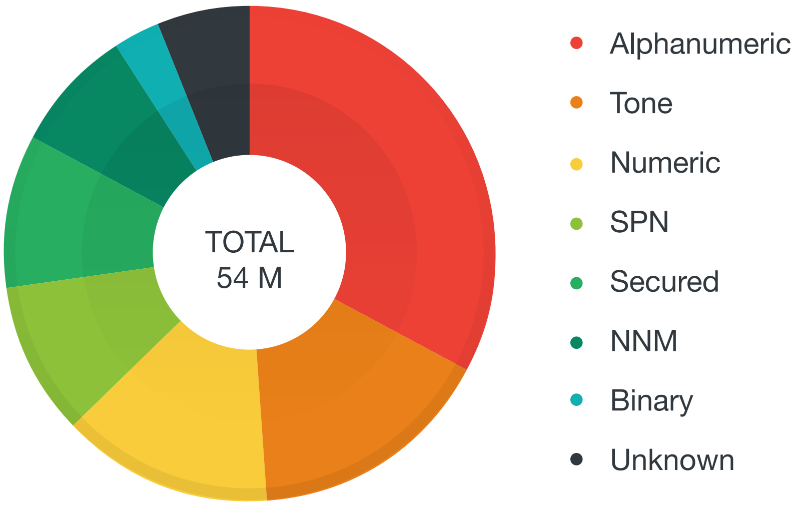


Figure 1: Data type distribution

Data Type	Percentage
Alphanumeric	33%
Tone	16%
Numeric	14%
SPN	10%
Secured	10%
NNM	8%
Binary	3%
Unknown	6%

While identifying the frequencies used in countries from around the world, we noticed that unencrypted pages are a systemic problem affecting several states in the US, and even other countries like Canada.

The period of our observation is from 25 January to 25 April 2016. During the four months of study, we have monitored 54,976,553 records of pages, among which 18,368,210 (33.41%) are alphanumeric, and among which 2,075,765 (11.3%) were transmitted from hospitals or healthcare centers.

Communication Inside and Outside the Hospital

Interfacility transfer (IFT) is defined as "any transfer, after initial assessment and stabilization, from and to a health care facility,"[6] a scenario where paging messages would be transmitted. Medical facilities include, but are not limited to clinics, hospitals, acute service, surgery hospitals, rehabilitation centers, and long-term care.

The protected health information (PHI) are associated to a patient in all forms of documentation, both in physical and electronic records, which includes the name, date of birth, telephone number, diagnosis.[7] It also includes information that that "enables safe, effective and efficient" IFT[8] such as levels of acuity, syndromes, hospital data, emergency department data, medical orders and special care,

To exercise discretion, a low voice is advised for oral communication. Although data encryption is not written in the protocols, "during a radio patch, information should be limited to what the receiving facility needs to know about the patient to prepare for the patent's arrival and treatment."[8] The name of the accepting physician may have to be included with the transfer orders, according to state or local laws.[9]

We have observed abundant IFT pages that were either generated by software with interfacility coordination functions or manually entered, as well as pages transmitted in the EMS (Emergency Medical Services) workflow.

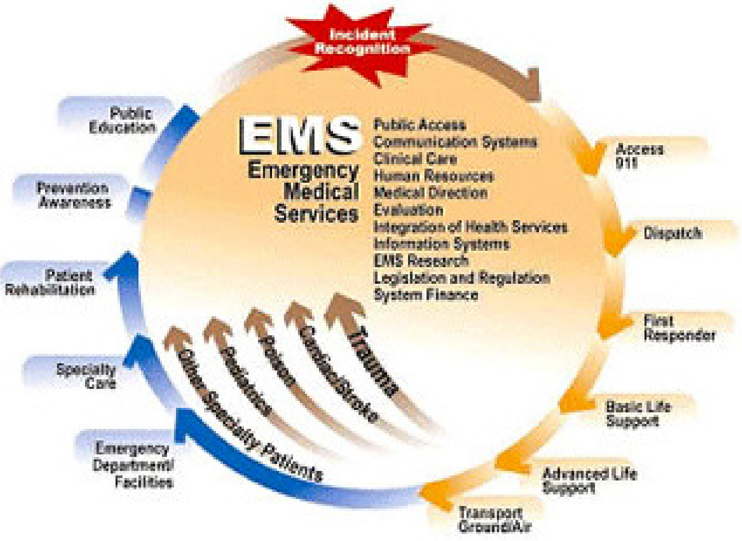
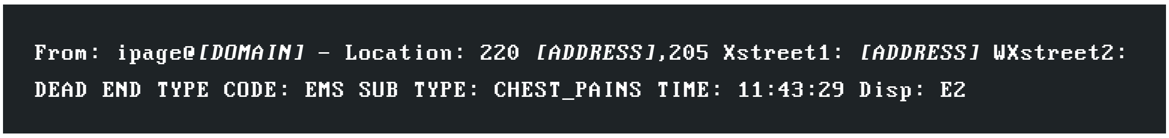


Figure 2: EMS System Approach and Components[10]

Imagine a case where there is a patient and someone calls 911 for help. As 911 receives the call, a message is sent to pagers in order to indicate location, incident type, and sub type.

The page for a patient with chest pain, for instance, may look like this:



```
From: ipage@[DOMAIN] - Location: 220 [ADDRESS],205 Xstreet1: [ADDRESS] WXstreet2:
DEAD END TYPE CODE: EMS SUB TYPE: CHEST_PAINS TIME: 11:43:29 Disp: E2
```

Based on what we've seen from the pages, transfer requests are not limited to 911. It could be a rescue team or an ambulance of a hospital, or even another medical facility, giving details before a patient arrives.

In fact, every step of the medical transaction could be observed from pages. We've seen pages describing admission to the emergency department, bed requests, in-facility transfer preparation requests, treatment orders, patient status updates up until the discharge or further transfer process. Many other similar tasks and activities transmitted via workflow software or otherwise can be observed through the pages.

Workflow software integrates a patient's electronic medical records (EMR), room/bed status, in-facility transportation, and location service (such that an alarm is automatically suppressed when a nurse comes), as well as post-acute referral and post-care phone calls. While some vendors put emphasis on security and confidentiality in their data centers, unencrypted radio signals may have a negative impact to confidentiality.

We also observed that a medical reference number (MRN) is usually included in pages sent by workflow software.

Protected Health Information

The table below shows statistics of protected health information (PHI) or sensitive information that were observed during the span of the research:

Email	805,609	28%
Medical terms	647,745	23%
English names	510,313	18%
Syndromes / Diagnosis	399,862	14%
Medicine on FDA drug list	164,117	6%
Phone numbers	124,949	4%
Date of birth, age, gender	110,708	4%
Medical reference number	90,124	3%
URL	6,371	0%

Table 1: Distribution of PHI seen during the span of the research

Among 84,400 records of a specific workflow software, there are 12,921 records with MRN, among which we could identify 4,628 distinct MRN, roughly 5,468 distinct names, and 21,795 distinct dates of birth. Patients are frequently transported from and to the following places: emergency department (ED), Diagnostic Radiology, Computed Tomography (CT), Echo, Magnetic Resonance Imaging (MRI), CPC, Interventional Holding, Ultrasound, Pediatric ED, Vascular Lab, Stress Lab. Interestingly, we found cases like a patient who went to EEG on the first day, MRI on the second, and EEG again on the third day. Some of these records are simple bed requests and do not contain PHI.

From an unidentified software, we have 401,795 records of PHI, where we can identify about 77 thousand patient names. There are optional medical reference numbers (MRN), patient's name, age, gender, unit, diagnosis and names of doctors. Popular units in this kind of pages are Central PPC, ED (emergency department), PACU (post-anesthesia care unit), SICU (surgical intensive care unit), ICU (intensive care unit), CCU (critical care unit), 2COH, operating room, DSU (day surgery unit).

The common diagnoses observed in the pages are the following:

Popular units in this kind of pages are Central PPC, ED (emergency department), PACU (post-anesthesia care unit), SICU (surgical intensive care unit), ICU (intensive care unit), CCU (critical care unit), 2COH, Operating Room, DSU (day surgery unit).

Exactly as written in pages, the common diagnoses observed are the following:

- CHEST PAIN (CP)
- UNSPECIFIED ABDOMINAL PAIN
- ENCOUNTER FOR SUPRVSN OF NORMAL PREGNANCY, UNSP TRIMESTER
- PNEUMONIA
- DYSPNEA
- SYNCOPE AND COLLAPSE
- FEVER
- WEAKNESS
- HEART FAILURE
- DEHYDRATION
- SHORTNESS OF BREATH (SOB)
- URINARY TRACT INFECTION
- SEPSIS
- ATHSCL HEART DISEASE OF NATIVE CORONARY ARTERY W/O ANG PCTRS
- OTHER INTESTINAL OBSTRUCTION
- ALTERED MENTAL STATUS
- BLEEDING
- HEADACHE

Uncommon diagnoses observed are the following:

- Suicidal intention
- PERIANAL ABSCESS
- Acute CVA (cerebrovascular accident)

Medical terms found in pages are related to the treatment or which organ or area is being examined in the patient. They may reveal the sickness and its severity. Note that ‘phleb’ is the first place, because a hospital used group pages to send copies of messages to a group of people, resulting in data bias.

Phleb	85,079
EKG	35,138
Sepsis	29,430
Xray	20,218
Ortho	12,591
Kidney	11,197
Anemia	10,988
Cellulitis	10,124
Resistivity	9,594
Dyspnea	8,417
Anesthesia	7,752
Atrial	6,767
Hemorrhage	6,529
Troponin	6,262
Nebulizer	6,107
Pharm	5,720
Stenosis	4,503
Pancreatitis	4,287
Endoscopy	3,894
Spirometry	2,429
Transvaginal	2,058

Table 2: Medical terms related to diseases seen in the research

Drugs in pages are even more relevant to a patient's sickness. We may guess a patient's disease through the kind of treatment accorded to the patient. We can also get a rough estimate of common sicknesses affecting an area.

Albuterol (a common bronchodilator)	23,175
Tylenol	6,134
Duoneb (treats COPD and asthma)	5,586
Coumadin (AKA Warfarin)	5,240
Ipratropium	5,020
Zofran (prevents nausea and vomiting)	4,844
Heparin (prolongs blood clotting time)	4,238
Insulin	4,197
Acetaminophen	3,669
Ativan (a benzodiazepine tranquilizer)	3,630
Ondansetron (treats vomiting)	3,545
Lasix (treats fluid retention in people with congestive heart failure, etc.)	3,278
Vancomycin[18] (last-line antibiotics)	3,029
Morphine	2,763
Nikki (treatment of moderate acne vulgaris)	1,554

Table 3: Medical terms related to treatments or cures seen in the research

Fortunately, the researchers also observed good practices that uphold the security of PHI. Some pages simply contain a patient's age, gender and a brief summary of symptoms. While the privacy is well-protected, doctors and nurses can still prepare before the patient arrives.

Case Studies

The following three case studies are meant to show that through the pages we were able to draw some reasonable assumptions related to the patient's medical transaction, treatment plan, and other details that would be considered confidential.

Case study of pages from the pharmacy

Pharmacies commonly receive a lot of pages. People with malicious intent can correlate the drugs used by a specific patient. For example, let's say Ondansetron, Pantoprazole and Cefepime are required for a certain patient. We can reasonably deduce that he or she has erosive esophagitis and the anti-nausea drug Ondansetron was prescribed to prevent side effects.

Case study of patient with acute kidney injury

A 26-year-old female was vomiting in the emergency department. A bed (#1029) was quickly requested and assigned as she was diagnosed with acute kidney injury, dehydration, DM gastroparesis (a condition where stomach motility is impaired), and hypokalemia (potassium deficiency in the blood stream, which can be fatal in this case).

After 10 days, she came to the hospital again with the same complaint. With her condition, she was supposed to die if the condition persisted for 10 days, so we could assume her that symptoms were relieved (or the first diagnosis was not accurate, which we cannot deduce). Another bed was requested and assigned for her.

After 12 days, she came to the hospital again, complaining of vomiting and nausea. Again, a bed (#0535) was requested and assigned. She was quickly diagnosed again as hypertensive emergency, N/V (nausea/vomiting), and diabetic gastroparesis.

For an unknown reason, she stayed in room #0393 and later transferred to #0565. We have no idea why her symptoms recurred and why such a serious disease happened to a 26-year-old woman.

Case study of patient with hyponatremia

A female patient of unknown age was sent to an emergency department at 3 AM on the first day. She was immediately transferred to a bed and diagnosed with chest pain and hyponatremia (a condition where the level of sodium in the blood is very low). At 7 AM, she went to CT and went to nuclear medication afterwards. She was back to bed at 9 AM and rested for the rest of the day.

On the second day, she went from the room to the stress lab at 8 AM, underwent inspection, and returned to her room at noon.

We don’t know what happened on the third day.

On the fourth day, she went from bed to nuclear medication again at 9 AM. Having done diagnostic radiology, she came back to bed and was discharged on a wheelchair with IV (intravenous injection) and left the hospital.

In this case, we could not guess the reason of her chest pain and hyponatremia. No medicine was prescribed through the paging system.

Spoofing Pages

Lots of information can be seen from sniffing pager messages. However, it is also possible to inject your own pages if you have basic information about the systems in use. Without encryption and authentication, pager messages are easy to spoof as there is no way to verify that the messages are sent from trusted and known sources.

To test these theories, Trend Micro bought some pagers to simulate the sending of pager messages. The goal was to send pages that were created by the researchers and prove that valid pagers would receive crafted messages from SDR. The simulation was done in a secure environment so it would not affect any existing pager systems.

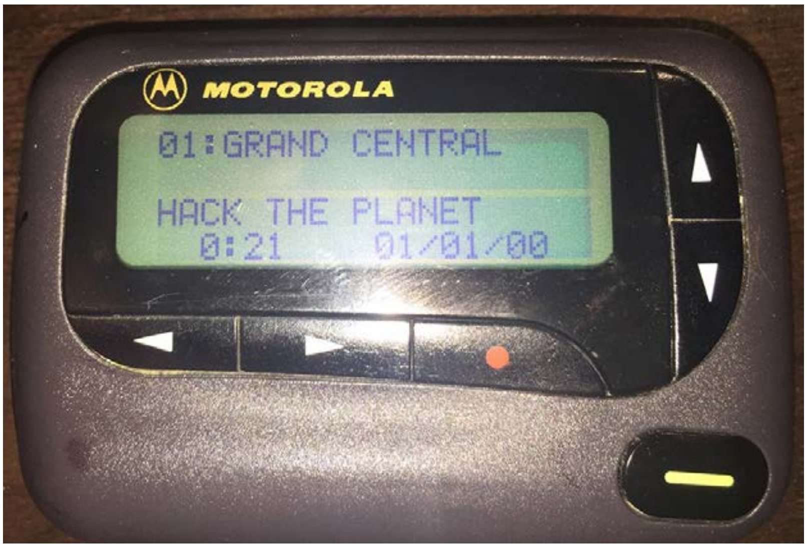


Figure 3: Test pager receiving test messages

Multiple tests were conducted to see the type of pager message formats sent and the cloning of these types. The messages were successfully sent and decoded by a couple of popular paging decoder software.

Based on the results, we can conclude that messages can be sent to any pager with the same protocol, as long as the transmitting power of the radio and antenna support the distance needed to successfully spoof messages. In this case, we tested the POCSAG (Post Office Code Standardization Advisory Group) protocol, which is one of just two protocols typically used by pagers, the other one being FLEX.

Our experiment proves that systems relying on pager technology can be easily compromised.

Possible Attacks

With private information being sent over the air through paging technologies that have no encryption and authentication, an obvious attack is to take advantage of the information against a potential target. Privacy regulations in various countries have prohibited protected health information from being leaked. However, this research reveals that the lack of encryption on private information has been overlooked for a long time.

While some people assume that communication is secure as it is going through private registered frequencies, it does not stop an attacker from looking into unencrypted frequencies. Trend Micro came up with some hypothetical attack scenarios based on information we saw during the research.

- **Sending pages to the pharmacy for medication –** Motivated attackers could sabotage a target's treatment program, wherein spoof pages can be sent to deliver medicine with a counter-effect (like Warfarin to patients with hemophilia). Patients dealing with drug addiction issues could perpetuate substance abuse by paging the pharmacy for excessive dosages of painkillers like morphine. Verification depends on the back end of the system to check whether the originating page was from an authorized source, along with pharmacists or other concerned medical staff to prevent the wrong medication from being administered.

- **Moving patients within facilities –** Attackers can also hijack pager messages to direct a target to the wrong operating room. This could cause issues with medical staff performing the wrong procedures to patients if the documentation is not updated or located in other venues within the facility. This could lead to inconvenience, irreparable damage or death, if attackers are aware of a target's preexisting condition.

- **Declaring an emergency inside facilities –** Pranksters and threat actors could spoof pages to declare an emergency. With this scenario, people can be driven to a specific area so that the attacker can isolate areas and have little resistance in gaining physical access to specific locations or facilities. The attacker could be physically going after a target or working on getting access to confidential information.

- **Intercepting calls from the officiating doctors –** Prior to surgery, the staff may ask for a conversation with the doctor. Pages can be sent to request the doctor to call the staff, which can be redirected to an attacker's phone number. If the doctor is not familiar with the requesting party, the information may be leaked to another person. Information like a patient's condition and severity of the disease can then be used as part of reconnaissance or directly for sabotage.

- **Stealing a dead person's identity –** In some countries and regions, a death notification is sent when a patient dies. It may be possible to steal relevant information and use the details to make claims on the family's behalf. Alternatively, an attacker can send pages to declare someone dead, causing unnecessary confusion or grief.
- **Spoofing messages –** There is an SMS gateway that forwards SMS messages to pagers. With messages claiming to be from a trusted source, this could be used in multiple types of attacks such as getting someone to leave a room, have someone call a number, visit malicious links, and other social engineering tactics.

What This Means

Patients in different countries like the US, UK, and Australia are assured through their contracts that personal and medical information are confidential. Medical or health privacy is an important aspect of providing healthcare service, involving both doctor discretion in discussing details of a patient's condition and the security of a patient's medical records. However, hospitals and other medical facilities may be routinely violating medical privacy agreements unknowingly through the continuous use of pager technology.

HIPAA recognizes the risks of using pager technology with unencrypted messages, which is usually the case. In fact, HIPAA discourages the use of pagers. Should hospitals insist on using this technology, it requires additional safeguards like user authentication.

Violations of HIPAA regulations by covered entities (CE) have corresponding penalties based on these several categories:

Category	Description	Penalty
Category 1	A violation where the CE was unaware and could not have realistically avoided the circumstance, exerted reasonable effort to abide by HIPAA Rules.	Minimum fine of $100 per violation up to $50,000
Category 2	A violation that the CE should have been aware but could not have avoided the circumstance even with a reasonable amount of care (but falling short of willful neglect of HIPAA Rules.)	Minimum fine of $1,000 per violation up to $50,000
Category 3	A violation that results from willful neglect of HIPAA Rules, where an attempt has been made to correct the violation.	Minimum fine of $10,000 per violation up to $50,000
Category 4	A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation.	Minimum fine of $50,000 per violation

Table 4: HIPAA Violation Penalty Structure[11]

Conclusion

Paging technology has been in the market for more than 60 years. Despite smartphones' role in our everyday life, there are still some industries that are dependent on the pager technology. Before software defined radio became popular, pager technology was considered secure despite the lack of encryption and authentication. An attacker had to pay big money or must have good knowledge on radio and hardware wiring to sniff clear text in the air.

Nowadays, anyone can simply buy a US$20 DVB-T USB dongle and run relevant software to do the same task. Even if pager protocols are expected to transmit messages reliably with low power, sniffers can be miles away from the target and still get the same information.

Trend Micro recommends the following practices to mitigate security issues and protect the PHI's privacy:

- **Encrypt the communication** - Even a simple pre-shared key (PSK) encryption can raise the bar for the attacker. More sophisticated encryption methods mean more secure communication. Given the current development in embedded hardware, asymmetric encryption is possible without much impact on cost.
- **Authenticate the source** - To prevent spoofed messages from being accepted by the system, there should be authentication designed in the firmware. When in doubt of weird medical information, make a phone call or meet with the person to verify the information.
- **Do not transmit multiple factors of PHI** - As the researchers have mentioned in the case of some healthcare providers, it is good practice to send pages that cannot be identified without relevant documentation on the receiving end. For example, medical reference numbers and part of the date of birth should be enough to confirm the identity of the patient when combined with offline information on the receiving end.

References

1. Wikipedia. (Unknown). *Wikimedia Foundation*. “Pager.” Last accessed on 10 August 2016, https://en.wikipedia.org/wiki/Pager.

2. Claudia Hammond. (14 May 2013). *BBC*. “Are mobile phones dangerous in hospitals?” Last accessed on 10 August 2016, http://www.bbc.com/future/story/20130513-can-you-use-phones-in-hospitals.

3. Unknown. (Unknown). ｜ワイモバイル（*Y!mobile*）法人/ビジネス向け. “医療・福祉機関でのご利用なら低電磁波のPHS.”Last accessed on 10 August 2016, http://www.ymobile.jp/biz/sp/medical.

4. Tokyo Tele Message Co., Ltd. (Unknown). Tokyo Tele message Co., Ltd. “New Press Release.” Last accessed on 11 August 2016, http://www.teleme.co.jp/service/multicast.

5. UC Berkeley. (Unknown). *UC Berkeley Committee for Protection of Human Subjects*. “HIPAA PHI: List of 18 Identifiers and Definition of PHI.” Last accessed on 10 August 2016, http://cphs.berkeley.edu/hipaa/hipaa18.html.

6. National Highway Traffic Safety Administration. (April 2006). *NHTSA*. “Guide for Interfacility Patient Transfer.” Last accessed on 10 August 2016, http://www.nhtsa.gov/people/injury/ems/Interfacility/images/Interfacility.pdf.

7. Missouri State University. (8 January 2007). *Board of Governors, Missouri State University*. “Missouri State HIPAA Privacy & Security Training.” Last accessed on 10 August 2016, http://apps.missouristate.edu/human/training/hipaatraining/trainingtext.htm.

8. Patient Transport Services. (August 2013). *TriHealth*. “Notice of Privacy Practices.” Last accessed on 10 August 2016, http://www.patienttransportservices.com/2013-09-23%20Privacy%20Statement-FINAL.pdf.

9. Office of Emergency Services. (April 2016). *National Highway Traffic Safety Administration.* “Guide fort Inferfacility Patient Transfer.” Last accessed on 19 August 2016, https://www.ems.gov/pdf/advancing-ems-systems/Provider-Resources/Interfacility_Transfers.pdf

10. Office of Emergency Services. (Unknown). *National Highway Traffic Safety Administration.* “FAQs.” Last accessed on 19 August 2016, https://www.ems.gov/faqs.html

11. HIPAA Journal. (24 June 1015). *HIPAA Journal*. “WHAT ARE THE PENALTIES FOR HIPAA VIOLATIONS?” Last accessed on 11 August 2016, http://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096.

Created by:

TrendLabs

The Global Technical Support and R&D Center of **TREND MICRO**

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver topranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO™

Securing Your Journey
to the Cloud

www.trendmicro.com